Management Software

AT-S94

WEB User's Guide

For use with the AT-8000S Series Stackable Fast Ethernet Switches

Version 3.0.0.40

613-001364 Rev A

Allied Telesis™

Table of Contents

Preface

This guide contains instructions on how to configure an AT-8000S Series Layer 2 Fast Ethernet Switch using the interface in the *Embedded Management System* (EWS).

The Embedded Management System enables configuring, monitoring, and troubleshooting of network devices remotely via a web browser. The web pages are easy-to-use and easy-to-navigate.

This preface provides an overview of the Web Browser Interface User’s Guide, and includes the following sections:

- Web Browser Interface User’s Guide Overview
- Intended Audience

Web Browser Interface User's Guide Overview

The Web Browser Interface User's Guide provides the following sections:

- **Section 1,Section Title"Getting Started"** — Provides information for using the Embedded Web Management System, including adding, editing, and deleting configurations.
- **Section 2, Section Title"Defining System Information"** — Provides information for defining basic device information.
- **Section 3, Section Title"Configuring IPv6"** — Provides information for configuring IPv6.
- **Section 4**, **Section Title"Configuring System Time"** — Provides information for configuring Daylight Savings Time and Simple Network Time Protocol (SNTP).
- **Section 5, Section Title"Configuring Device Security"** — Provides information for configuring both system and network security, including traffic control, and switch access methods.
- **Section 6, Section Title"Configuring DHCP Snooping"**— Provides information for configuring DCHP Snooping.
- **Section 7, Section Title"Configuring Ports"** — Provides information for configuring ports, port aggregation, port mirroring and LACP.
- **Section 8, Section Title"Configuring Interfaces"** — Provides information for defining ports, LAGs, and VLANs.
- **Section 9, Section Title"Configuring System Logs"** — Provides information for setting up and viewing system logs, and configuring switch log servers.
- **Section 10, Section Title"Configuring Spanning Tree"** — Provides information for configuring Classic, Rapid, and Multiple Spanning Tree.
- **Section 11, Section Title"Configuring Multicast Forwarding"** — Provides information for configuring both the static and dynamic forwarding databases.
- **Section 12, Section Title"Configuring SNMP"** — Provides information for configuring SNMP access and management.
- **Section 13, Section Title"Configuring Power Over Ethernet"** — Provides information for configuring Power over Ethernet (PoE) on the device.
- **Section 14, Section Title"Configuring Services"** — Provides information for configuring Quality of Service CoS parameters.
- **Section 15, Section Title"System Utilities"** — Provides information for managing system files.
- **Section 16, Section Title"Viewing Statistics"** — Provides information about viewing device statistics, including Remote Monitoring On Network (RMON) statistics, and device history events.
- **Section 17, Section Title"Managing Stacking"** — Provides information for stacking, including a stacking overview.
- **Appendix A, Appendix Title"Downloading Software with the CLI"** — Provides information for downloading device software through the command line interface.
- **Appendix B, Appendix Title"System Defaults"**— Provides the device defaults.

Intended Audience

This guide is intended for network administrators familiar with IT concepts and terminology.

Document Conventions

This document uses the following conventions:

Note

Provides related information or information of special importance.

Caution

Indicates potential damage to hardware or software, or loss of data.

Warning

Indicates a risk of personal injury.

Contacting Allied Telesis

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

New Management Software Releases

New releases of management software are on the Allied Telesis web site. In addition, the installation and user guides are available for all Allied Telesis products in portable document format (PDF) on our web site. Both the management software and the product documentation are available at **www.alliedtelesis.com/support/software/**.

Once you access the web site, enter the hardware product model in the **Search by Product Name** field; for example, enter AT-8000S/24. Then click **Find.** You can download the management software. In addition, you can view the documents online or download them onto your local workstation or server.

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 Support section of the Allied Telesis web site: **www.alliedtelesis.com/support**.

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/support/rma.aspx**.

For Sales Information

You can find the contact information for Allied Telesis sales offices or valued resellers listed on our web site at **www.alliedtelesis.com/purchase**. To purchase Allied Telesis products directly, contact one of our sales representatives or one of our valued resellers.

Warranty

Go to **www.alliedtelesis.com/support/warranty** for the specific terms and conditions of the warranty and for warranty registration for the AT-8000S Series Stackable Ethernet Switches.

Chapter 1. Getting Started

This section provides an introduction to the Web Browser Interface, and includes the following topics:

- Starting the Application
- User Interface Components
- Logging Out
- Resetting the Device
- Configurable Login Banner

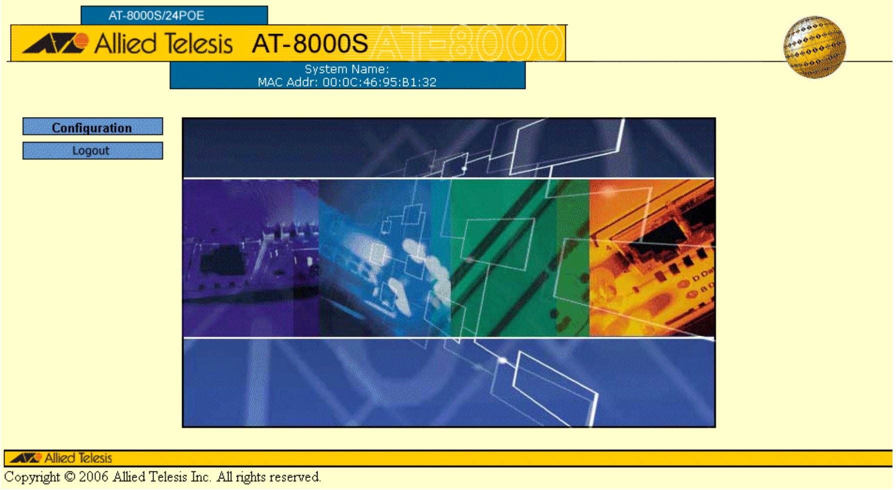
Starting the Application

This section contains information for starting the application. The login information is configured with a default user name and password. The default password is *friend*; the default user name is *manager*. Passwords are both case sensitive and alphanumeric. Additional user names can be added.

To open the application:

1. Open a web browser.
2. Enter the device IP address in the address bar and press <**Enter**>. The *Embedded Web System Login Page* opens:

Figure 1: Embedded Web System Login Page



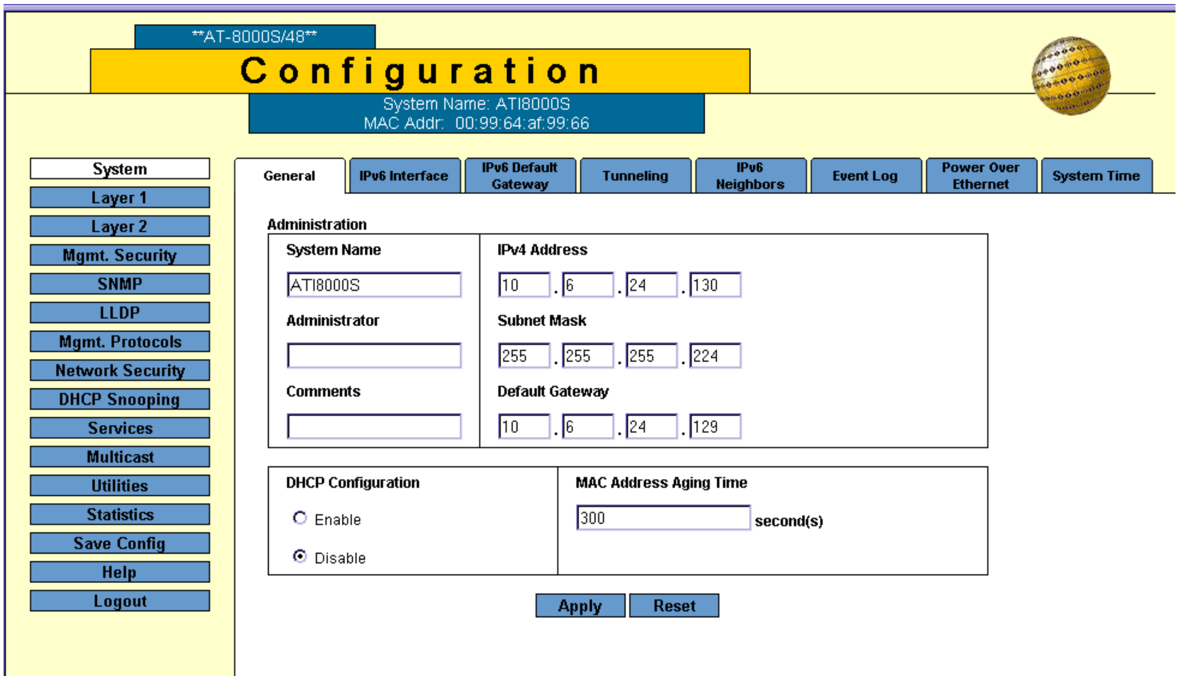
System Name:
MAC Addr: 00:0C:46:95:B1:32

Copyright © 2006 Allied Telesis Inc. All rights reserved.

3. Enter *manager* in the *User Name* field.
4. Enter *friend* in the *Password* field.

5. Click **Sign In**. The *System General Page* opens:

Figure 2: System General Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Administration

System Name: ATI8000S

Administrator:

Comments:

IPv4 Address: 10 . 6 . 24 . 130

Subnet Mask: 255 . 255 . 255 . 224

Default Gateway: 10 . 6 . 24 . 129

DHCP Configuration: ○ Enable ● Disable

MAC Address Aging Time: 300 second(s)

Using the Web Browser Interface

This section provides general information about the interface, and describes the following topics:

- Viewing the Device Representation
- User Interface Components
- Using the Management Buttons
- Adding, Modifying and Deleting Information

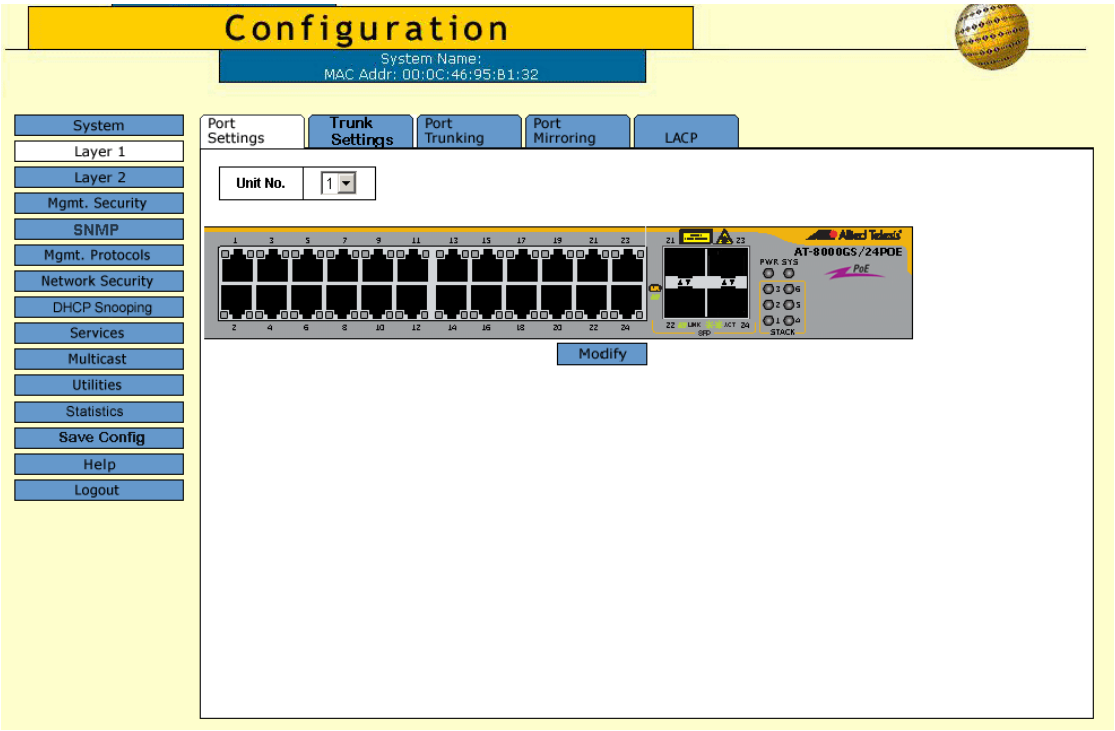
Viewing the Device Representation

Zoom Views provide a graphical representation of the device ports. The *Port Settings Page* displays an example of the Zoom View with a detailed graphical representation of the device ports.

To open a zoom view of device ports:

- Click **Layer 1 > Port Settings**. The *Port Settings Page* opens:

Figure 3: Port Settings Page



System Name:
MAC Addr: 00:0C:46:95:B1:32

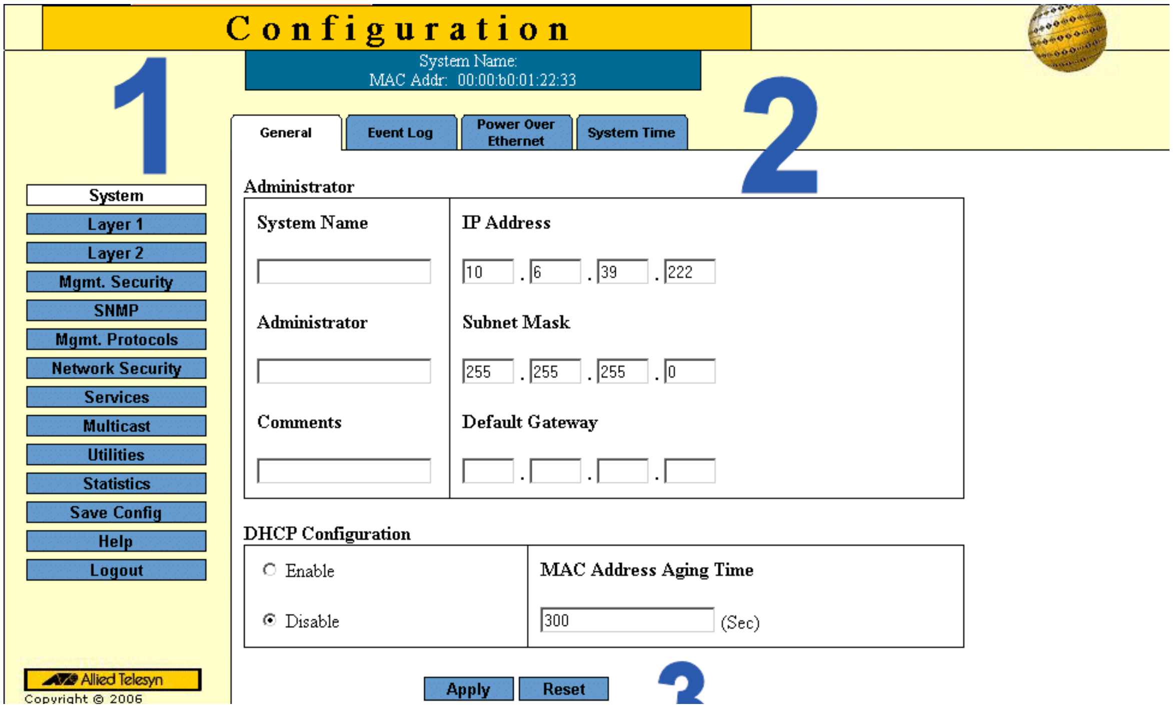
Unit No. 1

The port status indicators vary with context, for example the general port status indicators are as in the figure above while port mirror indicators are different. Indicator legend descriptions are provided with each context of the specific Zoom View.

User Interface Components

The *System General Page* example shows the interface components.

Figure 4: System General Page



System Name:
MAC Addr: 00:00:b0:01:22:33

Administrator

System Name
IP Address: 10 . 6 . 39 . 222
Administrator
Subnet Mask: 255 . 255 . 255 . 0
Comments
Default Gateway: . . .

DHCP Configuration
○ Enable
● Disable

MAC Address Aging Time: 300 (Sec)

The following table lists the interface components with their corresponding numbers:

Table 1: Interface Components

	Component	Description
1	Menu	The Menu provides easy navigation through the main management software features. In addition, the Menu provides general navigation options.
2	Tabs	Provide navigation to configurable device sub-features.
3	Management Buttons	Enable configuring parameters and navigation to other pages, see *Using the Management Buttons.*

Using the Management Buttons

Management buttons provide an easy method of configuring device information, and include the following:

Table 2: Configuration Management Buttons

Button	Button Name	Description
	Add	Opens a page which creates new configuration entries.
	Create	Opens a page which creates new configuration entries.
	Modify	Modifies the configuration settings. The configuration change is saved to the Running Configuration file and is maintained until reset or power-up.
	Apply	Saves configuration changes to the device. The configuration change is saved to the Running Configuration file and is maintained until reset or power-up.
	Configure	Opens a page which creates or modifies configuration entries.
	Delete	Deletes the selected table and configuration entries.
	View	Displays detailed information for the current page/configuration.
	Refresh	Refreshes information displayed on the current page.
	Reset	Device reset. Resets the device information for all device parameters according to current configuration.
	Defaults	Configuration reset. Resets the information for all parameters in the current context (page/tab) to predefined defaults.

Table 2: Configuration Management Buttons

Button	Button Name	Description
	Test	Performs a diagnostic test.
	Clear All Counters	Removes all counters.
The application menu includes the following general purpose buttons:		
	Configuration	Opens the default configuration page (*System General*).
	Login	Signs the user into the WBI, starts the management session.
	Logout	Signs the user out of the WBI, ending the management session.
	Help	Opens the online help page.
	Exit Help	Closes the online help page.
	Save Config	Used when configuration changes to the device need to be saved as permanent. The configuration is saved as permanent by copying the current Running Configuration file to the Startup Configuration file.

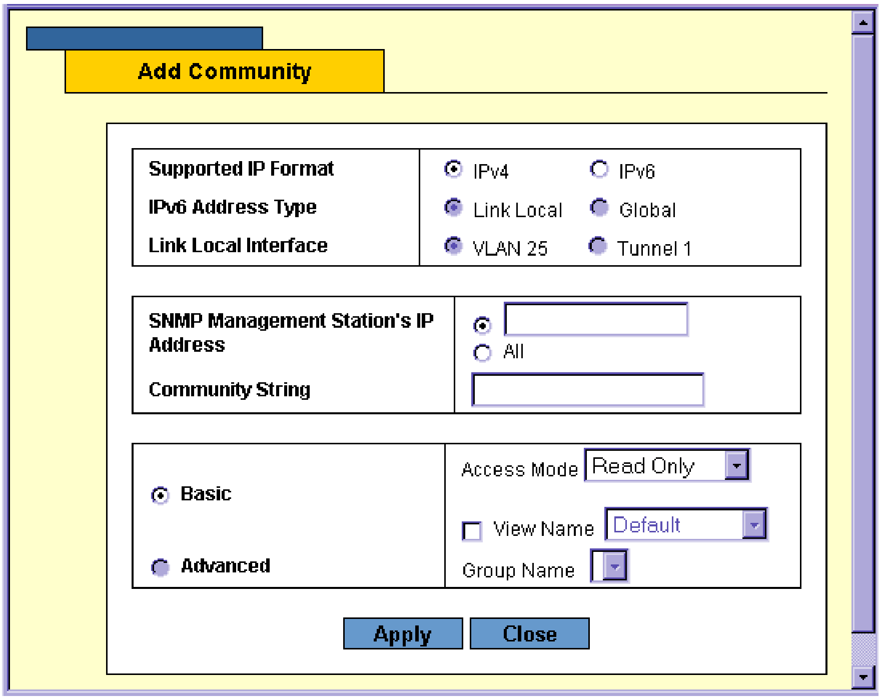
Adding, Modifying and Deleting Information

The WBI contains and tables for configuring devices. User-defined information can be added, modified or deleted in specific WBI pages.

To add information to tables or WBI pages:

1. Open a WBI page.
2. Click **Add**. An *Add* page opens, for example, the *Add Community Page*:

Figure 5: Add Community Page



Add Community

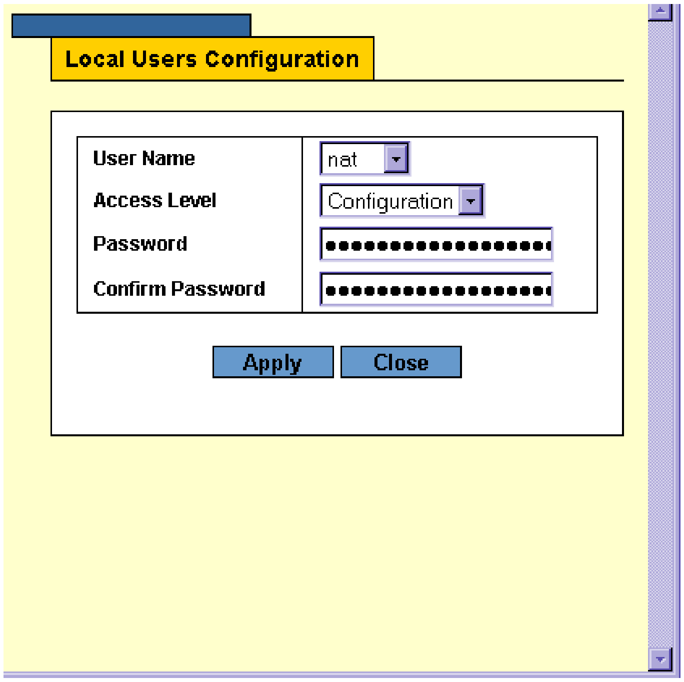
Supported IP Format ● IPv4 ○ IPv6
IPv6 Address Type ● Link Local ○ Global
Link Local Interface ● VLAN 25 ○ Tunnel 1
SNMP Management Station's IP Address ● ______ ○ All
Community String ______
● Basic
Access Mode Read Only
□ View Name Default
○ Advanced
Group Name

3. Define the fields.
4. Click **Apply**. The configuration information is saved, and the device is updated.

To modify information in tables or WBI pages:

1. Open a WBI page.
2. Select a table entry.
3. Click **Modify**. A Modify (or Settings) page opens, for example, the *Local User Settings Page*:

Figure 6: Local User Settings Page



User Name: nat
Access Level: Configuration
Password: ●●●●●●●●●●●●●●●●●●
Confirm Password: ●●●●●●●●●●●●●●●●●●

4. Define the fields.
5. Click **Apply**. The fields are modified, and the information is saved to the device.

To delete information in tables or WBI pages:

1. Open the WBI page.
2. Select a table row.
3. Click **Delete**. The information is deleted, and the device is updated.

Saving Configurations

User-defined information can be saved for permanent use or until next update, not just for the current session. A configuration is saved as permanent by copying the current Running Configuration file to the Startup Configuration file.

To save changes permanently:

- Click **Save Config** on the menu.

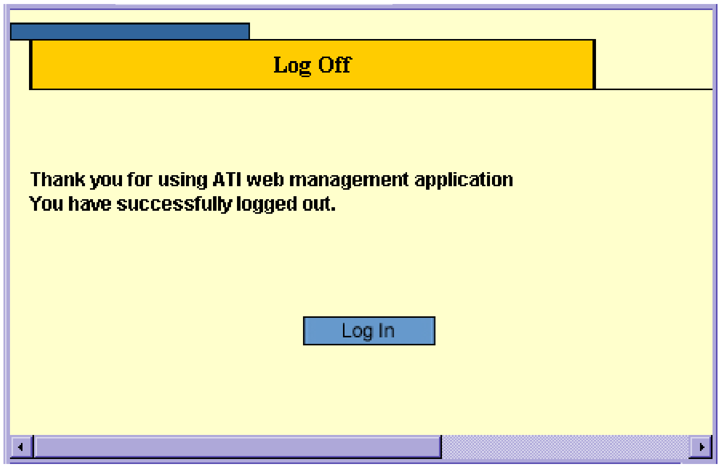
Logging Out

The Logout option enables the user to log out of the device thereby terminating the running session.

To log out:

- In any page, click **Logout** on the menu. The current management session is ended and the *Log Off Page* opens:

Figure 7: Log Off Page



Thank you for using ATI web management application
You have successfully logged out.

Resetting the Device

The Reset option enables resetting the device from a remote location.

Note

Save all changes to the Running Configuration file before resetting the device. This prevents the current device configuration from being lost. See also *"System Utilities"*.

To reset the device:

1. In the *System General Page*, click **Reset**. You are prompted to confirm.
2. Click **OK**. The device is reset. Resetting the device ends the web browser management session. You must restart the session to continue managing the device. After the device is reset, a prompt for a user name and password displays.
3. Enter a user name and password to reconnect to the Web Interface.

To reset the device to the predefined default configuration:

- In the *System General Page*, click **Defaults**. The default settings are restored and the device is reset.

Configurable Login Banner

The system supports a text based banner that is configurable only via a CLI command to enable the telnet session to display security messages above the login prompt prior to login.

To compose a login banner:

- Enter the CLI command **login_banner "*text string*"**. The text string length is a maximum of 159 characters (surrounded by quotes).

To remove the login banner:

- Enter the CLI command **login_banner ""** with an empty string.

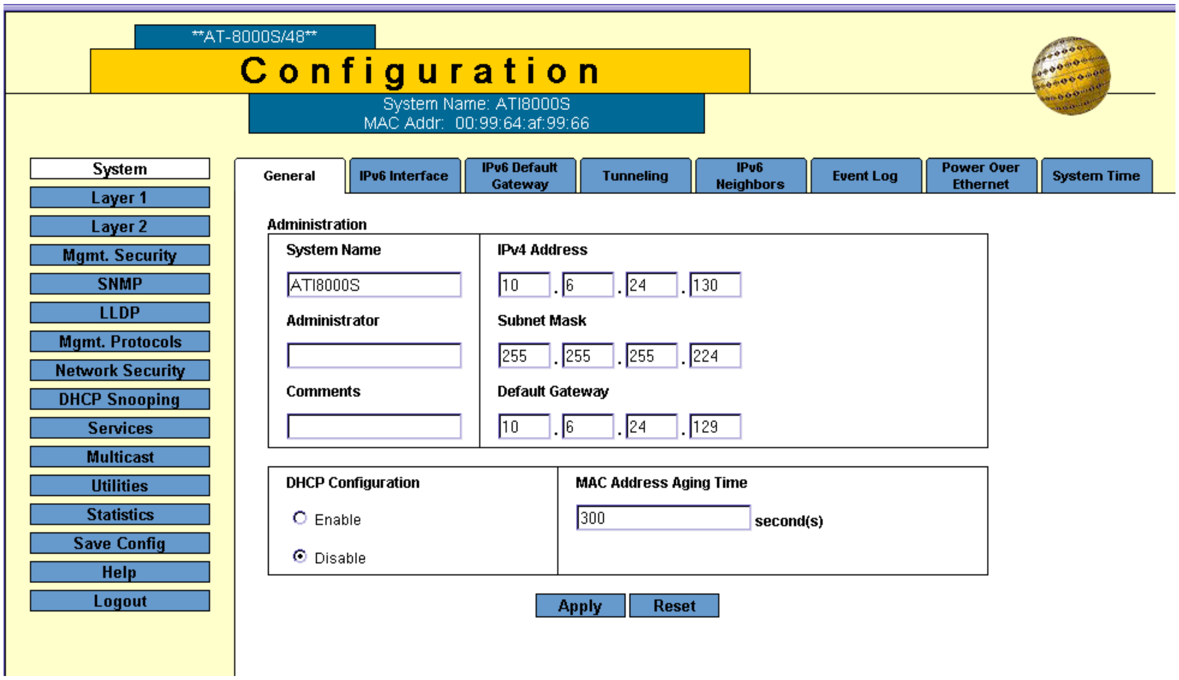
Chapter 2. Defining System Information

The *System General Page* contains general device information, including system name and its IPv4 addressing, administrator and passwords information, *Dynamic Host Configuration Protocol* (DHCP) configuration and MAC Address Aging Time.

To define the general system information:

1. Click **System > General**. The *System General Page* opens:

Figure 8: System General Page



AT-8000S/48

Configuration

System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Administration

System Name: ATI8000S

Administrator:

Comments:

IPv4 Address: 10 . 6 . 24 . 130

Subnet Mask: 255 . 255 . 255 . 224

Default Gateway: 10 . 6 . 24 . 129

DHCP Configuration

○ Enable

● Disable

MAC Address Aging Time: 300 second(s)

The *System General PageSystem General PageSystem General Page* comprises two sections: *Administration* and *DHCP Configuration*.

The *Administration* section of the*System General PageSystem General PageSystem General Page System General Page* contains the following fields:

- **System Name** — Indicates the user-defined name of the device. This is a required field.
  The field range is 0-159 characters.
- **Administrator** — Indicates the name of the administrator responsible for managing the device. The field range is 0-159 characters.
- **Comments** — (Optional) The user can add any comments about the device in this field, for example, fill in the location of the device.
- **IPv4 Address** — Indicates the device's IPv4 address.
- **Subnet Mask** — Indicates the device's subnet mask.
- **Default Gateway** — The IP address of a router for remote management of the device. The address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

Note

Packets are forwarded to the default IP when frames are sent to a remote network via the default gateway. The configured IP address must belong to the same subnet as one of the IP interfaces.

The *DHCP Configuration* section of the*System General Page System General Page* contains the following fields:

- **DHCP Configuration** — Indicates if the *Dynamic Host Configuration Protocol* (DHCP) is enabled.
  – *Enable* — DHCP dynamically assigns IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. If the DHCP client software is activated, the device immediately begins to query the network for a DHCP server. The device continues to query the network for its IP configuration until it receives a response. If the device and IP address are manually assigned, that address is deleted and replaced by the IP address received from the DHCP server.
  – *Disable* — Disables DHCP on the device. In this case, the device, following reset, checks if the IP address is already defined in the Startup Configuration. If not, the device tries to receive an IP address from a BootIP server until either an IP address is received or the user defines the IP address manually.
- **MAC Address Aging Time** — The time interval an inactive dynamic MAC address can remain in the MAC address table before it is deleted. The default time is 300 seconds, and the range is 10-630.

2. Define the relevant fields.
3. Click **Apply**. The system general information is defined and the device is updated.
4. Click **Save Config** on the menu to save the changes permanently.

Chapter 3. Configuring IPv6

The device functions as an IPv6 compliant Host, as well as an IPv4 Host (also known as dual stack). This allows device operation in a pure IPv6 network as well as in a combined IPv4/IPv6 network.

The primary change from IPv4 to IPv6 is the length of network addresses. IPv6 addresses are 128 bits long, whereas IPv4 addresses are 32 bits; allowing a much larger address space.

This section contains information on configuring the Internet Protocol Version 6 (IPv6) of the device.

IPv6 Syntax

The 128-bit IPv6 address format is divided into eight groups of four hexadecimal digits. Abbreviation of this format is done by replacing a group of zeros with *double colons*. The IPv6 address representation can be further simplified by suppressing the leading zeros.

IPv6 Prefixes

While Unicast IPv6 addresses written with their prefix lengths are permitted, in practice their prefix lengths are always 64 bits and therefore are not required to be expressed. Any prefix that is less than 64 bits is a route or address range that is summarizing a portion of the IPv6 address space.

For every assignment of an IP address to an interface, the system runs the *Duplicate Address Detection* algorithm to ensure uniqueness.

An intermediary transition mechanism is required for IPv6-only nodes to communicate with IPv6 nodes over an IPv4 infrastructure. The tunneling mechanism implemented is the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). This protocol treats the IPv4 network as a virtual IPv6 local-link, with each IPv4 address mapped to a Link Local IPv6 address.

This section describes the following topics:

- Defining IPv6 Interfaces
- Defining the IPv6 Default Gateway
- Configuring Tunnels
- Defining IPv6 Neighbors

Defining IPv6 Interfaces

The *IPv6 Interface Page* provides parameters for defining an IPv6 interface. When an interface is selected on a locally connected device, the system creates an IP interface and automatically configures a Link Local address on the interface. The automatically generated Link Local IPv6 address cannot be removed.

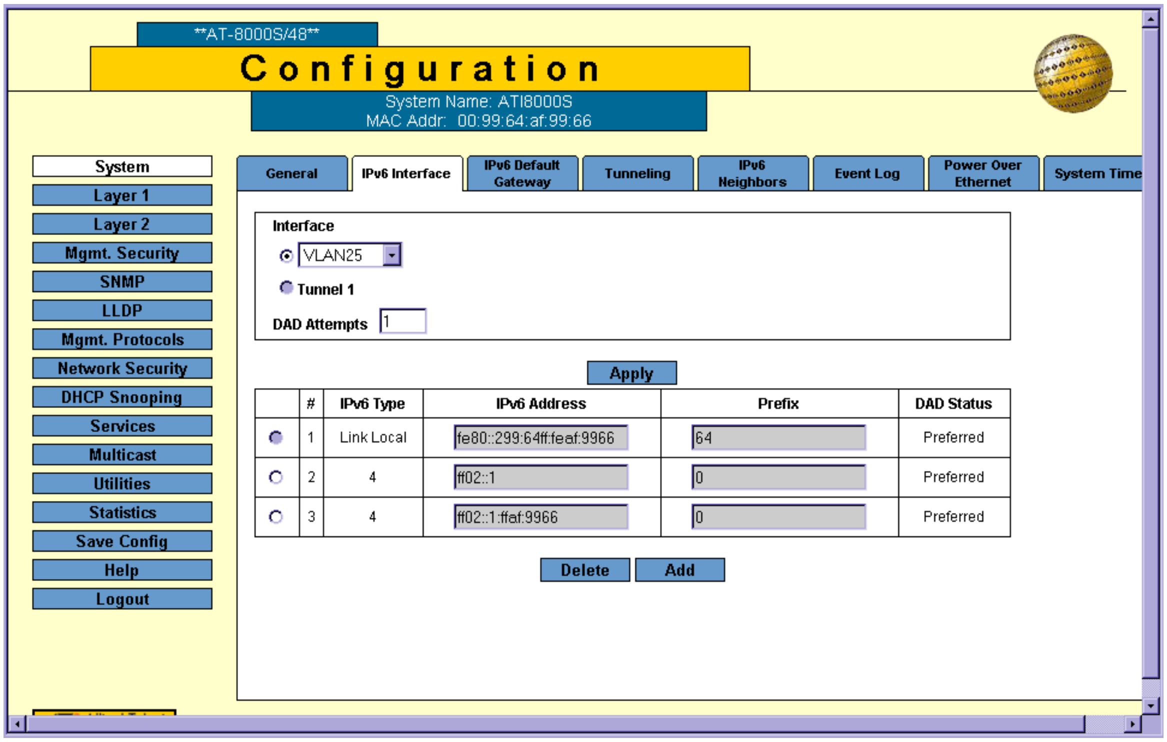
In addition to the dynamically configured IPv6 interfaces, there are two types of static IP addresses that can be configured on an IPv6 interface:

- **Link Local Address** — Defines a Link Local address that is non-routable and used for communication on the same network only.
- **Global Addresses** — Defines a globally unique IPv6 address; visible and reachable from different subnets.

To define IPv6 Interfaces:

1. Click **System > IPv6 Interface**. The *IPv6 Interface Page* opens.

Figure 9: IPv6 Interface Page



Interface
● VLAN25
○ Tunnel 1
DAD Attempts 1

	#	IPv6 Type	IPv6 Address	Prefix	DAD Status
●	1	Link Local	fe80::299:64ff:feaf:9966	64	Preferred
○	2	4	ff02::1	0	Preferred
○	3	4	ff02::1:ffaf:9966	0	Preferred

The *IPv6 Interface Page* contains the following fields:

- **Interface** — Indicates the interface on which the IPv6 interface is defined. The possible field values are:
  - *VLAN* — Indicates the VLAN ID on which IPv6 is enabled.
  - *Tunnel1* — Indicates the IPv6 tunnel on which IPv6 is enabled.
- **DAD Attempts** — Defines the number of consecutive neighbor solicitation messages that are sent on an interface while DAD is performed on Unicast IPv6 addresses on this interface. New addresses remain in a tentative state while duplicate address detection is performed. The range is 0 - 600. A field value of 0, disables duplicate address detection processing on the specified interface. A field value of 1 is the default.

The IPv6 Table on the *IPv6 Interface Page* displays the IPv6 addresses defined on the Interface. This table contains the following fields:

- **Delete Button** — Deletes the selected IPv6 address. Entries that cannot be removed because they are generated automatically by the system are unavailable. Only addresses configured by a user can be removed. The possible field values are:
  - *Selected* — Removes the selected IPv6 address.
  - *Cleared* — Maintains the IPv6 address.
- **IPv6 Type** — Defines the type of configurable IPv6 IP address for the interface. The possible values are:
  - *Link Local* — Defines a Link Local address; non routable and can be used for communication on the same network only. A Link Local address has a prefix of 'FE80'.

  - *Global* — Defines a globally unique IPv6 address; visible and reachable from different subnets.
- **IPv6 Address** — Indicates the IPv6 address assigned to the interface.
- **Prefix** — Specifies the length of the IPv6 prefix. The length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). The range is 3 -128 (64 in the case EUI-64 parameter is used). The Prefix field is applicable only on a static IPv6 address defined as a Global IPv6 address.
- **DAD Status** — Displays the DAD Status which is the process of verifying and assuring an inserted IPv6 address is unique. This is a read-only parameter with the following field values:
  - *Tentative* — Indicates the system is in process of IPv6 address duplication verification.
  - *Duplicate* — Indicates the IPv6 address is being used by another host on the network. The duplicated IPv6 address is suspended and is not used for sending or receiving any traffic.
  - *Active* — Indicates the IPv6 address is set to active.

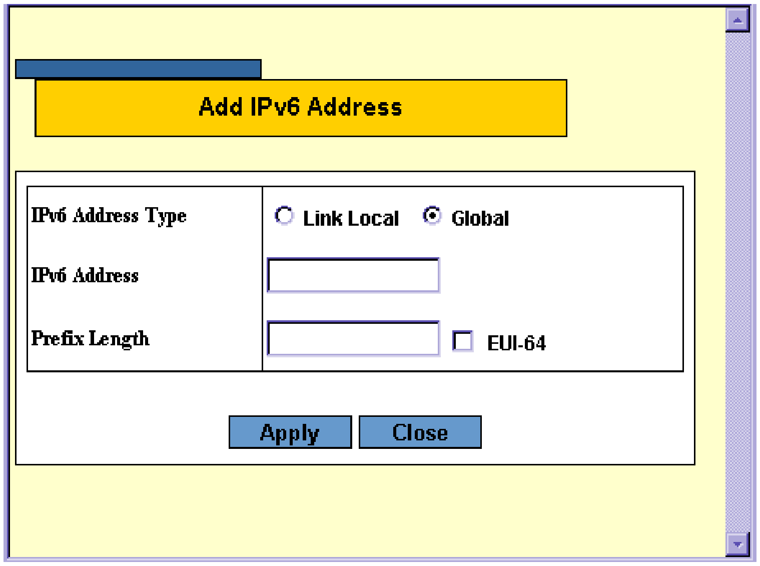
2. Select an Interface.
3. Define the **DAD Attempts** for an existing interface. DAD Attempts are disabled for Tunnel interface. The range is 0 - 600.
4. Click **Apply**. The DAD Attempts are defined, and device is updated.

Adding Multiple IPv6 Addresses

The Add IPv6 Address Page allows the user to add multiple IPv6 addresses to an existing IPv6 interface.

1. Click **Add**. The *Add IPv6 Address Page* opens.

Figure 10: Add IPv6 Address Page



Add IPv6 Address

IPv6 Address Type	○ Link Local ● Global
IPv6 Address	
Prefix Length	□ EUI-64

In addition to the fields in the Add IPv6 Address Page, the Add IPv6 Address Page contains the following field:

- **EUI-64** — Indicates the interface ID (low-order 64 bits of the IPv6 address) is built from the system base MAC address. The following fields options are:
  - *Checked* — Enables the **EUI-64** option. This option is relevant only to Global IPv6 addresses.
  - *Unchecked* — Disables the **EUI-64** option. This is the default value.

2. Select an Interface to map to the IP address.
3. Select an IPv6 Address Type.
4. Define the IPv6 address. Selecting a **Global** in the **IPv6 Address Type** requires defining the Prefix Length or selecting the **EUI-64** check box.
5. Click **Apply**. The IPv6 address is mapped to the Interface, and the device is updated.

Defining the IPv6 Default Gateway

The *IPv6 Default Gateway Page* enables you to configure the IPv6 address of the next hop that can be used to reach the network. Two IPv6 Link-Local address formats are used: standard and one with a specified IPv6 interface identifier. For IPv6, the configuration of the default gateway is not mandatory, as hosts can automatically learn of the existence of a router on the local network via the router advertisement procedure.

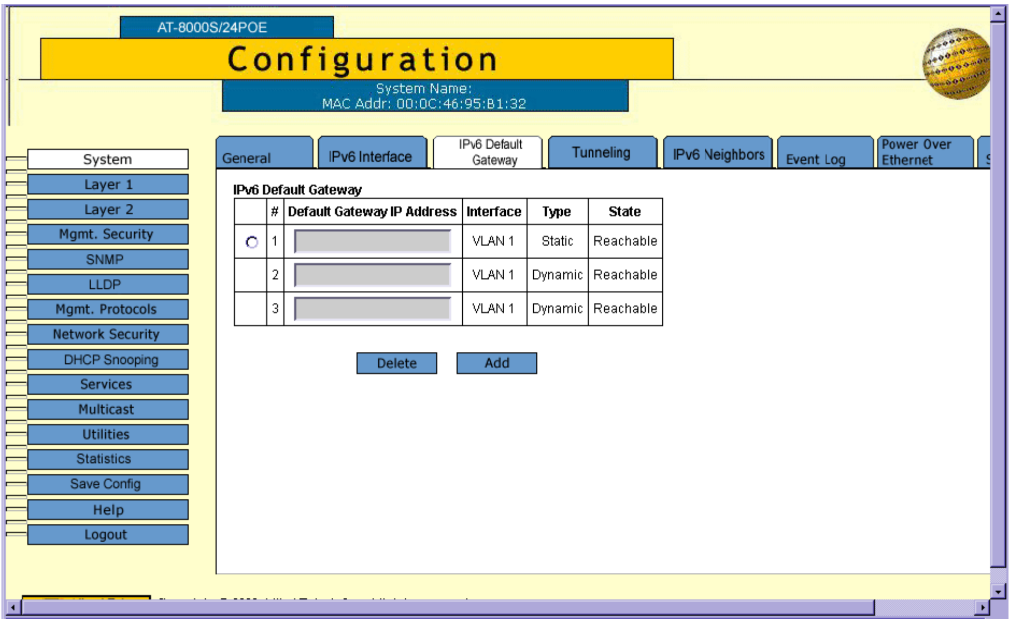
Unlike IPv4, the IPv6 default gateway can have multiple IPv6 addresses, which may include only one user-defined static address and multiple dynamic addresses that are learned via router advertised message provided in the IPv6 Default Gateway configuration. The user-defined default gateway has a higher precedence over automatically advertised addresses. It should be noted that configuring a new static default gateway without deleting the previously configured one overwrites the previous configuration.

- When removing an IP interface, all of its default gateway IP addresses are removed.
- An Alert message appears when attempting to insert a global IPv6 address.
- An Alert message appears when attempting to insert more than one user-defined address.

To define an IPv6 Preferred Router:

1. Click **System > IPv6 Default Gateway**. The *IPv6 Default Gateway Page* opens.

Figure 11: IPv6 Default Gateway Page



IPv6 Default Gateway

	#	Default Gateway IP Address	Interface	Type	State
○	1		VLAN 1	Static	Reachable
	2		VLAN 1	Dynamic	Reachable
	3		VLAN 1	Dynamic	Reachable

The *IPv6 Default Gateway Page* contains the following fields:

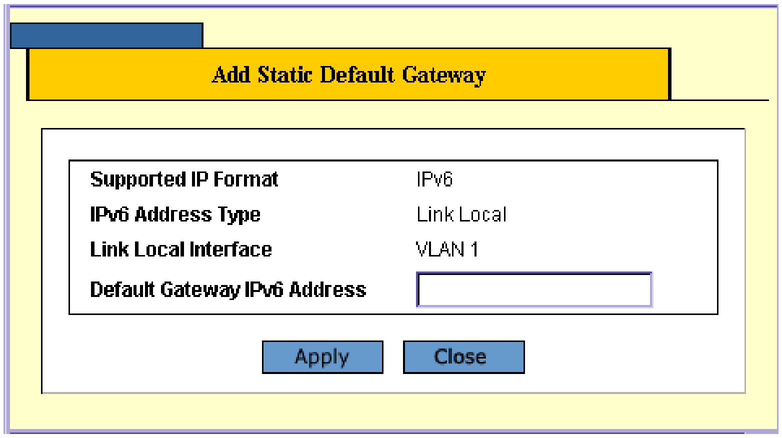
- The radio button is selected to delete/add/modify an entry.
- **Default Gateway IPv6 Address** — Displays the Link Local IPv6 address of the default gateway.
- **Interface** — Specifies the outgoing IPv6 interface through which the default gateway can be reached.
- **Type** — Specifies the means by which the default gateway was configured. The possible field values are:
  - *Static* — Indicates the default gateway is user-defined.

- *Dynamic* — Indicates the default gateway is dynamically configured.

- **State** — Displays the default gateway status. The following states are available: *Incomplete*, *Reachable*, *Stale*, *Delay*, *Probe* and *Unreachable*.

2. Select an Interface.
3. Click **Add**. The *Add Static Default Gateway Page* opens.

Figure 12: Add Static Default Gateway Page



Add Static Default Gateway

Supported IP Format	IPv6
IPv6 Address Type	Link Local
Link Local Interface	VLAN 1
Default Gateway IPv6 Address	

4. Define the **Default Gateway IPv6 Address** field for the IP Interface. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons. An example of an IPv6 address is 2031:0:130F:0:0:9C0:876A:130D and the compressed version is represented as 2031:0:130F::9C0:876A:130D.
5. Click **Apply**. The default gateway is defined, and the device is updated.

Configuring Tunnels

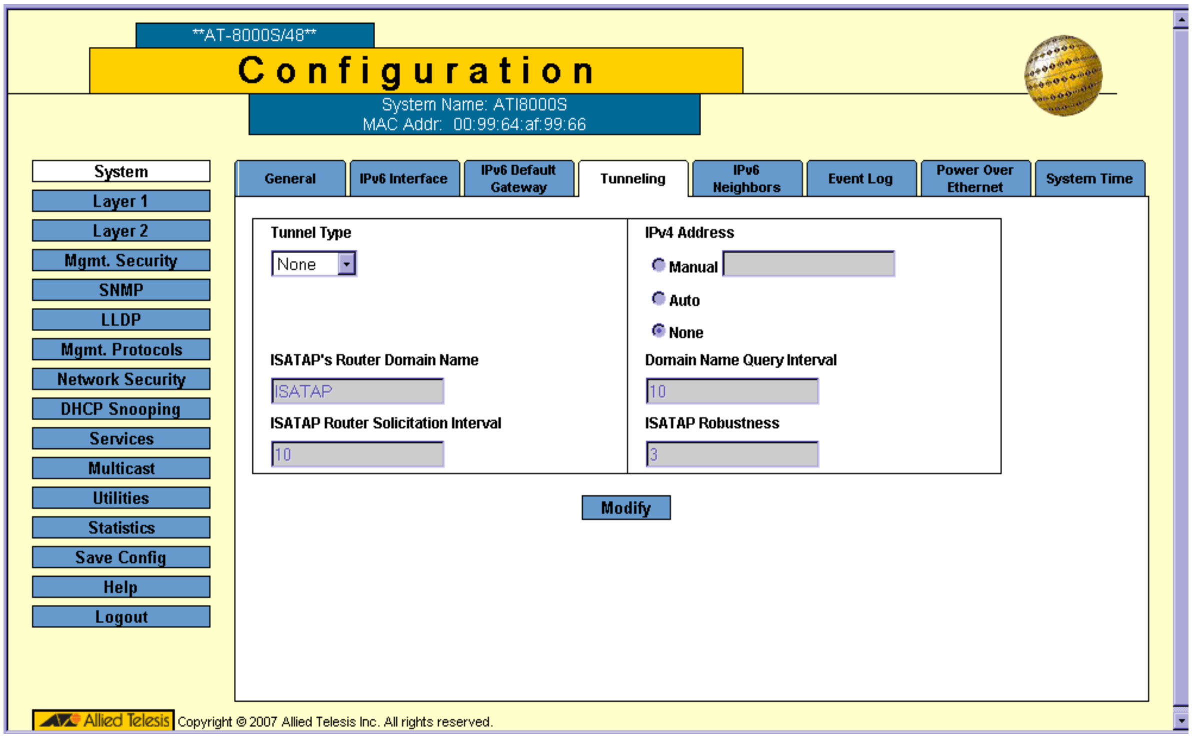
The *Tunneling Page* defines the tunneling process on the device, which encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 network.

The *Intra-Site Automatic Tunnel Addressing Protocol* (ISATAP) address assignment and automatic tunneling mechanism is used for Unicast communication between IPv6/IPv4 nodes in an IPv4 intranet.

To define Tunneling:

1. Click **System > Tunneling**. The *Tunneling Page* opens.

Figure 13: Tunneling Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Tunnel Type: None

IPv4 Address: ○ Manual ○ Auto ● None

ISATAP's Router Domain Name: ISATAP

Domain Name Query Interval: 10

ISATAP Router Solicitation Interval: 10

ISATAP Robustness: 3

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Tunneling Page* contains the following fields:

- **Tunnel Type** — Indicates the tunnel type. The possible field values are:
  - *ISATAP* — Indicates ISATAP is the selected tunnel type.
  - *None* — IPv6 transition mechanism is not used. This is the default value.
- **IPv4 Address** — Specifies the source IPv4 address of a tunnel interface. The possible field values are:
  - *Manual* — Specifies the IPv4 address to be used as the source address for packets sent on the tunnel interface.
  - *Auto* — The system minimum IPv4 address is used as the source address for packets sent on the tunnel interface.

  - *None* — Indicates that the tunnel local address is not set.
- **ISATAP's Router Domain Name** — Specifies a global string that represents a specific automatic tunnel router domain name. The default value is ISATAP.
- **Domain Name Query Interval** (10-3600) — Specifies the interval between DNS Queries (before the IP address of the ISATAP router is known) for the automatic tunnel router domain name. The range is 10 - 3600 seconds. The default is 10 seconds.
- **ISATAP Router Solicitation Interval** (10-3600) — Specifies the interval between router solicitations messages when there is no active router. The range is 10 - 3600 seconds. The default is 10.
- **ISATAP Robustness** (1-20) — Specifies the number of DNS Query/ Router Solicitation refresh messages that the device sends. The range is 1 - 20 seconds. The default is 3.

2. Click **Apply**. The Tunnel is defined, and the device is updated.

Defining IPv6 Neighbors

The *IPv6 Neighbors Page* contains information for defining IPv6 Neighbors which is similar to the functionality of the IPv4 Address Resolution Protocol (ARP). IPv6 Neighbors enables detecting Link Local addresses within the same subnet, and includes a database for maintaining reachability information about the active neighbors paths.

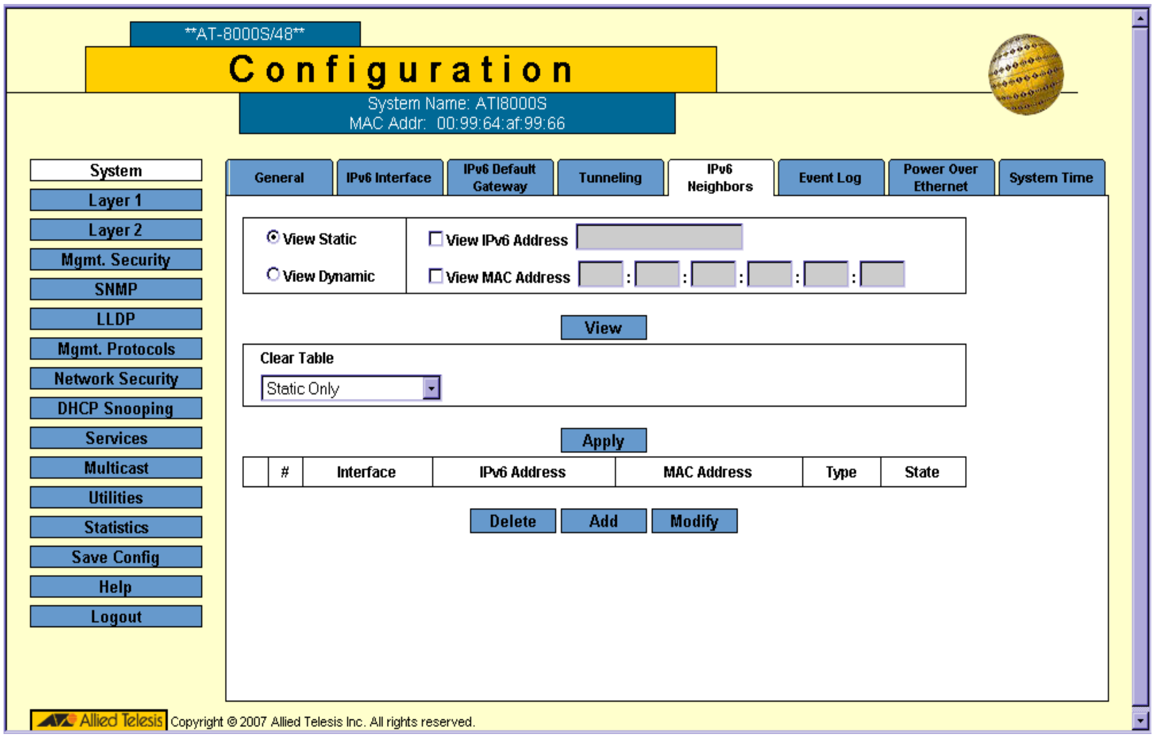
The device supports a total of up to 256 neighbors obtained either statically or dynamically.

When removing an IP interface, all neighbors learned statically and dynamically are removed.

To define IPv6 Neighbors:

1. Click **System > IPv6 Neighbors**. The *IPv6 Neighbors Page* opens.

Figure 14: IPv6 Neighbors Page



AT-8000S/48

Configuration

System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

● View Static
○ View Dynamic

□ View IPv6 Address
□ View MAC Address : : : : :

Clear Table
Static Only

	#	Interface	IPv6 Address	MAC Address	Type	State

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *IPv6 Neighbors Page* contains the following fields:

View IPv6 Neighbors

- **View Static** — Displays the static IPv6 address entries from the IPv6 Neighbor Table.
- **View Dynamic** — Displays the dynamic IPv6 address entries from the IPv6 Neighbor Table.
- **View IPv6 Address** — Displays the currently configured neighbor IPv6 address entries from the IPv6 Neighbor Table. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.
- **View MAC Address** — Displays the MAC address mapped to the IPv6 address.

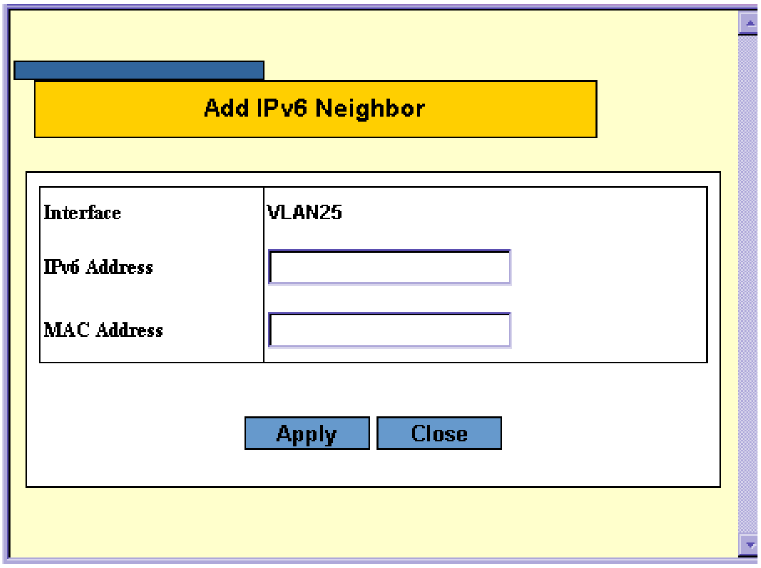
IPv6 Neighbors

- **Clear Table** — Deletes the entries in the IPv6 Neighbor Table. The possible field values are:
  - *Static Only* — Deletes the static IPv6 address entries from the IPv6 Neighbor Table.
  - *Dynamic Only* — Deletes the dynamic IPv6 address entries from the IPv6 Neighbor Table.
  - *All Dynamic and Static* — Deletes the IPv6 Neighbor Table static and dynamic address entries.
- The radio button is selected to delete/add/modify an entry.
- **Interface** — Displays the interface (VLAN) on which the IPv6 interface is configured.
- **IPv6 Address** — Defines the currently configured neighbor IPv6 address. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.
- **MAC Address** — Displays the MAC address mapped to the IPv6 address.
- **Type** — Displays the type of the neighbor discovery cache information entry. The possible field values are:
  - *Static* — Shows static neighbor discovery cache entries.
  - *Dynamic* — Shows dynamic neighbor discovery cache entries.
- **State** — Displays the IPv6 Neighbor status. The following states are available: *Incomplete*, *Reachable*, *Stale*, *Delay* and *Probe*.

2. Select an interface.

3. Click **Add**. The *Add IPv6 Neighbor Page* opens.

Figure 15: Add IPv6 Neighbor Page



Add IPv6 Neighbor

Interface	VLAN25
IPv6 Address	
MAC Address	

4. Define the static **IPv6 Address** and **MAC Address** fields.
5. Click **Apply**. The IPv6 Neighbors entry is defined, and the device is updated.

To modify IPv6 Neighbor entries:

1. Click **System > IPv6 Neighbors**. The *IPv6 Neighbors Page* opens.
2. Select the **IPv6 Address** field to be edited.
3. Click **Modify**. The *IPv6 Neighbor Configuration Page* opens.

Notes

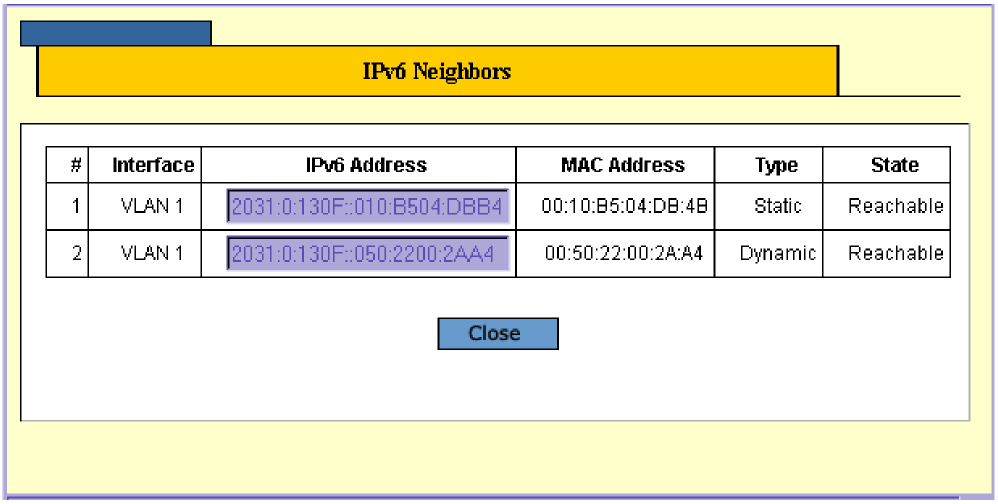
- Static IPv6 addresses require a MAC address whereas dynamic addresses are configured automatically.
- Selecting the Dynamic option in the Type field, disables the fields and prevents reselecting the Static option.

4. Define the **MAC Address** for the static IPv6 address.
5. Click **Apply**. The IPv6 Neighbor entry is modified and the device is defined.

To view IPv6 Neighbor entries:

1. Click **System > IPv6 Neighbors**. The *IPv6 Neighbors Page* opens.
2. Select an interface.
3. Click **View**. The *View IPv6 Neighbors Page* opens.

Figure 16: View IPv6 Neighbors Page



IPv6 Neighbors

#	Interface	IPv6 Address	MAC Address	Type	State
1	VLAN 1	2031:0:130F::010:B504:DBB4	00:10:B5:04:DB:4B	Static	Reachable
2	VLAN 1	2031:0:130F::050:2200:2AA4	00:50:22:00:2A:A4	Dynamic	Reachable

The *View IPv6 Neighbors Page* contains the following fields:

- **Interface** — Displays the interface (VLAN) on which the IPv6 interface is configured.
- **IPv6 Address** — Defines the currently configured neighbor IPv6 address. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.
- **MAC Address** — Displays the MAC address mapped to the IPv6 address.
- **Type** — Displays the type of the neighbor discovery cache information entry. The possible field values are:
  - *Static* — Shows static neighbor discovery cache entries.
  - *Dynamic* — Shows dynamic neighbor discovery cache entries.
- **State** — Displays the IPv6 Neighbor status. The field possible values are:
  - *Incomplete* — Indicates address resolution is in process. The neighbor has not yet responded.
  - *Reachable* — Indicates the neighbor is known to be reachable.
  - *Stale* — Indicates the previously known neighbor is no longer reachable. No action is taken to verify its reachability, until traffic need to be sent.
  - *Delay* — Indicates the previously known neighbor is no longer reachable. The Interface is in Delay state for a predefined Delay Time that if no reachability confirmation is received, the state changes to Probe.
  - *Probe* — Indicates the neighbor is no longer known to be reachable, and Unicast Neighbor Solicitation probes are being sent to verify reachability.

Chapter 4. Configuring System Time

The *System Time Page* provides information for configuring system time parameters, including:

- Setting the System Clock
- Configuring SNTP
- Configuring Daylight Saving Time

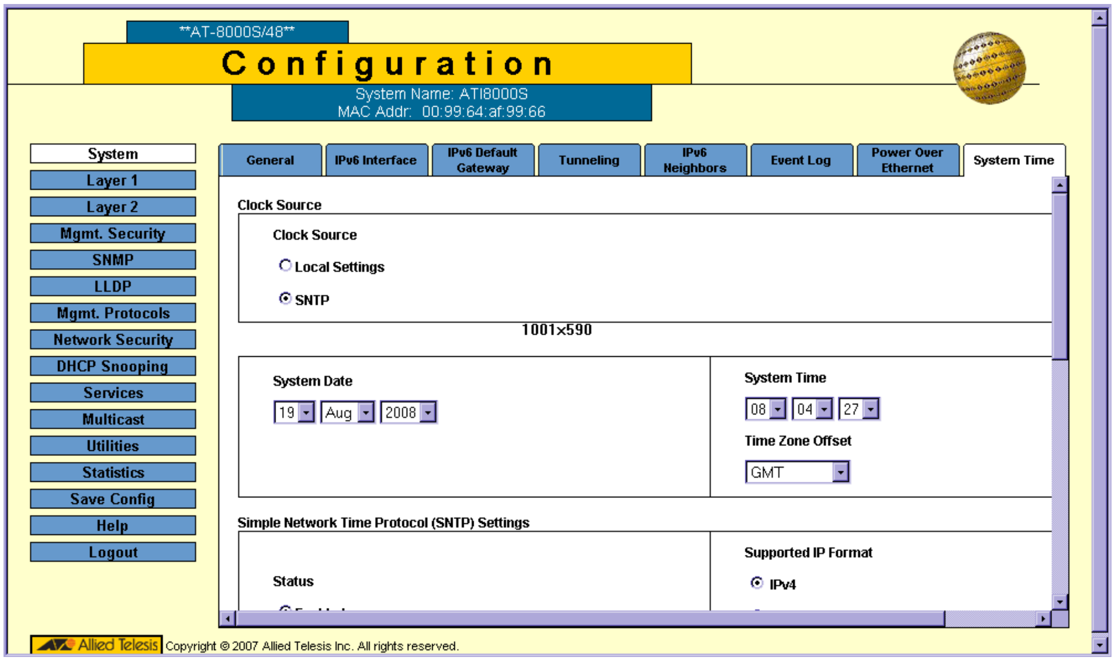
Setting the System Clock

The *System Time Page* contains fields for defining system time parameters for both the local hardware clock and the external SNTP clock. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight Savings Time can be enabled on the device.

To configure the system clock time:

1. Click **System > System Time**. The *System Time Page* opens:

Figure 17: System Time Page



AT-8000S/48

Configuration

System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Clock Source

Clock Source
○ Local Settings
● SNTP

System Date: 19 Aug 2008

System Time: 08 04 27

Time Zone Offset: GMT

Simple Network Time Protocol (SNTP) Settings

Status

Supported IP Format
● IPv4

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Clock Source* and *System Time* sections of the *System Time Page* contain the following fields:

- **Clock Source** — The source used to set the system clock. The possible field values are:
  - *Local Settings* — Indicates that the clock is set locally.

  - *SNTP* — Indicates that the system time is set via an SNTP server.
- **System Time** — Sets the local clock time. The field format is HH:MM:SS. For example: 21:15:03.
- **System Date** — Sets the system date. The field format is Day/Month/Year. For example: 04/May/2050 (May 4, 2050).
- **Time Zone Offset** — The difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT –5.

To set the system clock:

1. Select the system time mode.
2. Define the *System Date*, *System Time and Time Zone Offset* fields.
3. Click **Apply** in each section. The local system clock settings are saved, and the device is updated.
4. Click **Save Config** on the menu to save the changes permanently.

Configuring SNTP

The device supports the *Simple Network Time Protocol* (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client, and cannot provide time services to other systems. The device can poll the following server types for the server time:

- Unicast
- Anycast
- Broadcast

Time sources are established by stratums. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above. The following is an example of stratums:

Stratum 0 — A real time clock (such as a GPS system) is used as the time source.

Stratum 1 — A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.

Stratum 2 — The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Polling for Unicast Time Information

Polling for Unicast information is used for polling a server for which the IP address is known. T1 - T4 are used to determine the server time. This is the preferred method for synchronizing device time.

Polling for Anycast Time Information

Polling for Anycast information is used when the SNTP server IP address is unknown. The first Anycast server to return a response is used to set the time value. Time levels T3 and T4 are used to determine the server time. Using Anycast time information for synchronizing device time is preferred to using Broadcast time information.

Broadcast Time Information

Broadcast information is used when the server IP address is unknown. When a Broadcast message is sent from an SNTP server, the SNTP client listens for the response. The SNTP client neither sends time information requests nor receives responses from the Broadcast server.

Message Digest 5 (MD5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

To define SNTP global parameters:

1. Click **System > System Time**. The *System Time Page* opens.

The *Simple Network Time Protocol* (SNTP) section of the *System Time Page* contains the following fields:

- **Status** — Indicates if SNTP is enabled on the device. The possible field values are:
  - *Disabled* — Indicates that SNTP is disabled.
  - *Enabled* — Indicates that SNTP is enabled.
- **Poll Interval** — Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 1024 seconds.
- **Server IP Address** — Displays a user-defined SNTP server IP address.
- **Supported IP Format** — Indicates the supported Internet Protocol on the device. The possible field values are:
  - *IPv4* — Indicates that IPv4 is supported.
  - *IPv6* — Indicates that IPv6 is supported.
- **IPv6 Address Type** — If IPv6 is selected as a Supported IP Format, the IPv6 address type should be selected. The possible field values are:
  - *Link Local* — Indicates that link local addressing is supported by the interface.
  - *Global* — Indicates that global Unicast addressing is supported by the interface.
- **Link Local Interface** — Indicates the interface type. The possible field values are:
  - *VLAN* — Indicates that VLAN 1 is supported.
  - *Tunnel* — Indicates that ISATAP tunneling (Tunnel 1) mechanism is supported.

2. Select the SNTP *Status, Supported IP Format* and when applicable the *IPv6 Address Type* and *Link Local Interface.*
3. Define the *Server IP Address* and the *Poll Interval* fields.
4. Click **Apply**. The SNTP global settings are defined, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

Configuring Daylight Saving Time

To configure Daylight Saving Time:

1. Click **System > System Time**. The *System Time Page* opens:

The *Additional Time Parameters* section of the *System Time Page* contains the following fields:

- **Daylight Saving** — Enables automatic Daylight Saving Time (DST) on the device based on the device's location. There are two types of daylight settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the *Daylight Savings* area, and for a recurring setting, complete the *Recurring* area. The possible field values are:
  - *USA* — The device changes to DST at 2:00 a.m. on the second Sunday of March, and reverts to standard time at 2:00 a.m. on the first Sunday of November.
  - *European* — The device changes to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The *European* option applies to EU members, and other European countries using the EU standard.

- *Other* — The DST definitions are user-defined based on the device locality. If Custom is selected, the *From* and *To* fields must be defined.

- **Time Set Offset** — Used for non-USA and European countries to set the amount of time for DST (in minutes). The default time is 60 minutes. The range is 1-1440 minutes.
- **From** — Indicates the time that DST begins in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST begins on October 25, 2007 at 5:00 am, the two fields should be set to 25/Oct./07 and 05:00. The possible field values are:
  - *Date* — The date on which DST begins. The possible field range is 1-31.
  - *Month* — The month of the year in which DST begins. The possible field range is Jan.-Dec.
  - *Year* — The year in which the configured DST begins.
  - *Time* — The time at which DST begins. The field format is HH:MM. For example: 05:30.
- **To** — Indicates the time that DST ends in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST ends on March 23, 2008 at midnight, the two fields should be 23/Mar/08 and 00:00. The possible field values are:
  - *Date* — The date on which DST ends. The possible field range is 1-31.
  - *Month* — The month of the year in which DST ends. The possible field range is Jan-Dec.
  - *Year*— The year in which the configured DST ends.
  - *Time* — The time at which DST starts. The field format is HH:MM. For example: 05:30.
- **Recurring** — Enables user-defined DST for countries in which DST is constant from year to year, other than the USA and Europe.
- **From** — The time that DST begins each year. In the example, DST begins locally every first Sunday in April at midnight. The possible field values are:
  - *Day* — The day of the week from which DST begins every year. The possible field range is Sunday-Saturday.
  - *Week* — The week within the month from which DST begins every year. The possible field range is 1-5.
  - *Month* — The month of the year in which DST begins every year. The possible field range is Jan.-Dec.
  - *Time* — The time at which DST begins every year. The field format is Hour:Minute. For example: 02:10.
- **To** — The time that DST ends each year. In the example, DST ends locally every first Sunday in October at midnight. The possible field values are:
  - *Day* — The day of the week at which DST ends every year. The possible field range is Sunday-Saturday.
  - *Week* — The week within the month at which DST ends every year. The possible field range is 1-5.
  - *Month* — The month of the year in which DST ends every year. The possible field range is Jan.-Dec.
  - *Time* — The time at which DST ends every year. The field format is HH:MM. For example: 05:30.

2. To configure the device to automatically switch to DST, select *Daylight Savings* and select either *USA*, *European*, or *Other*. If you select *Other*, you must define its *From* and *To* fields. To configure DST parameters that recur every year, select *Recurring* and define its *From* and *To* fields.
3. Click **Apply**. The DST settings are saved, and the device is updated.
4. Click **Save Config** on the menu to save the changes permanently.

Daylight Savings Time by Country

The following is a list of Daylight Savings Time start and end dates by country:

- **Albania** — From the last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia - Tasmania** — From the beginning of October until the end of March.
- **Armenia** — From the last weekend of March until the last weekend of October.
- **Austria** — From the last weekend of March until the last weekend of October.
- **Bahamas** — From April to October, in conjunction with Daylight Savings Time in the United States.
- **Belarus** — From the last weekend of March until the last weekend of October.
- **Belgium** — From the last weekend of March until the last weekend of October.
- **Brazil** — From the third Sunday in October until the third Saturday in March. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast.
- **Chile** — In Easter Island, from March 9 until October 12. In the rest of the country, from the first Sunday in March or after 9th March.
- **China** — China does not use Daylight Saving Time.
- **Canada** — From the first Sunday in April until the last Sunday of October. Daylight Saving Time is usually regulated by provincial and territorial governments. Exceptions may exist in certain municipalities.
- **Cuba** — From the last Sunday of March to the last Sunday of October.
- **Cyprus** — From the last weekend of March until the last weekend of October.
- **Denmark** — From the last weekend of March until the last weekend of October.
- **Egypt** — From the last Friday in April until the last Thursday in September.
- **Estonia** — From the last weekend of March until the last weekend of October.
- **Finland** — From the last weekend of March until the last weekend of October.
- **France** — From the last weekend of March until the last weekend of October.
- **Germany** — From the last weekend of March until the last weekend of October.
- **Greece** — From the last weekend of March until the last weekend of October.
- **Hungary** — From the last weekend of March until the last weekend of October.
- **India** — India does not use Daylight Saving Time.
- **Iran** — From Farvardin 1 until Mehr 1.
- **Iraq** — From April 1 until October 1.
- **Ireland** — From the last weekend of March until the last weekend of October.
- **Israel** — Varies year-to-year.
- **Italy** — From the last weekend of March until the last weekend of October.
- **Japan** — Japan does not use Daylight Saving Time.
- **Jordan** — From the last weekend of March until the last weekend of October.
- **Latvia** — From the last weekend of March until the last weekend of October.
- **Lebanon** — From the last weekend of March until the last weekend of October.
- **Lithuania** — From the last weekend of March until the last weekend of October.
- **Luxembourg** — From the last weekend of March until the last weekend of October.
- **Macedonia** — From the last weekend of March until the last weekend of October.
- **Mexico** — From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.
- **Moldova** — From the last weekend of March until the last weekend of October.
- **Montenegro** — From the last weekend of March until the last weekend of October.
- **Netherlands** — From the last weekend of March until the last weekend of October.

- **New Zealand** — From the first Sunday in October until the first Sunday on or after March 15.
- **Norway** — From the last weekend of March until the last weekend of October.
- **Paraguay** — From April 6 until September 7.
- **Poland** — From the last weekend of March until the last weekend of October.
- **Portugal** — From the last weekend of March until the last weekend of October.
- **Romania** — From the last weekend of March until the last weekend of October.
- **Russia** — From the last weekend of March until the last weekend of October.
- **Serbia** — From the last weekend of March until the last weekend of October.
- **Slovak Republic** - From the last weekend of March until the last weekend of October.
- **South Africa** — South Africa does not use Daylight Saving Time.
- **Spain** — From the last weekend of March until the last weekend of October.
- **Sweden** — From the last weekend of March until the last weekend of October.
- **Switzerland** — From the last weekend of March until the last weekend of October.
- **Syria** — From March 31 until October 30.
- **Taiwan** — Taiwan does not use Daylight Saving Time.
- **Turkey** — From the last weekend of March until the last weekend of October.
- **United Kingdom** — From the last weekend of March until the last weekend of October.
- **United States of America** — From the second Sunday in March at 02:00 to the first Sunday in November at 02:00.

Chapter 5. Configuring Device Security

This section describes setting security parameters for ports, device management methods, users, and servers. This section contains the following topics:

- Configuring Management Security
- Configuring Server Based Authentication
- Configuring Network Security
- Defining Access Control

Configuring Management Security

This section provides information for configuring device management security, device authentication methods, users and passwords.

This section includes the following topics:

- Defining Access Profiles
- Defining Profile Rules
- Defining Authentication Profiles
- Mapping Authentication Profiles

Defining Access Profiles

Access profiles are profiles and rules for accessing the device. Access to management functions can be limited to user groups. User groups are defined for interfaces according to IP addresses or IP subnets. Access profiles contain management methods for accessing and managing the device. The device management methods include:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)

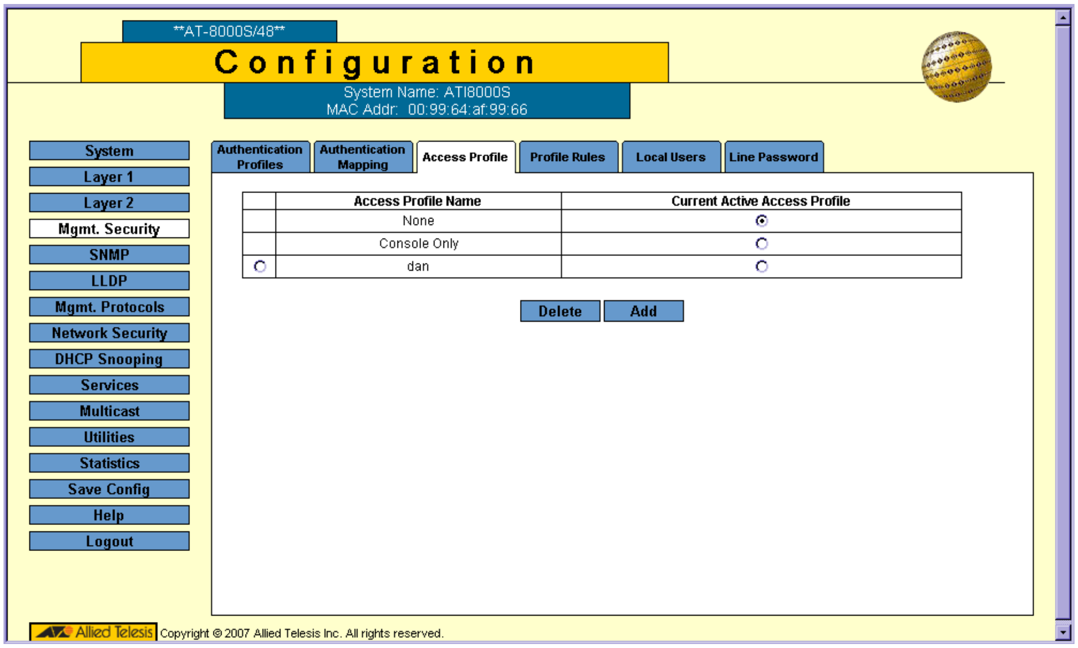
Management access to different management methods may differ between user groups. For example, User Group 1 can access the device module only via an HTTPS session, while User Group 2 can access the device module via both HTTPS and Telnet sessions. The *Access Profile Page* contains the currently configured access profiles and their activity status.

Assigning an access profile to an interface denies access via other interfaces. If an access profile is assigned to any interface, the device can be accessed by all interfaces.

To define access profiles:

1. Click **Mgmt. Security > Access Profile**. The *Access Profile Page* opens:

Figure 18: Access Profile Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

	Access Profile Name	Current Active Access Profile
	None	●
	Console Only	○
○	dan	○

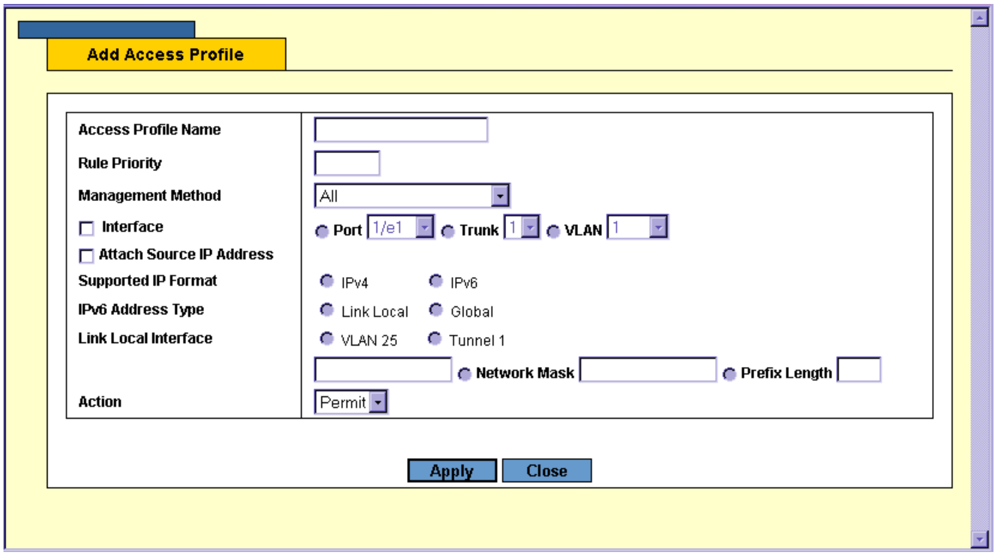
Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Access Profile Page* contains a table listing the currently defined profiles and their active status:

- **Access Profile Name** — The name of the profile. The access profile name can contain up to 32 characters.
- **Current Active Access Profile** — Indicates if the profile is currently active. The possible field values are:
  - *Checked* — The access profile is currently active. Access Profiles cannot be deleted when active.
  - *Unchecked* — Disables the active access profile.

2. Click **Add**. The *Add Access Profile Page* opens:

Figure 19: Add Access Profile Page



Add Access Profile

Access Profile Name	
Rule Priority	
Management Method	All
□ Interface	○ Port 1/e1 ○ Trunk 1 ○ VLAN 1
□ Attach Source IP Address	
Supported IP Format	○ IPv4 ○ IPv6
IPv6 Address Type	○ Link Local ○ Global
Link Local Interface	○ VLAN 25 ○ Tunnel 1
	○ Network Mask ○ Prefix Length
Action	Permit

In addition to the *Access Profile Page*, the *Add Access Profile Page* contains the following fields:

- **Access Profile Name** — Defines the name of a new access profile.
- **Rule Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the *Profile Rules Page*.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet* (SSH) — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - *Secure HTTP* (HTTPS) — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
  - *Port* — Specifies the port on which the access profile is defined.
  - *Trunk* — Specifies the trunk on which the access profile is defined.

- – *VLAN* — Specifies the VLAN on which the access profile is defined.
- **Supported IP Format** — Indicates the supported Internet Protocol on the device. Only IPv6 Global is supported
- **IPv6 Address Type** — Defines the type of configurable static IPv6 IP address for an interface. The possible field values are:
  - *Link Local* — Specifies that link local addressing is supported by the interface.
  - *Global* — Specifies that global Unicast addressing is supported by the interface.
- **Link Local Interface** — Specifies the interface on which IPv6 processing is enabled. The possible field values are:
  - *VLAN 1* — Specifies that VLAN 1 is supported.
  - *None* — Disables IPv6 support on the interface. This option is only available the first time you configure the access profile.
  - *Tunnel 1* — Specifies that ISATAP tunneling (Tunnel 1) mechanism is supported.

Note

You must initially select the *VLAN 1* option to enable IPv6 support on the interface. After doing so, the *VLAN 1* and *Tunnel 1* options are available, but the *None* option is not.

- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork.
  - *Network Mask* — Defines the network mask of the source IP address.
  - *Prefix Length* — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the access rule. The possible field values are:
  - *Permit* — Permits access to the device.
  - *Deny* — Denies access to the device. This is the default.

3. Define the fields.
4. Click **Apply**. The access profile is saved and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

Defining Profile Rules

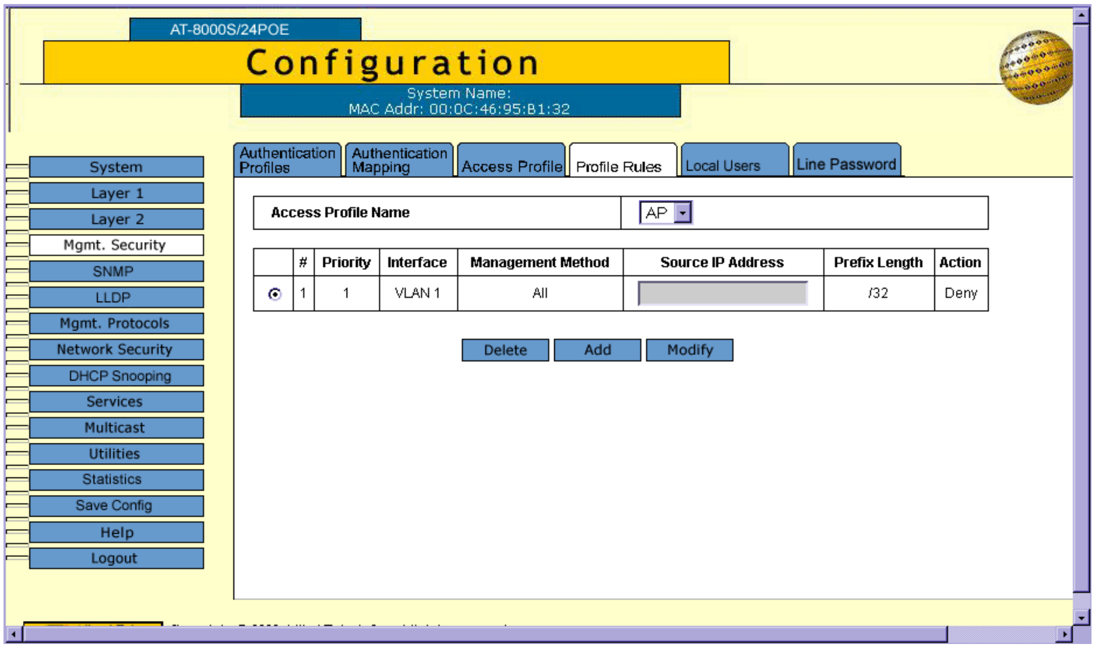
Access profiles can contain up to 128 rules that determine which users can manage the device module, and by which methods. Users can also be blocked from accessing the device. Rules are composed of filters including:

- Rule Priority
- Interface
- Management Method
- IP Address
- Prefix Length
- Forwarding Action

To define profile rules:

1. Click **Mgmt. Security > Profile Rules**: The *Profile Rules Page* opens:

Figure 20: Profile Rules Page



Access Profile Name: AP

	#	Priority	Interface	Management Method	Source IP Address	Prefix Length	Action
◉	1	1	VLAN 1	All		/32	Deny

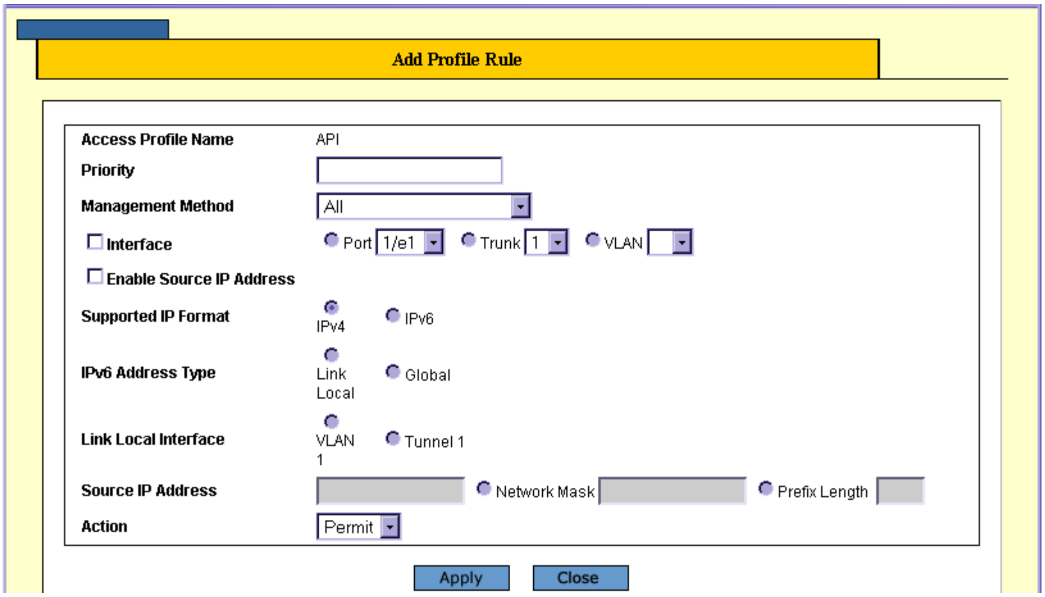
The *Profile Rules Page* contains the following fields:

- **Access Profile Name** — Displays the access profile to which the rule is attached.
- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis.
- **Interface** — Indicates the interface type to which the rule applies. The possible field values are:
  - *Port* — Attaches the rule to the selected port.
  - *Trunk* — Attaches the rule to the selected trunk.
  - *VLAN* — Attaches the rule to the selected VLAN.

- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet* (SSH) — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - *Secure HTTP* (HTTPS) — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- **Source IP Address** — Defines the interface source IP address to which the rule applies.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
  - *Permit* — Permits access to the device.
  - *Deny* — Denies access to the device. This is the default.

2. Click **Add**. The *Add Profile Rule Page* opens:

Figure 21: Add Profile Rule Page



Add Profile Rule

Access Profile Name	API
Priority	
Management Method	All
□ Interface	○ Port 1/e1 ○ Trunk 1 ○ VLAN
□ Enable Source IP Address	
Supported IP Format	● IPv4 ○ IPv6
IPv6 Address Type	○ Link Local ○ Global
Link Local Interface	○ VLAN 1 ○ Tunnel 1
Source IP Address	○ Network Mask ○ Prefix Length
Action	Permit

Profile Rules Page, the *Add Profile Rule Page* contains the following fields:

- **Supported IP Format** — Indicates the supported Internet Protocol on the device. The possible field values are:
  - *IPv4* — Indicates that IPv4 is supported.

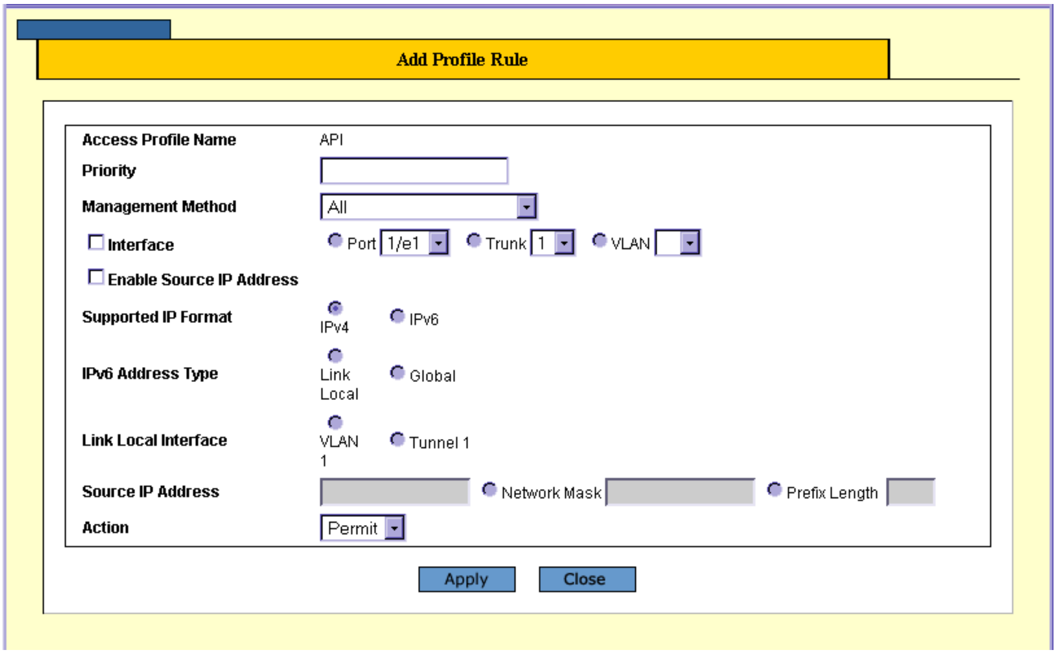
  - *IPv6* — Indicates that IPv6 is supported.
- **IPv6 Address Type** — Defines the type of configurable static IPv6 IP address for an interface. The possible field values are:
  - *Link Local* — Specifies that link local addressing is supported by the interface.
  - *Global* — Specifies that global Unicast addressing is supported by the interface.
- **Link Local Interface** — Specifies the interface on which IPv6 processing is enabled. The possible field values are:
  - *VLAN 1* — Specifies the VLAN ID on which the IPv6 Interface is configured.
  - *Tunnel 1* — Specifies that ISATAP tunneling (Tunnel 1) mechanism is supported.

3. Define the fields.
4. Click **Apply**. The profile rule is added to the access profile, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

To modify an access rule:

1. Click **Mgmt. Security > Profile Rules**: The *Profile Rules Page* opens.
2. Click **Modify**. The *Profiles Rules Configuration Page* opens:

Figure 22: Profiles Rules Configuration Page



Add Profile Rule

Access Profile Name	API
Priority	
Management Method	All
□ Interface	○ Port 1/e1 ○ Trunk 1 ○ VLAN
□ Enable Source IP Address	
Supported IP Format	● IPv4 ○ IPv6
IPv6 Address Type	○ Link Local ○ Global
Link Local Interface	○ VLAN 1 ○ Tunnel 1
Source IP Address	○ Network Mask ○ Prefix Length
Action	Permit

3. Define the fields.
4. Click **Apply**. The profile rule is saved, and the device is updated.

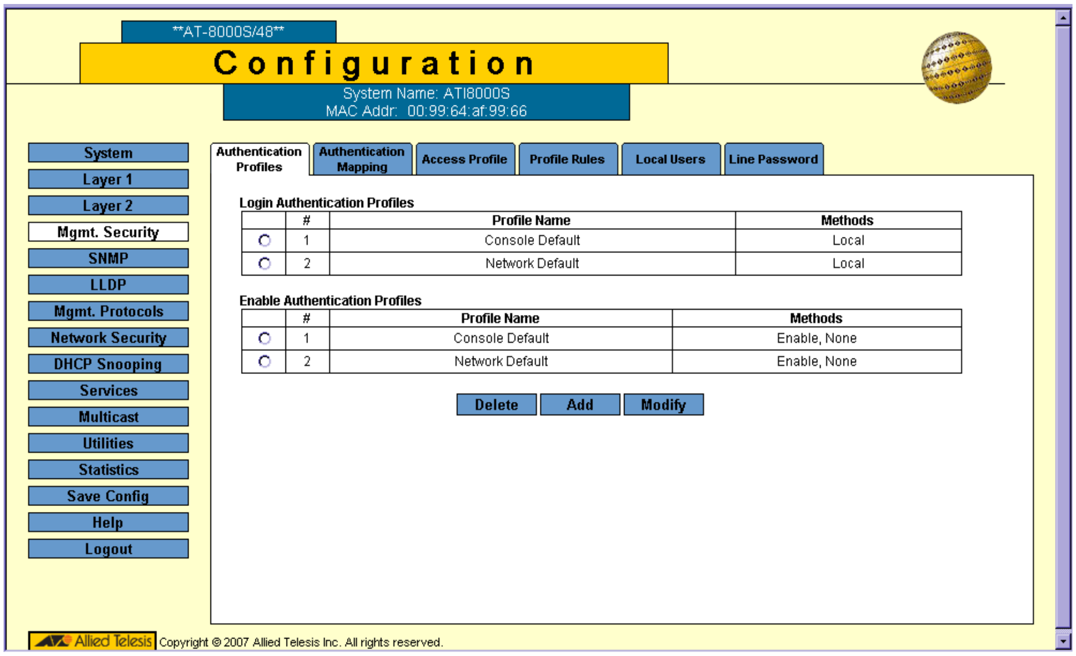
Defining Authentication Profiles

Authentication profiles allow network administrators to assign authentication methods for user authentication. User authentication can be performed either locally or on an external server. User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and the RADIUS server is not available, then the user is authenticated locally.

To define Authentication profiles:

1. Click **Mgmt. Security > Authentication Profiles**. The *Authentication Profiles Page* opens:

Figure 23: Authentication Profiles Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Login Authentication Profiles

	#	Profile Name	Methods
○	1	Console Default	Local
○	2	Network Default	Local

Enable Authentication Profiles

	#	Profile Name	Methods
○	1	Console Default	Enable, None
○	2	Network Default	Enable, None

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Authentication Profiles Page* contains two tables which display the currently defined profiles:

- **Login Authentication Profiles** — Provides the method by which system users logon to the device.
- **Enable Authentication Profiles** — Provides user authentication levels for users accessing the device.

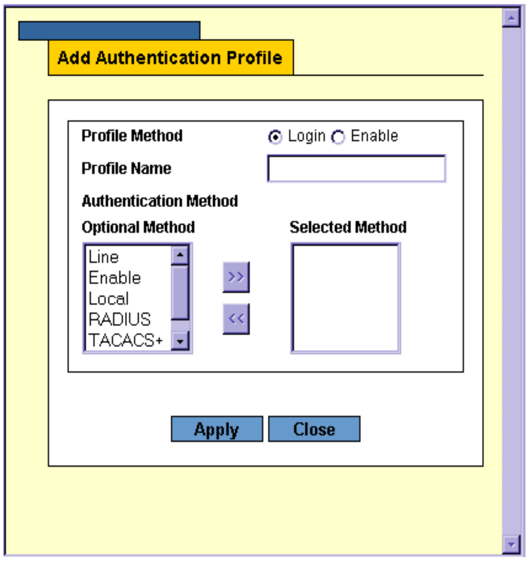
Each table contains the following fields:

- **Profile Name** — Contains a list of user-defined authentication profile lists to which user-defined authentication profiles are added. The default configuration displays as: *Console Default*, and *Network Default*.
- **Methods** — Indicates the authentication method for the selected authentication profile. The possible authentication methods are:
  - *None* — Assigns no authentication method to the authentication profile.
  - *Line* — Indicates that authentication uses a line password.
  - *Enable* — Indicates that authentication uses an Enable password.
  - *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication.

- *RADIUS* — Authenticates the user at the RADIUS server. For more information, see *Defining RADIUS Server Settings*.
- *TACACS+* — Authenticates the user at the TACACS+ server. For more information, see *Defining TACACS+ Host Settings*.
- *Local, RADIUS* — Indicates that authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is blocked.
- *RADIUS, Local* — Indicates that authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.
- *Local, RADIUS, None* — Indicates that authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is permitted.
- *RADIUS, Local, None* — Indicates that Authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.
- *Local, TACACS+* — Indicates that Authentication first occurs locally. If authentication cannot be verified locally, the TACACS+ server authenticates the management method. If the TACACS+ server cannot authenticate the management method, the session is blocked.
- *TACACS+, Local* — Indicates that authentication first occurs at the TACACS+ server. If authentication cannot be verified at the TACACS+ server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.
- *Local, TACACS+, None* — Indicates that authentication first occurs locally. If authentication cannot be verified locally, the TACACS+ server authenticates the management method. If the TACACS+ server cannot authenticate the management method, the session is permitted.
- *TACACS+, Local, None* — Indicates that authentication first occurs at the TACACS+ server. If authentication cannot be verified at the TACACS+ server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.

2. Click **Add**. The *Add Authentication Profile Page* opens:

Figure 24: Add Authentication Profile Page



Profile Method ● Login ○ Enable

Profile Name

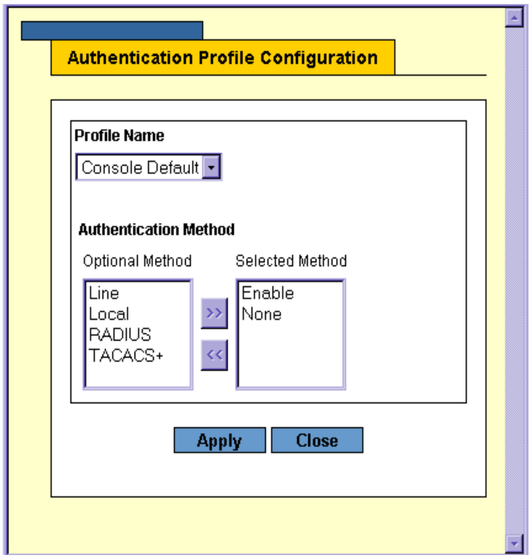
Optional Method: Line, Enable, Local, RADIUS, TACACS+

3. Select the type of function to configure for the profile: *Method* or *Login*.
4. Enter the *Profile Name.*
5. Using the arrows, move the method(s) from the *Optional Method* list to the *Selected Method* list.
6. Click **Apply**. The authentication profile is defined. The profile is added to the profiles table and the device is updated.

To modify the authentication profile settings:

1. Click **Mgmt. Security > Authentication Profiles**. The *Authentication Profiles Page* opens.
2. Click **Modify**. The *Authentication Profile Configuration Page* opens:

Figure 25: Authentication Profile Configuration Page



Authentication Profile Configuration

Profile Name: Console Default

Authentication Method

Optional Method: Line, Local, RADIUS, TACACS+

Selected Method: Enable, None

3. Select the *Profile Name* from the list.
4. Using the arrows, move the method(s) from the *Optional Method* list to the *Selected Method* list.
5. Click **Apply**. The profile settings are saved and the device is updated.

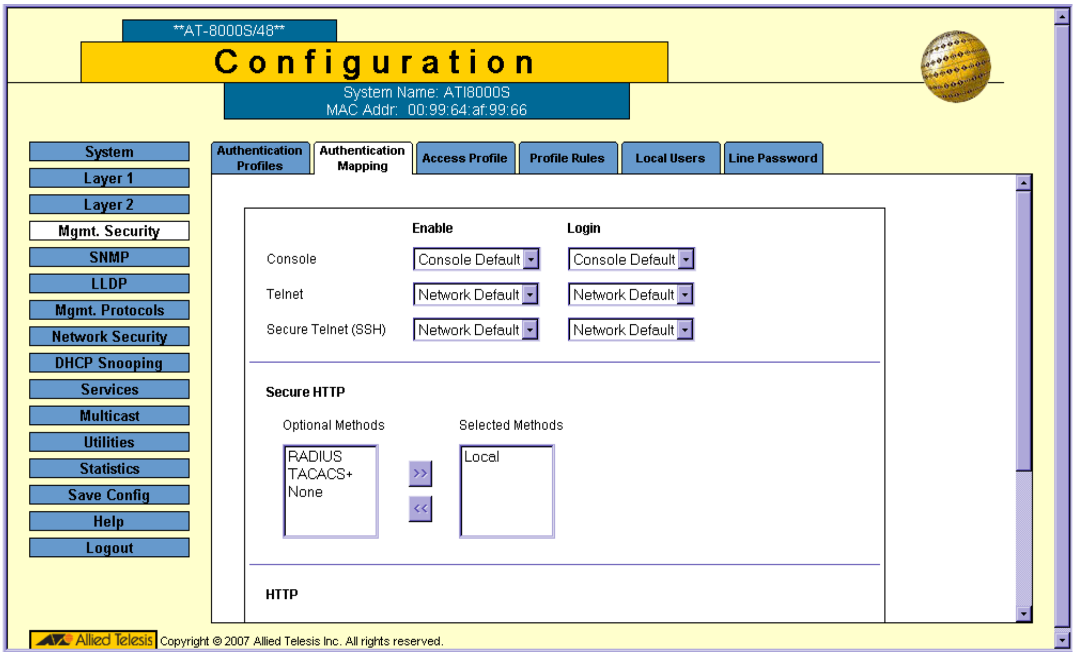
Mapping Authentication Profiles

After authentication profiles are defined, they can be applied to management access methods. For example, console users can be authenticated by Authentication Profile List 1, while Telnet users are authenticated by Authentication Profile List 2. Authentication methods are selected using arrows. The order in which the methods are selected is the order by which the authentication methods are used.

To map authentication methods:

1. Click **Mgmt. Security > Authentication Mapping**. The *Authentication Mapping Page* opens:

Figure 26: Authentication Mapping Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

	Enable	Login
Console	Console Default	Console Default
Telnet	Network Default	Network Default
Secure Telnet (SSH)	Network Default	Network Default

Secure HTTP

Optional Methods	Selected Methods
RADIUS TACACS+ None	Local

HTTP

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Authentication Mapping Page* comprises three sections:

- Authentication Login and Enable
- Secure HTTP
- HTTP

The *Authentication Mapping Page* contains the following fields:

- **Console** — Indicates that authentication profiles are used to authenticate console users.
- **Telnet** — Indicates that authentication profiles are used to authenticate Telnet users.
- **Secure Telnet (SSH)** — Indicates that authentication profiles are used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.

- **Secure HTTP** — Indicates that authentication methods are used for secure HTTP access. The possible methods are:
  - *Local* — Authentication occurs locally.
  - *RADIUS* — Authenticates the user at the RADIUS server.
  - *TACACS+* — Authenticates the user at the TACACS+ server.
  - *None* — Indicates that no authentication method is used for access.
- **HTTP** — Indicates that authentication methods are used for HTTP access. Possible methods are:
  - *Local* — Authentication occurs locally.
  - *RADIUS* — Authenticates the user at the RADIUS server.
  - *TACACS+* — Authenticates the user at the TACACS+ server.
  - *None* — Indicates that no authentication method is used for access.

2. Define the *Console*, *Telnet*, and *Secure Telnet (SSH)* fields.
3. Map the authentication method(s) in the *Secure HTTP* selection box using the >> arrow.
4. Map the authentication method(s) in the *HTTP* selection box.
5. Click **Save Config** on the menu to save the changes permanently.

Configuring Server Based Authentication

Network administrators assign authentication methods for user authentication. User authentication can be performed locally, or on an external server. User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used.

This section describes the following configuration methods:

- Configuring TACACS+
- Configuring RADIUS
- Configuring Local Users
- Defining Line Passwords

Configuring TACACS+

Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation. The system supports up-to 8 TACACS+ servers. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

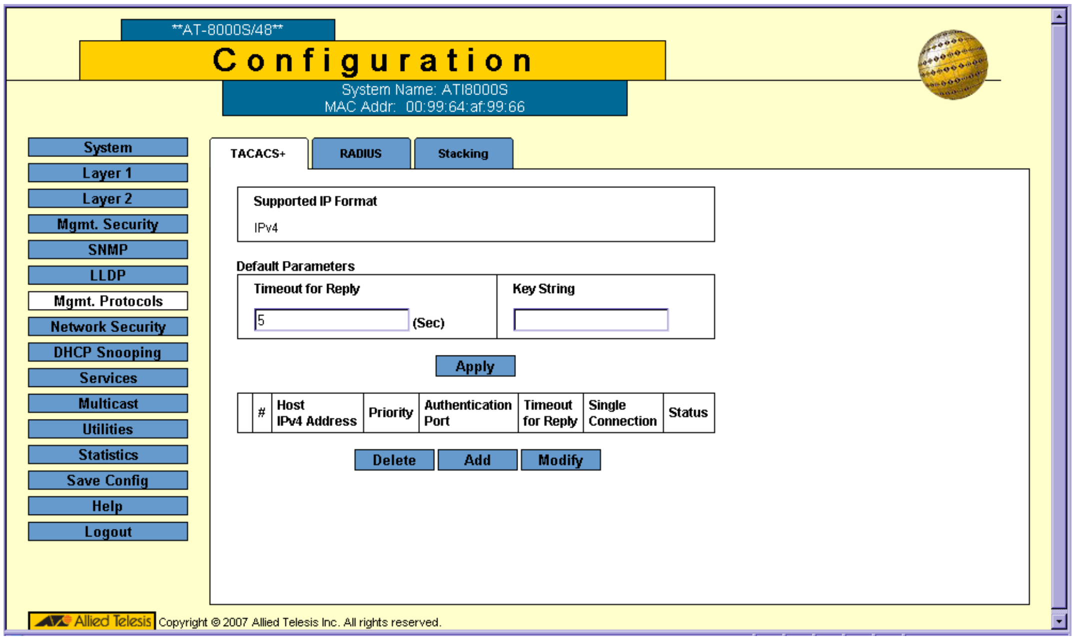
- **Authentication** — Performed at login and via user names and user-defined passwords.
- **Authorization** — Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the client and TACACS+ server.

To define TACACS+ security settings:

1. Click **Mgmt. Protocols > TACACS+**. The *TACACS+ Page* opens.

Figure 27: TACACS+ Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Supported IP Format
IPv4

Default Parameters

Timeout for Reply	Key String
5 (Sec)	

	#	Host IPv4 Address	Priority	Authentication Port	Timeout for Reply	Single Connection	Status

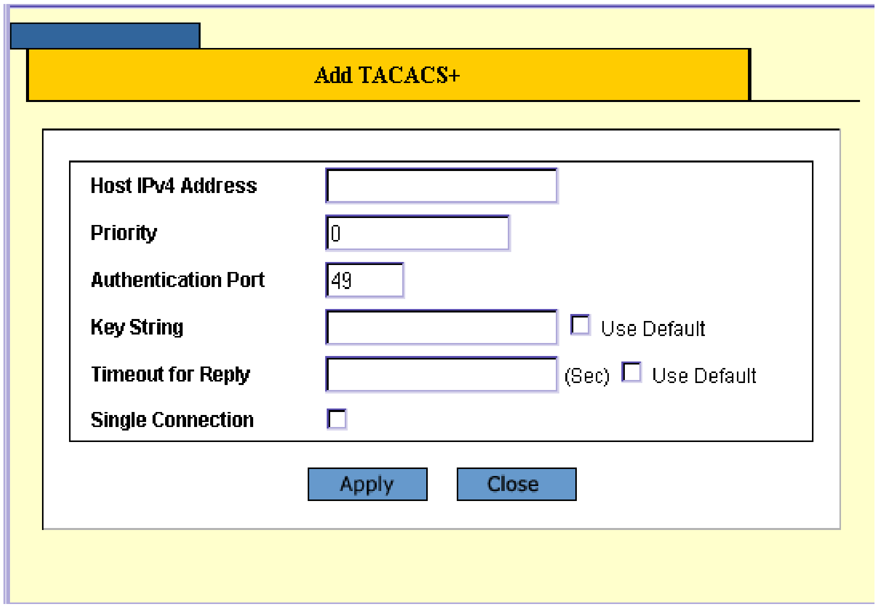
Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *TACACS+ Page* contains the following fields:

- **Supported IP Format** — Indicates that IPv4 is supported.
- **Timeout for Reply** — Defines the time interval, in seconds, that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds and the default is 5 seconds.
- **Key String** — Defines the default key string.
- **Server #** — Displays the server number.
- **Host IPv4 Address** — Displays the TACACS+ server IPv4 address.
- **Priority** — Defines the order in which the TACACS+ servers are used. The field range is 0-65535. The default is 0.
- **Authentication Port** — Identifies the authentication port. The device communicates with the TACACS+ server through the authentication port. The default is 49.
- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server. The possible field values are:
  - *Checked* — Enables a single connection.
  - *Unchecked* — Disables a single connection.
- **Status** — Indicates the connection status between the device and the TACACS+ server. The possible field values are:
  - *Connected* — Indicates there is currently a connection between the device and the TACACS+ server.
  - *Not Connected* — Indicates there is not currently a connection between the device and the TACACS+ server.

2. Click **Add**. The *Add TACACS+ Page* opens.

Figure 28: Add TACACS+ Page



Add TACACS+

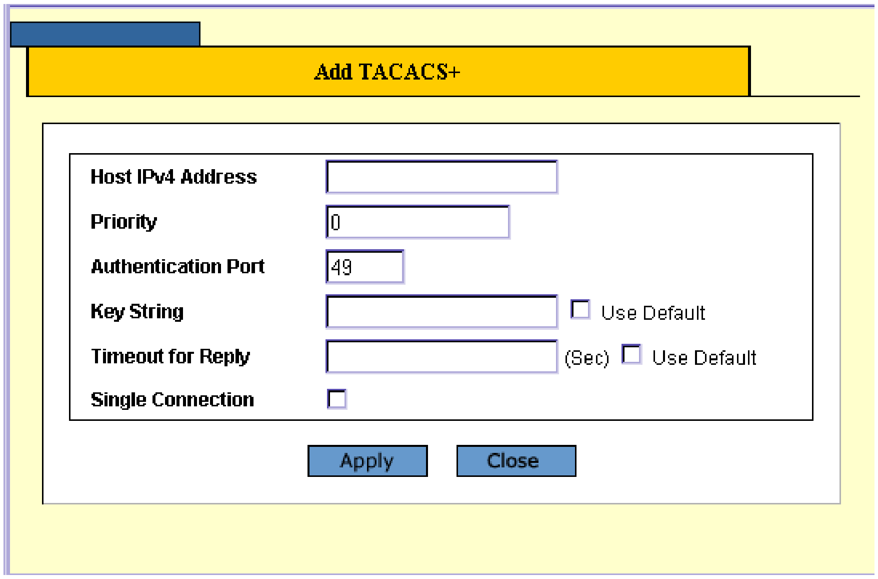
Host IPv4 Address	
Priority	0
Authentication Port	49
Key String	□ Use Default
Timeout for Reply	(Sec) □ Use Default
Single Connection	□

3. Define the fields.
4. Click **Apply**. The TACACS+ profile is saved, and the device is updated.

To modify TACACS+ server settings:

1. Click **Mgmt. Protocols > TACACS+**. The *TACACS+ Page* opens.
2. Click **Modify**. The *TACACS+ Configuration Page* opens:

Figure 29: TACACS+ Configuration Page



Host IPv4 Address	
Priority	0
Authentication Port	49
Key String	□ Use Default
Timeout for Reply	(Sec) □ Use Default
Single Connection	□

3. Define the relevant fields.
4. Click **Apply**. The TACACS+ settings are modified, and the device is updated.

Configuring RADIUS

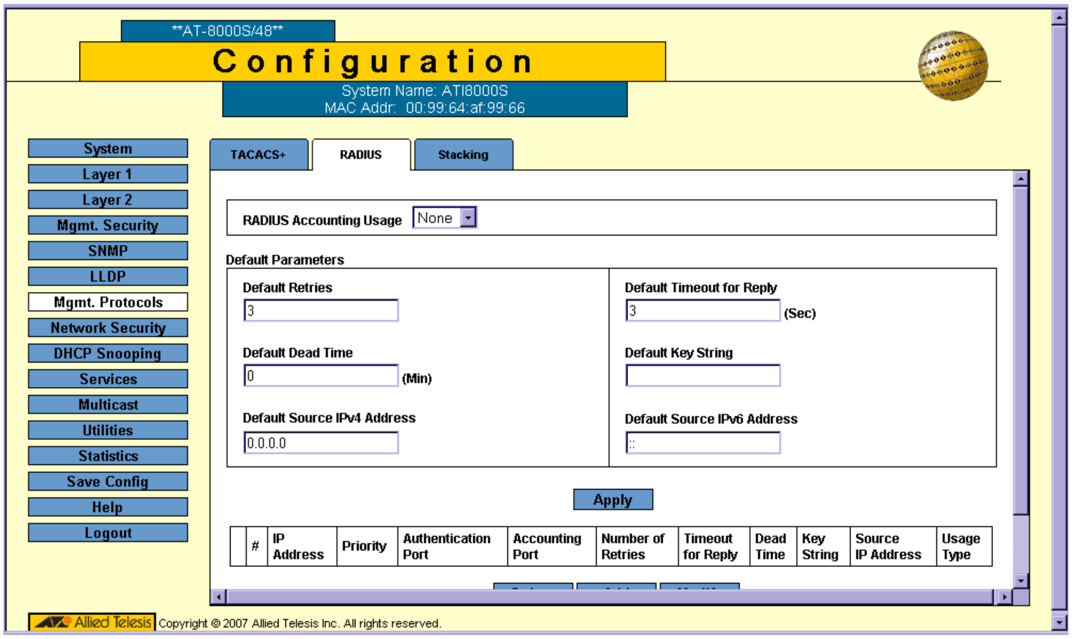
Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for web access.

In addition, RADIUS servers, when activated, record device management sessions on Telnet, serial and WEB and/or 802.1x authentication sessions. The device uses the configured priorities of the available RADIUS servers to select the RADIUS server that holds the accounting information. For IPv6, only *global* IPv6 addressing is supported.

To configure RADIUS security settings:

1. Click **Mgmt. Protocols > RADIUS**. The *RADIUS Page* opens:

Figure 30: RADIUS Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

RADIUS Accounting Usage: None

Default Parameters

Default Retries: 3

Default Timeout for Reply: 3 (Sec)

Default Dead Time: 0 (Min)

Default Key String:

Default Source IPv4 Address: 0.0.0.0

Default Source IPv6 Address: ::

	#	IP Address	Priority	Authentication Port	Accounting Port	Number of Retries	Timeout for Reply	Dead Time	Key String	Source IP Address	Usage Type

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *RADIUS Page* contains the following fields:

- **Radius Accounting Usage** — Specifies the RADIUS recording session type. The default value is *None*. The possible field values are:
  - *802.1X* — Indicates the RADIUS recording session is used for 802.1X authentication.
  - *Login* — Indicates the RADIUS recording session is used for management accounting from login to logout.

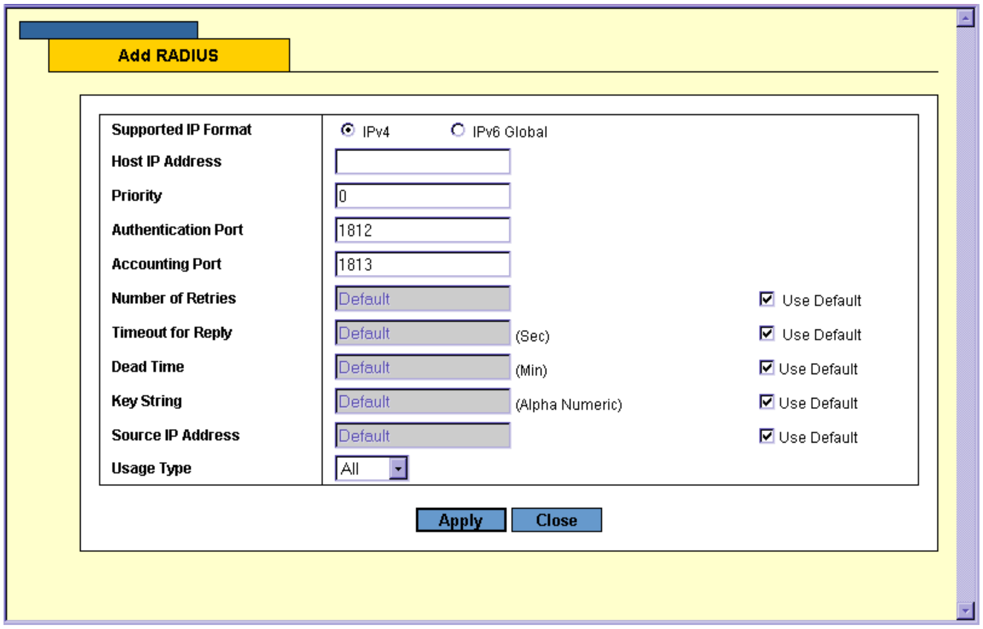
  - *Both* — Indicates the RADIUS recording session is used for 802.1X authentication and management accounting from login to logout.
- **Default Retries** — Defines the default number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are 1-10. The default number of retries is 3.
- **Default Timeout for Reply** — Defines the default time interval in seconds that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds and the default is 5 seconds.
- **Default Dead Time** — Defines the default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000.
- **Default Source IPv4 Address** — Defines the default IPv4 address. The default IPv4 addresses are 32 bits.
- **Default Source IPv6 Address** — Defines the default IPv6 address. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons.
- **Default Key String** — Defines the default key string used for authenticating and encrypting all RADIUS-communications between the device and the RADIUS server. This key must match the RADIUS encryption.

The RADIUS table lists known RADIUS servers and contains the following fields:

- **#** — Displays the RADIUS server number.
- **IP Address** — Displays the RADIUS server IP address.
- **Priority** — Displays the RADIUS server priority. The possible values are 1-65535, where 1 is the highest value. The RADIUS server priority is used to configure the server query order.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **Accounting Port** — Identifies the accounting port. The accounting port is used to verify the RADIUS server recording session. The accounting port default is 1813.
- **Number of Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are 1-10.
- **Timeout for Reply** — Defines the time interval in seconds that passes before the connection between the device and the RADIUS server times out. The field range is 1-30 seconds and the default is 3 seconds.
- **Dead Time** — Defines the amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default is 0 minutes.
- **Source IP Address** — Displays the default IP address of a device accessing the RADIUS server.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is *All*. The possible field values are:
  - *Log in* — Indicates the RADIUS server is used for authenticating user name and passwords.
  - *802.1X* — Indicates the RADIUS server is used for 802.1X authentication.
  - *All* — Indicates the RADIUS server is used for authenticating user names and passwords, and 802.1X port authentication.

2. Click **Add**. The *Add RADIUS Page* opens.

Figure 31: Add RADIUS Page



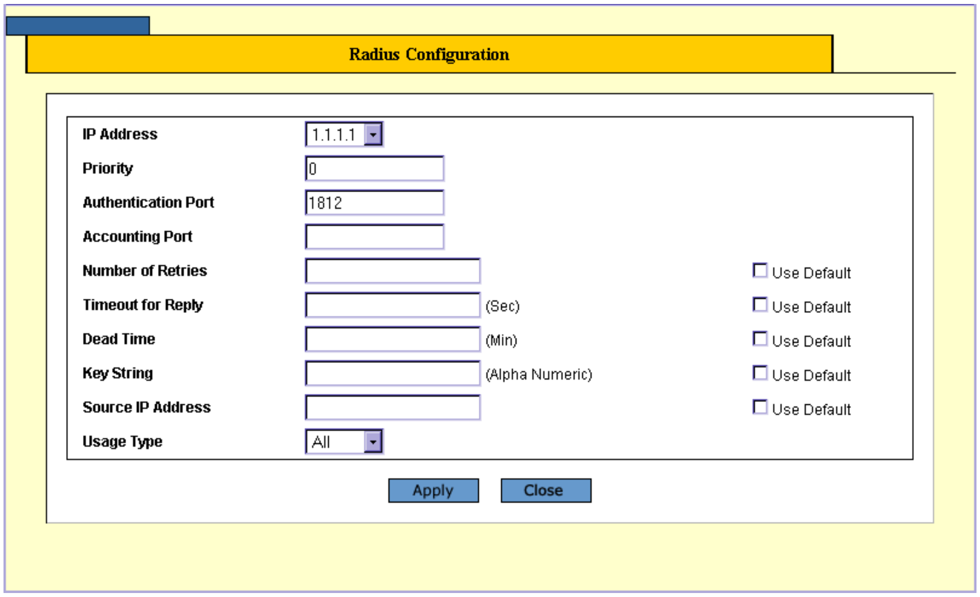
Supported IP Format	● IPv4 ○ IPv6 Global		
Host IP Address			
Priority	0		
Authentication Port	1812		
Accounting Port	1813		
Number of Retries	Default		☑ Use Default
Timeout for Reply	Default	(Sec)	☑ Use Default
Dead Time	Default	(Min)	☑ Use Default
Key String	Default	(Alpha Numeric)	☑ Use Default
Source IP Address	Default		☑ Use Default
Usage Type	All		

3. Define the fields.
4. Click **Apply**. The RADIUS profile is saved, and the device is updated.

To modify RADIUS server settings:

1. Click **Mgmt. Protocols > RADIUS**. The *RADIUS Page* opens:
2. Click **Modify**. The *RADIUS Configuration Page* opens:

Figure 32: RADIUS Configuration Page



Radius Configuration

IP Address	1.1.1.1 ▾		
Priority	0		
Authentication Port	1812		
Accounting Port			
Number of Retries			□ Use Default
Timeout for Reply		(Sec)	□ Use Default
Dead Time		(Min)	□ Use Default
Key String		(Alpha Numeric)	□ Use Default
Source IP Address			□ Use Default
Usage Type	All ▾		

3. Define the relevant fields.
4. Click **Apply**. The RADIUS server settings are modified, and the device is updated.

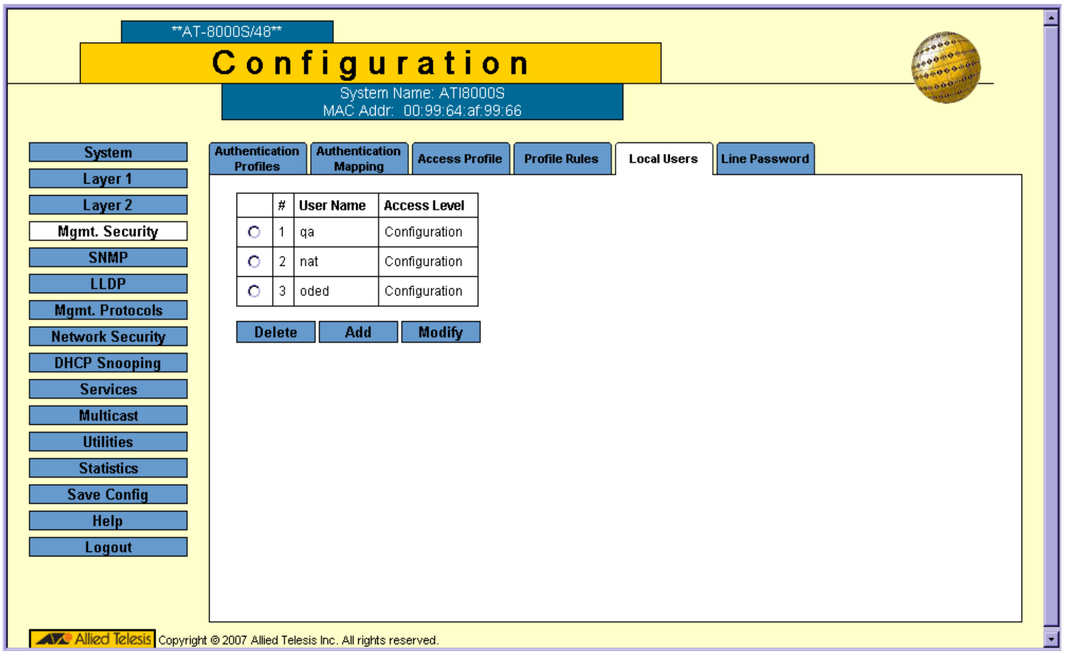
Configuring Local Users

Network administrators can define users, passwords, and access levels for users using the *Local Users Page*.

To configure local users and passwords:

1. Click **Mgmt. Security > Local Users**. The *Local Users Page* opens:

Figure 33: Local Users Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

	#	User Name	Access Level
○	1	qa	Configuration
○	2	nat	Configuration
○	3	oded	Configuration

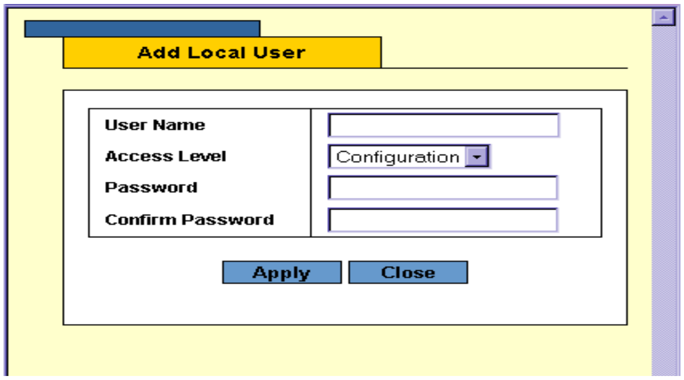
Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Local Users Page* displays the list of currently defined local users and contains the following fields:

- **User Name** — Displays the user's name.
- **Access Level** — Displays the user access level. The lowest user access level is 1 and the highest is 15. Users assigned access level 15 have read/write access to the device. Users assigned an access level of 1 have read-only access. The possible field values are:
  - *Configuration* — Provides Read/Write privileges (level 15).
  - *Monitoring* — Provides Read privileges (level 1).

2. Click **Create**. The *Add Local User Page* opens:

Figure 34: Add Local User Page



User Name
Access Level: Configuration
Password
Confirm Password

In addition to the fields in the *Local Users Page*, the *Add Local User Page* contains the following fields:

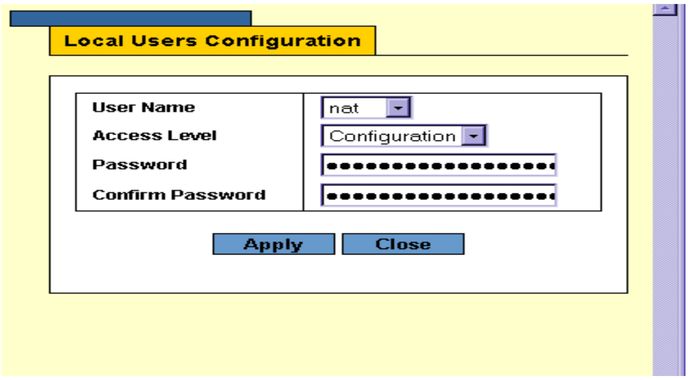
- **Password** — Defines the local user password. Local user passwords can contain up to 159 characters.
- **Confirm Password** — Verifies the password.

3. Define the fields.
4. Click **Apply**. The user is added to the Local Users table and the device is updated.

To modify local users:

1. Click **Mgmt. Security > Local Users**. The *Local Users Page* opens.
2. Click **Modify**. The *Local Users Configuration Page* opens:

Figure 35: Local Users Configuration Page



User Name: nat
Access Level: Configuration
Password: ••••••••••••••••••
Confirm Password: ••••••••••••••••••

3. Define the *User Name*, *Access Level*, *Password*, and *Confirm Password* fields.
4. Click **Apply**. The local user settings are defined, and the device is updated.

Defining Line Passwords

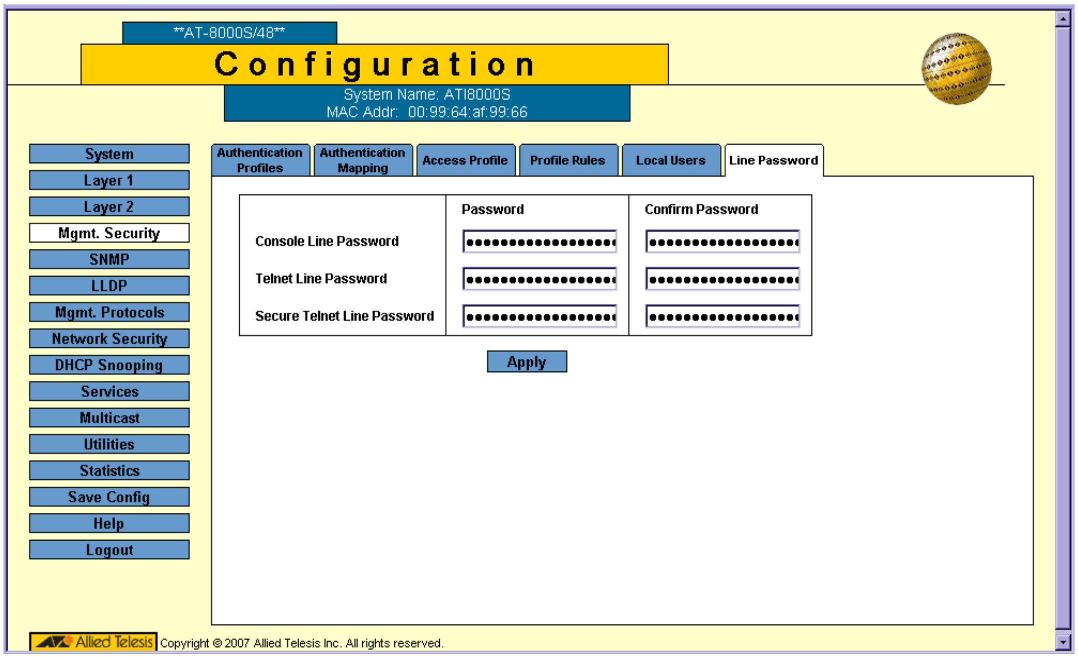
Network administrators can define line passwords in the *Line Password Page*. The administrator enters the new password in the **Password** column and then confirms it in the **Confirm Password** column. After the line password is defined, a management method is assigned to the password. The device can be accessed using the following methods:

- Console
- Telnet
- Secure Telnet

To define line passwords:

1. Click **Mgmt. Security > Line Password**. The *Line Password Page* opens:

Figure 36: Line Password Page



	Password	Confirm Password
Console Line Password	••••••••••••••••••	••••••••••••••••••
Telnet Line Password	••••••••••••••••••	••••••••••••••••••
Secure Telnet Line Password	••••••••••••••••••	••••••••••••••••••

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Line Password Page* contains the following fields:

- **Console Line Password** — Defines the line password for accessing the device via a Console session. Passwords can contain a maximum of 159 characters.
- **Telnet Line Password** — Defines the line password for accessing the device via a Telnet session. Passwords can contain a maximum of 159 characters.
- **Secure Telnet Line Password** — Defines the line password for accessing the device via a secure Telnet session. Passwords can contain a maximum of 159 characters.

2. Define the *Password* and *Confirm Password* fields for the relevant connection.
3. Click **Apply**. The passwords are modified, and the device is updated.

Configuring Network Security

Network security manages locked ports.

Port-based authentication provides traditional 802.1x support, as well as, Guest VLANs. Guest VLANs limited network access to authorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN is enabled, the port receives limited network access. For example, a network administrator can use Guest VLANs to deny network access via port-based authentication, but grant Internet access to unauthorized users.

This section contains the following topics:

- Managing Port Security
- Defining 802.1x Port Access
- Enabling Storm Control

Managing Port Security

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned or statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is locked. When a packet is received on a locked port, and the packet source MAC address is not tied to that port (either it was learned on a different port, or it is unknown to the system), the protection mechanism is invoked (unless it is statically configured on another port, or was learned/configured on another secured port), and can provide various options. Unauthorized packets arriving at a locked port are handled by one of the following actions:

- Forwarded with or without a trap, but the source address is not learned on the port.
- Discarded with or without a trap.
- The port is shut down with or without a trap.

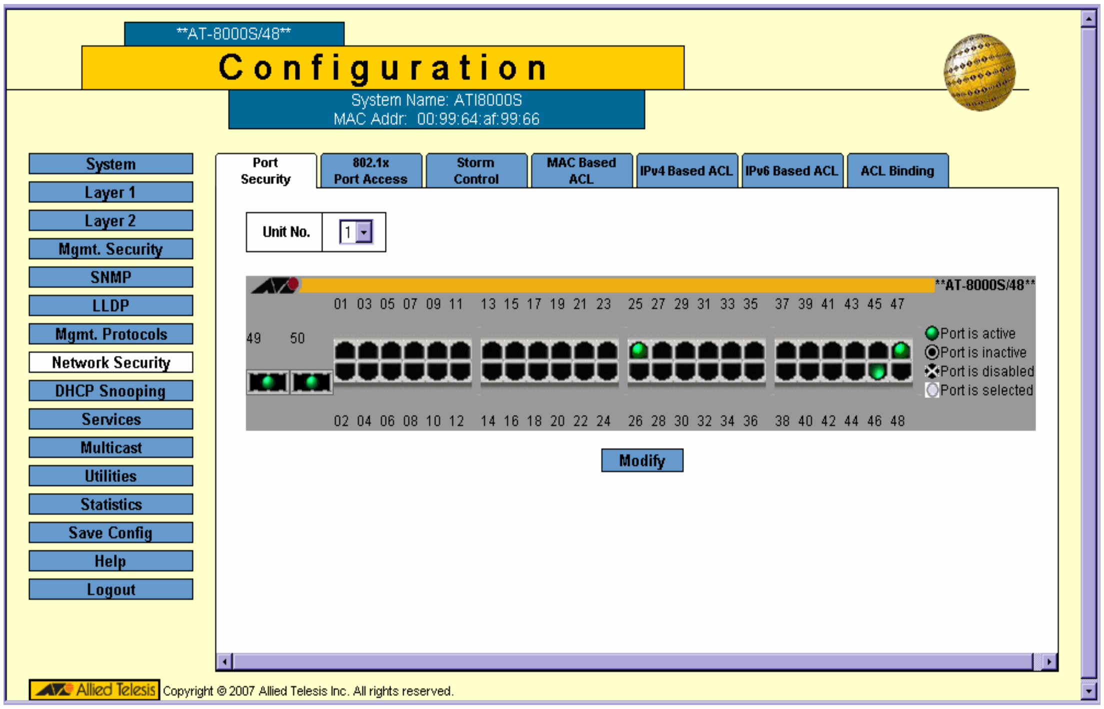
Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset. Disabled ports are activated from the *Port Security Page*.

The *Port Security Page* enhances network security by providing port locking management to network administrators.

To configure secure ports:

1. Click **Network Security > Port Security**. The *Port Security Page* opens:

Figure 37: Port Security Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Unit No. 1

Copyright © 2007 Allied Telesis Inc. All rights reserved.

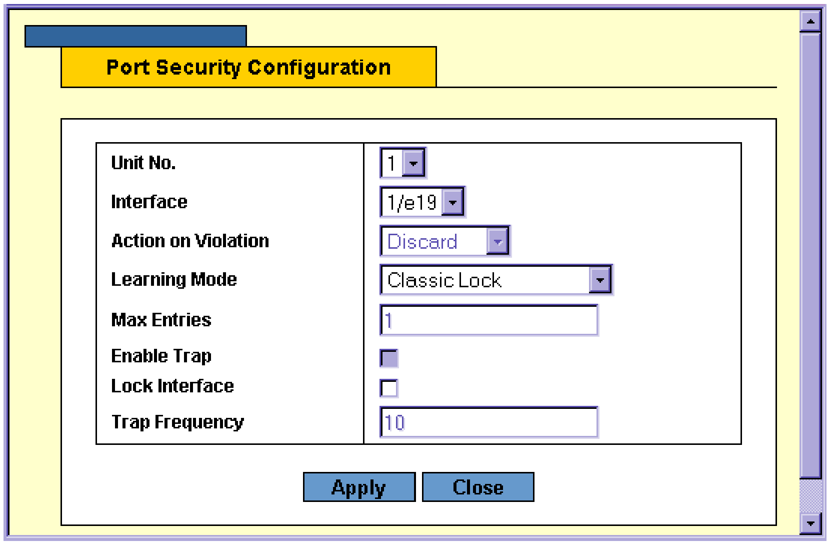
The *Port Security Page* displays the Zoom View of the selected stacking member's (defined in the **Unit No.** field) ports. The possible port indicators are:

- ● *Port is active* — Indicates that the port is linked.
- ◉ *Port is inactive* — Indicates that the port is not linked.
- ✖ *Port is disabled* — Indicates that the port is disabled.
- ○ *Port is selected* — Indicates that the port is selected for modification.

2. In the **Unit No.** field, select the stacking member to display.
3. Select the ports to lock. The port indicator changes to *selected*.

4. Click **Modify**. The *Port Security Configuration Page* opens:

Figure 38: Port Security Configuration Page



Port Security Configuration

Unit No.	1
Interface	1/e19
Action on Violation	Discard
Learning Mode	Classic Lock
Max Entries	1
Enable Trap	☐
Lock Interface	☐
Trap Frequency	10

The *Port Security Configuration Page* contains the following fields:

- **Interface** — Displays the port name.
- **Action On Violation** — Indicates the intruder action defined for the port. Indicates the action to be applied to packets arriving on a locked port. The possible values are:
  - *Forward* — Forwards packets from an unknown source without learning the MAC address.
  - *Discard* — Discards packets from any unlearned source. This is the default value.
  - *Shutdown* — Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Learning Mode** — Defines the locked port type. The possible field values are:
  - *Classic Lock* — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
  - *Limited Dynamic Lock* — Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled. Previously learned MAC addresses are not deleted but are converted to a static MAC address.
- **Max Entries** — Specifies the number of MAC addresses that can be learned on the port before the port is locked. The field range is 1-128. The default is 1.
- **Enable Trap** — Indicates if the SNMP trap generated if there is a violation. The possible values are:
  - *Yes* — Trap is generated.
  - *No* — No trap is generated.
- **Lock Interface** —Locks the interface.
- **Trap Frequency** — The time interval (in seconds) between traps. The possible field range is 1-1,000,000 seconds, and the default is 10 seconds.

5. Select the security mode for the selected port(s).

6. Click **Apply**. The port security settings are saved and the device is updated.
7. Click **Save Config** on the menu to save the changes permanently.

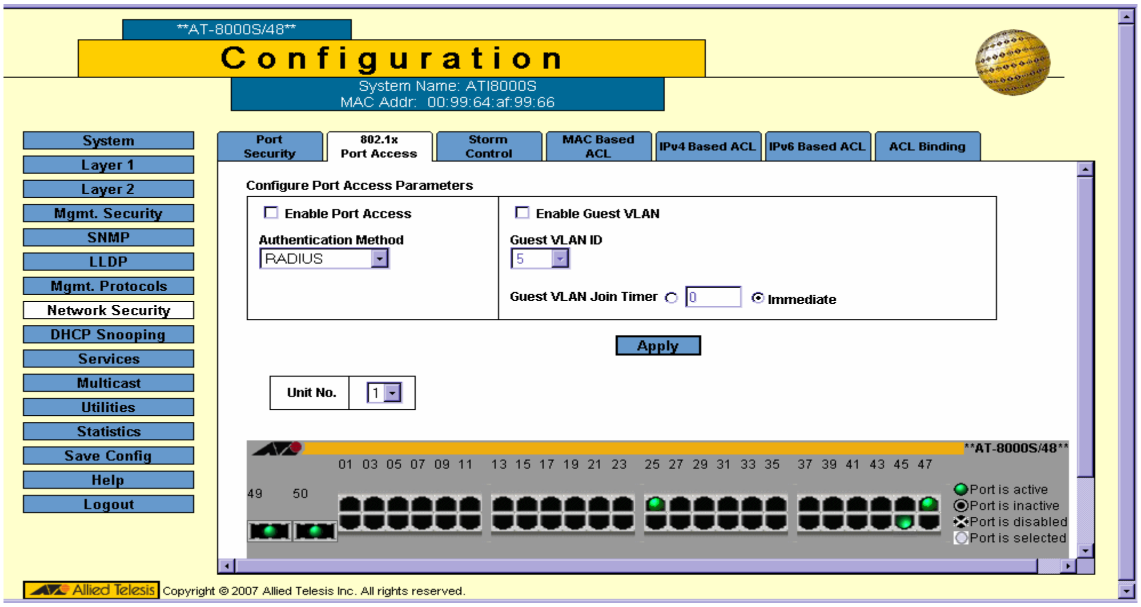
Defining 802.1x Port Access

The *802.1x Port Access Page* allows enabling port access globally, defining the authentication method, and configuration of port roles and settings.

To configure 802.1x port access parameters:

1. Click **Network Security > 802.1x Port Access**. The *802.1x Port Access Page* opens:

Figure 39: 802.1x Port Access Page



Configure Port Access Parameters

☐ Enable Port Access

Authentication Method: RADIUS

☐ Enable Guest VLAN

Guest VLAN ID: 5

Guest VLAN Join Timer ○ 0 ● Immediate

Apply

Unit No. 1

● Port is active
● Port is inactive
● Port is disabled
○ Port is selected

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *802.1x Port Access Page* contains the following fields:

- **Enable Port Access** — Enables the 802.1x port access globally. The possible values are:
  - *Checked* — Enables the 802.1x port access on the device.
  - *Unchecked* — Disables the 802.1x port access on the device. This is the default value.
- **Authentication Method** — Displays the method by which the last session was authenticated. The possible field values are:
  - *None* — Indicates that no authentication method is used to authenticate the port.
  - *RADIUS* — Provides port authentication using the RADIUS server.
  - *RADIUS, None* — Provides port authentication, first using the RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.
- **Enable Guest VLAN** — Provides limited network access to unauthorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN field is enabled, the port receives limited network access.
  For example, a network administrator can use Guest VLANs to deny network access via port-based authentication, but grant Internet access to unauthorized users. The possible field values are:

  - *Enable* — Enables Guest VLAN.
  - *Disable* — Disables Guest VLAN.
- **Guest VLAN ID** — Specifies the VLAN ID assigned to the Guest VLAN.
- **Guest VLAN** — Sets Guest VLAN timers for the device. The possible field values are:
  - *Join Timer* — Enables the join timer. Enter the time period for reauthentication.
  - *Immediate* — Reauthenticates the port immediately.

The *802.1x Port Access Page* also displays the Zoom View of the selected stacking member’s (defined in the **Unit No.** field) ports. The possible port indicators are:

● *Port is active* — Indicates that the port is linked.

◙ *Port is inactive* — Indicates that the port is not linked.

☒ *Port is disabled* — Indicates that the port is disabled.

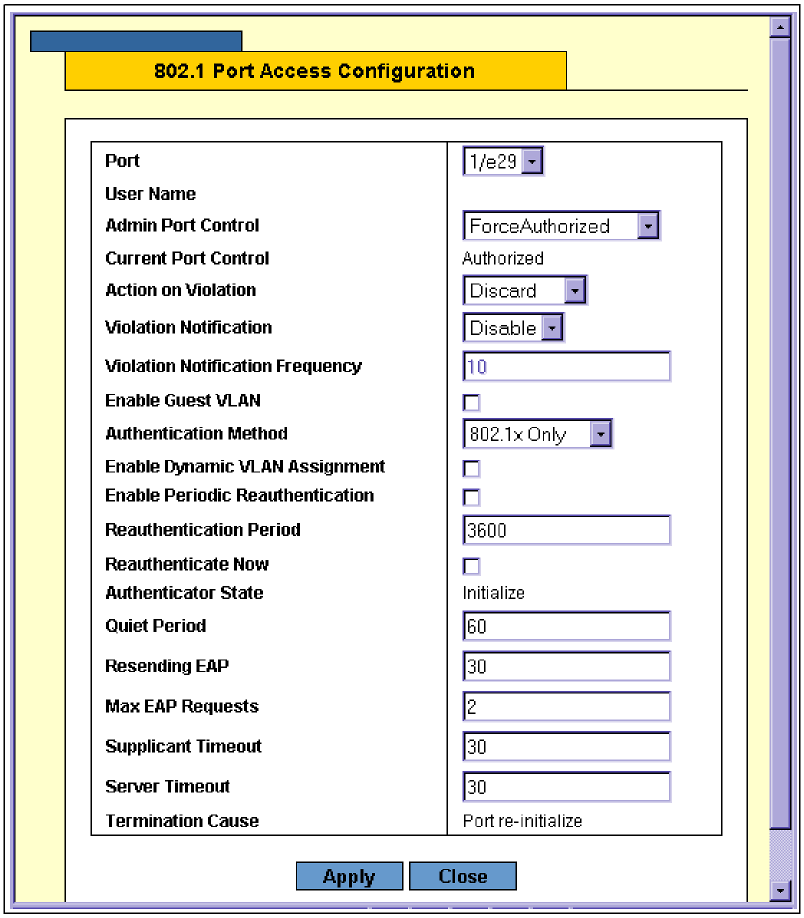
○ *Port is selected* — Indicates that the port is selected for modification.

2. Select **Enable Port Access**.
3. Select the *Authentication Method.*
4. Define the VLAN fields
5. Click **Apply**. The 802.1x access is configured globally and device information is updated.

To modify port based authentication settings:

1. Click **Modify**. The *Port Authentication Settings Page* opens:

Figure 40: Port Authentication Settings Page



802.1 Port Access Configuration

Port	1/e29
User Name	
Admin Port Control	ForceAuthorized
Current Port Control	Authorized
Action on Violation	Discard
Violation Notification	Disable
Violation Notification Frequency	10
Enable Guest VLAN	□
Authentication Method	802.1x Only
Enable Dynamic VLAN Assignment	□
Enable Periodic Reauthentication	□
Reauthentication Period	3600
Reauthenticate Now	□
Authenticator State	Initialize
Quiet Period	60
Resending EAP	30
Max EAP Requests	2
Supplicant Timeout	30
Server Timeout	30
Termination Cause	Port re-initialize

The *Port Authentication Settings Page* contains the following port authentication parameters:

The *Port Authentication Settings Page* contains the following port authentication parameters:

- **Port** — Displays a list of interfaces on which port-based authentication is enabled.
- **User Name** — Displays the supplicant user name.
- **Admin Port Control** — Indicates the port state. The possible field values are:
- **Admin Port Control** — Indicates the port state. The possible field values are:
  - *Auto* —Enables port-based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
  - *ForceAuthorized* — Indicates the interface is in an authorized state without being authenticated. The interface re-sends and receives normal traffic without client port-based authentication.
  - *ForceUnauthorized* — Denies the selected interface system access by moving the interface into unauthorized state. The device cannot provide authentication services to the client through the interface.
- **Current Port Control** — Displays the current port authorization state. The possible field values are:
  - *Authorized* — Indicates the interface is in an authorized state.
  - *Unauthorized* — Denies the selected interface system access.
- **Action on Violation** — Indicates the intruder action defined for the port. Indicates the action to be applied to packets arriving on a locked port. The possible values are: The possible field values are:
  - *Forward* — Enables the forwarding of frames with source addresses that are **not** the supplicant's address, while **not** learning the source addresses.
  - *Discard* — Enables the discarding of frames with source addresses that are **not** the supplicant's address. This is the default value.
  - *Shutdown* — The port is shut down and enables the discarding of frames with source addresses that are not the supplicant's address.
- **Violation Notification** — Indicates if the SNMP trap generated if there is a violation. The possible field values are:
  - *Enable* — A notification is sent.
  - *Disable* — A notification is **not** sent.
- **Violation Notification Frequency** — Enter the frequency to send notifications.
- **Enable Guest VLAN** — Indicates if the Guest VLAN is enabled. The possible field values are:
  - *Checked* — Enables the Guest VLAN.
  - *Unchecked* — Disables the Guest VLAN. This is the default value.
- **Authentication Method** — Defines the user authentication methods. MAC authentication ensures that end-user stations meet security policies criteria, and protects networks from viruses. The possible values are:
  - *802.1X Only* – Enables only 802.1X authentication on the device.
  - *MAC Only* — Enables only MAC authentication on the device.
  - *MAC + 802.1X* – Enables MAC Authentication + 802.1X authentication on the device. In case of MAC+ 802.1x, 802.1x takes precedence.
- **Enable Dynamic VLAN Assignment** — Enables automatically assigning users to VLANs during RADIUS server authentication. When a user is authenticated by the RADIUS server, the user is automatically joined to the VLAN that is defined in the RADIUS server. The VLANs that cannot participate in DVA are:
  - An Unauthenticated VLAN.
  - A Dynamic VLAN that was created by GVRP.
  - A Voice VLAN.
  - A Default VLAN
  - A Guest VLAN:

The possible field values are:

  - *Enable* — Enables dynamic VLAN assignment.
  - *Disable* — Disables dynamic VLAN assignment. This is the default value.
- **Enable Periodic Reauthentication** — Permits port reauthentication. The possible field values are:
  - *Enable* — Enables port reauthentication. This is the default value.
  - *Disable* — Disables port reauthentication.
- **Reauthentication Period** — Displays the time span (in seconds) in which the selected port is reauthenticated. The field default is 3600 seconds.
- **Reauthenticate Now** — Reauthenticates the port immediately.
- **Authenticator State** — Displays the current authenticator state (as defined in Admin Port Control).
- **Quiet Period** — Displays the number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.
- **Resending EAP** — Defines the amount of time (in seconds) that lapses before EAP requests are resent. The field default is 30 seconds.
- **Max EAP Requests** — Displays the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is two retries.
- **Supplicant Timeout** — Displays the amount of time (in seconds) that lapses before EAP requests are resent to the supplicant. The field default is 30 seconds.
- **Server Timeout** — Displays the amount of time (in seconds) that lapses before the device re-sends a request to the authentication server. The field default is 30 seconds.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated.

2. Click **Apply**. The port authentication configuration is saved and the device is updated.
3. Click **Save Config** on the menu to save the changes permanently.

To activate MAC authentication first define the following:

1. Enable Guest VLAN.
2. Set the **Admin Port Control** option to **Auto**.

Enabling Storm Control

Storm control limits the amount Multicast and Broadcast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast, and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes on all ports.

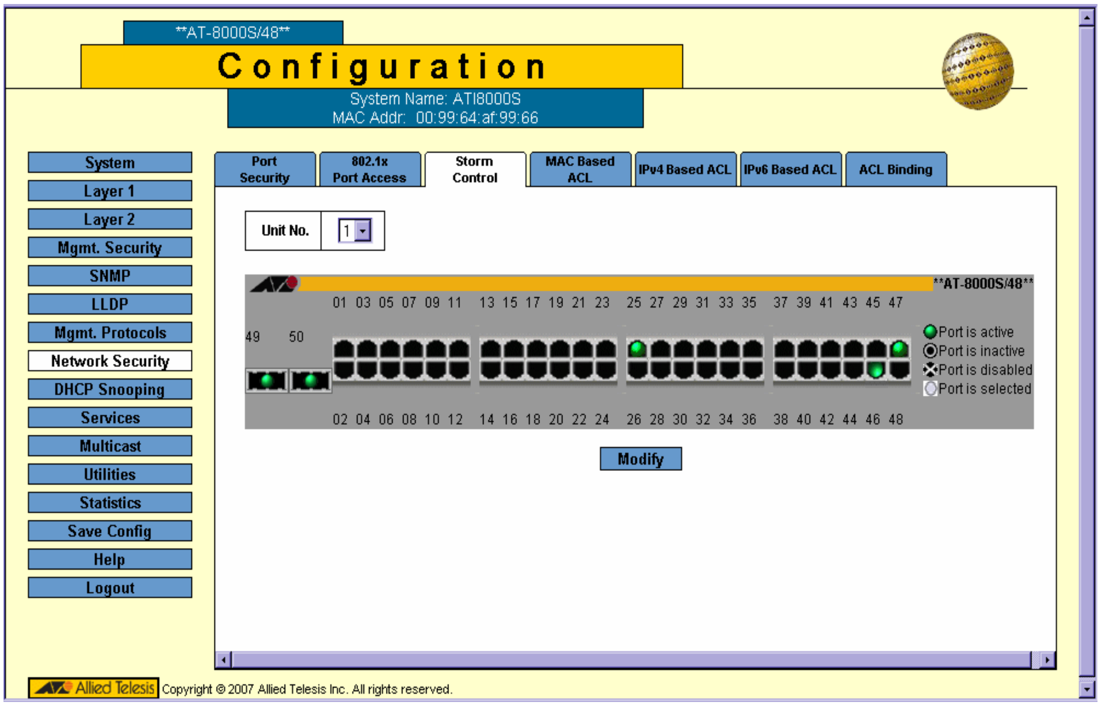
A Broadcast Storm is a result of an excessive amount of Broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

Storm control is enabled for all ports by defining the packet type and the rate the packets are transmitted. The system measures the incoming Broadcast and Multicast frame rates separately on each port, and discards the frames when the rate exceeds a user-defined rate. The *Storm Control Page* provides fields for configuring Broadcast storm control.

To enable storm control:

1. Click **Network Security > Storm Control**. The *Storm Control Page* opens:

Figure 41: Storm Control Page



The *Storm Control Page* displays the Zoom View of the selected stacking member's (defined in the **Unit No.** field) ports. The possible port indicators are:

● *Port is active* — Indicates that the port is linked.

◉ *Port is inactive* — Indicates that the port is not linked.

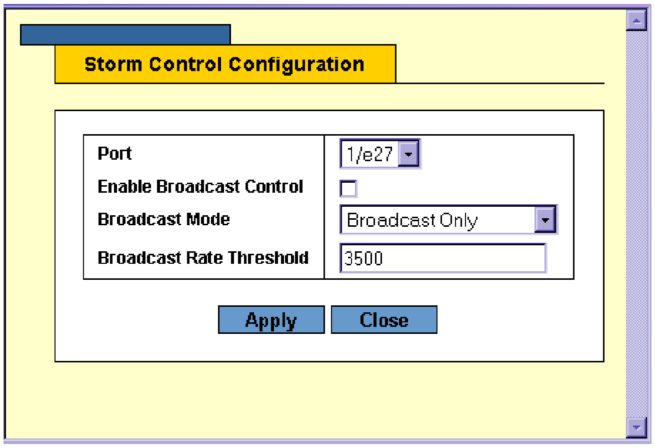
☒ *Port is disabled* — Indicates that the port is disabled.

○ *Port is selected* — Indicates that the port is selected for modification.

Select a port to configure. The port indicator changes to *Port is selected* (white).

2. Click **Modify**. The *Storm Control Configuration Page* opens:

Figure 42: Storm Control Configuration Page



Storm Control Configuration

Port	1/e27
Enable Broadcast Control	□
Broadcast Mode	Broadcast Only
Broadcast Rate Threshold	3500

The *Storm Control Configuration Page* contains the following fields:

- **Port —** Indicates the port from which storm control is enabled.
- **Enable Broadcast Control —** Indicates if forwarding Broadcast packet types is enabled on the port. The field values are:
  - *Enabled* — Enables storm control on the selected port.
  - *Disabled* — Disables storm control on the selected port.
- **Broadcast Mode —** Specifies the Broadcast mode currently enabled on the device. The possible field values are:
  - *Multicast & Broadcast* — Counts both Broadcast and Multicast traffic together.
  - *Broadcast* Only — Counts only the Broadcast traffic.
- **Broadcast Rate Threshold** — Indicates the maximum rate (kilobits per second) at which unknown packets are forwarded.

  The range for Giga ports is 3500-100,000. The default value is 3500.

3. Select the *Port Storm Control Settings*.
4. Click *Enable Broadcast Control*, and define the *Rate Threshold*.
5. Click **Apply**. Storm control is enabled on the device for the selected port.
6. Click **Save Config** on the menu to save the changes permanently.

Defining Access Control

Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Your switch supports up to 256 ACLs. Packets entering an ingress port, with an active ACL, are either admitted or denied entry. If they are denied entry, the user can disable the port. ACLs are composed of access control entries (ACEs) that are made of the filters that determine traffic classifications. The total number of ACEs that can be defined in all ACLs together is 256.

This section contains the following topics:

- Defining MAC Based ACL
- Defining IPv4 Based ACL
- Defining IPv6 Based ACL
- Defining ACL Binding

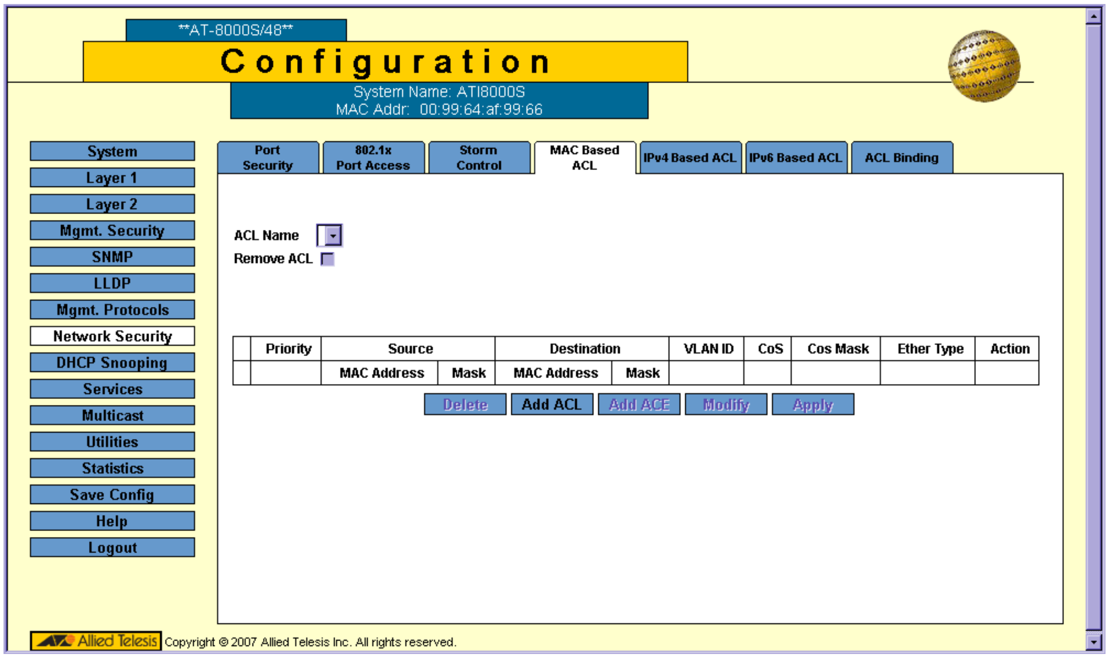
Defining MAC Based ACL

The *MAC Based ACL Page* allows a MAC-based Access Control List (ACL) to be defined. The table lists Access Control Elements (ACE) rules, which can be added only if the ACL is not bound to an interface.

To define a MAC Based ACL:

1. Click **Network Security** > **MAC Based ACL**. The *MAC Based ACL Page* opens:

Figure 43: MAC Based ACL Page



ACL Name
Remove ACL □

	Priority	Source		Destination		VLAN ID	CoS	Cos Mask	Ether Type	Action
		MAC Address	Mask	MAC Address	Mask					

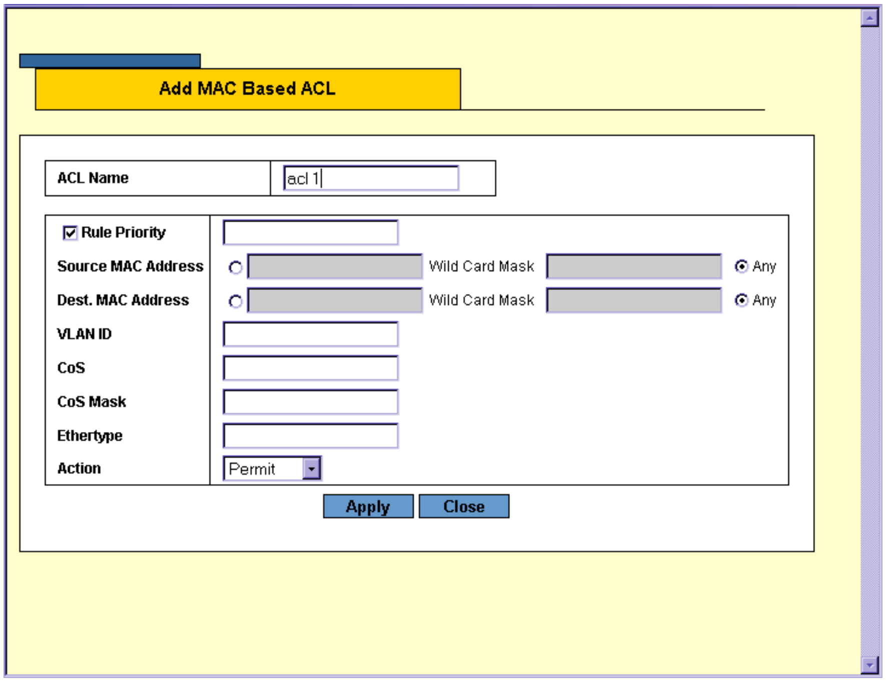
Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *MAC Based ACL Page* contains the following fields:

- **ACL Name** — Displays the specific MAC based ACLs.
- **Remove ACL** — Deletes the specified ACL. The possible field values are:
  - *Checked* — Deletes the ACL when user clicks the **Apply** button.
  - *Unchecked* — Maintains the ACL.
- **Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address** — Matches the source MAC address from which packets are addressed to the ACE.
- **Source MAC Mask** — Indicates the source MAC Address wild card mask. Wildcards are used to mask all or part of a source MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wild card of 00:00:00:00:00:00 indicates that all the octets are important.
- **Destination MAC Address** — Matches the destination MAC address to which packets are addressed to the ACE.
- **Destination MAC Mask** — Indicates the destination MAC Address wild card mask. Wildcards are used to mask all or part of a destination MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wild card of 00:00:00:00:00:00 indicates that all the octets are important.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4093.
- **CoS** — Class of Service of the packet.
- **CoS Mask** — Wild card bits to be applied to the CoS.
- **Ether Type** — The Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. For example, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. Possible field values are:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Setting Configuration Page*.
- **Delete** — To remove an ACE, click the ACE's checkbox and click the **Delete** button.

2. Click the **Add ACL** button. The *Add MAC Based ACL Page* opens:

Figure 44: Add MAC Based ACL Page



Add MAC Based ACL

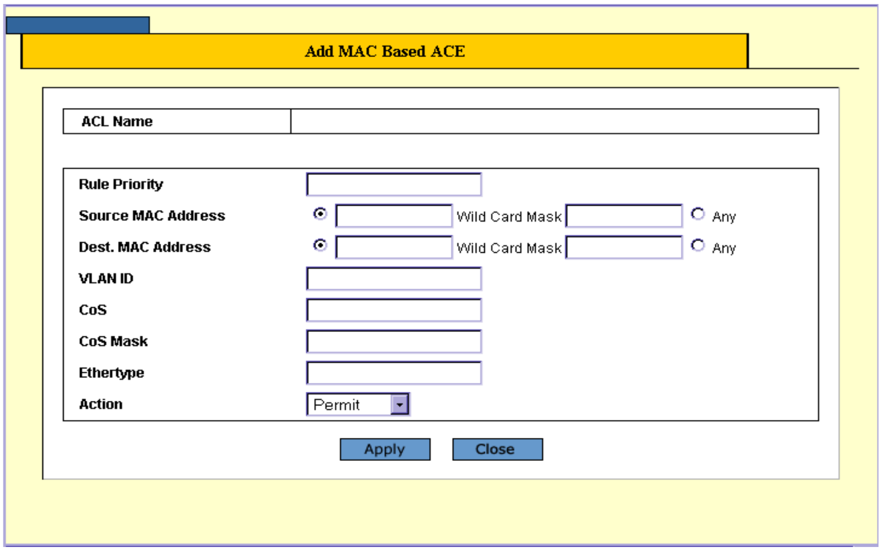
ACL Name	acl 1			
☑ Rule Priority				
Source MAC Address	○	Wild Card Mask		● Any
Dest. MAC Address	○	Wild Card Mask		● Any
VLAN ID				
CoS				
CoS Mask				
Ethertype				
Action	Permit			

3. In the **ACL Name** field, type a name for the ACL.
4. Enable **Rule Priority** and define the ACL’s relevant fields.
5. Click **Apply**. The MAC Based ACL configuration is defined and the device is updated.
6. Click **Save Config** on the menu to save the changes permanently.

Adding ACE Rules

1. Click **Network Security** > **MAC Based ACL**. The *MAC Based ACL Page* opens.
2. Click the Add ACE button. The *Add MAC Based ACE Page* opens.

Figure 45: Add MAC Based ACE Page



Add MAC Based ACE

ACL Name

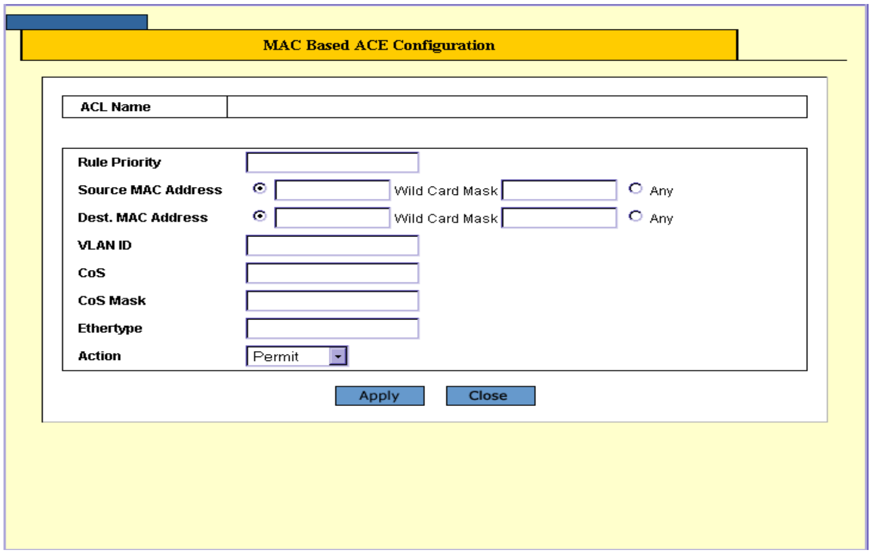
Rule Priority
Source MAC Address ● Wild Card Mask ○ Any
Dest. MAC Address ● Wild Card Mask ○ Any
VLAN ID
CoS
CoS Mask
Ethertype
Action Permit

3. Define the fields.
4. Click **Apply**. The MAC Based ACE rule is defined and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

To modify the MAC Based ACL configuration:

1. Click **Network Security > MAC Based ACL**. The *MAC Based ACL Page* opens.
2. Click **Modify**. The *MAC Based ACE Configuration Page* opens:

Figure 46: MAC Based ACE Configuration Page



MAC Based ACE Configuration

ACL Name

Rule Priority
Source MAC Address ● Wild Card Mask ○ Any
Dest. MAC Address ● Wild Card Mask ○ Any
VLAN ID
CoS
CoS Mask
Ethertype
Action: Permit

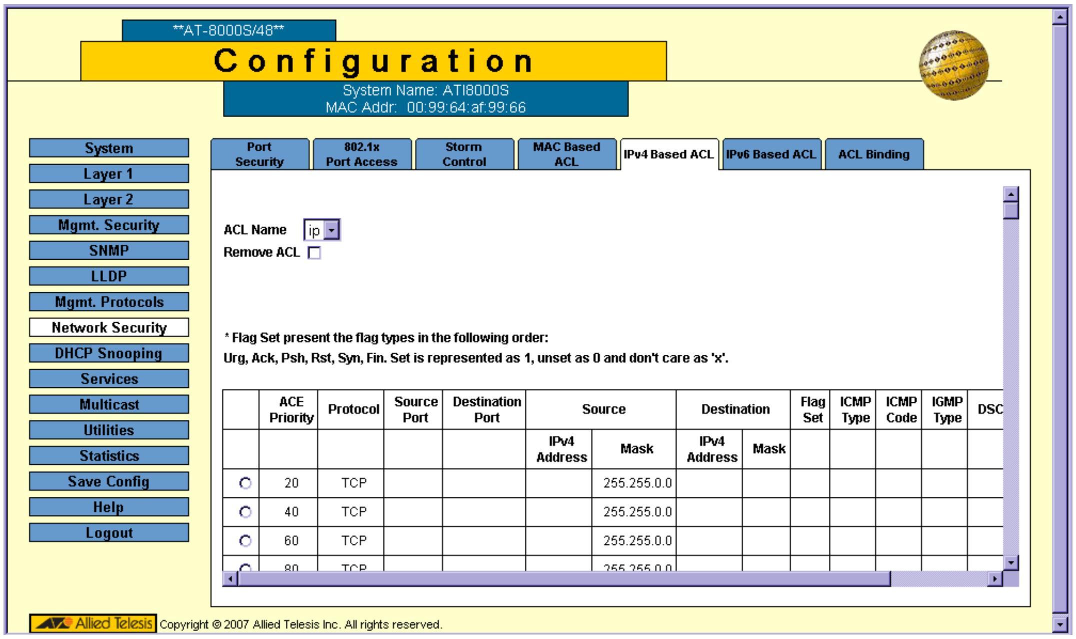
3. Define the fields.
4. Click **Apply**. The MAC Based ACL configuration is defined, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

Defining IPv4 Based ACL

The *IPv4 Based ACL Page* contains information for defining IPv4-based ACLs, including defining the ACEs for IPv4-based ACLs.

1. Click **Network Security** > **IPv4 Based ACL**. The *IPv4 Based ACL Page* opens.

Figure 47: IPv4 Based ACL Page



ACL Name ip

Remove ACL □

* Flag Set present the flag types in the following order:
Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, unset as 0 and don't care as 'x'.

	ACE Priority	Protocol	Source Port	Destination Port	Source		Destination		Flag Set	ICMP Type	ICMP Code	IGMP Type	DSC
					IPv4 Address	Mask	IPv4 Address	Mask					
○	20	TCP				255.255.0.0							
○	40	TCP				255.255.0.0							
○	60	TCP				255.255.0.0							
○	80	TCP				255.255.0.0							

The *IPv4 Based ACL Page* contains the following fields:

- **ACL Name** — Displays the specific IP based ACLs.
- **Remove ACL** — Deletes the specified ACL. The possible field values are:
  - *Checked* — Deletes the ACL when user clicks the **Apply** button.
  - *Unchecked* — Maintains the ACL.
- **ACE Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. The available protocols are:
  - *ICMP* — Internet Control Message Protocol (ICMP). The ICMP allows the gateway or destination host to communicate with the source host. For example, reporting a processing error.
  - *IGMP* — Internet Group Management Protocol (IGMP). Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific Multicast group.
  - *IP* — Internet Protocol (IP). Specifies the format of packets and their addressing method. IP defines addresses to packets and forwards the packets to the correct port.
  - *TCP* — Transmission Control Protocol (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order they are sent.
  - *EGP* — Exterior Gateway Protocol (EGP). Permits the exchange of routing information between two neighboring gateway hosts in an autonomous systems network.
  - *IGP* — Interior Gateway Protocol (IGP). Permits the exchange of routing information between gateways in an autonomous network.
  - *UDP* — User Datagram Protocol (UDP). Communication protocol that transmits packets but does not guarantee their delivery.

  - *HMP* — Host Mapping Protocol (HMP). Collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network.
  - *RDP* — Remote Desktop Protocol (RDP). Allows clients to communicate with the Terminal Server over the network.
  - *IDPR* — Matches the packet to the Inter-Domain Policy Routing (IDPR) protocol.
  - *IDRP*— Matches the packet to the Inter-Domain Routing Protocol (IDRP).
  - *RSVP* — Matches the packet to the ReSerVation Protocol (RSVP).
  - *AH* — Authentication Header (AH). Provides source host authentication and data integrity.
  - *EIGRP* — Enhanced Interior Gateway Routing Protocol (EIGRP). Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.
  - *OSPF* — The Open Shortest Path First (OSPF) protocol is a link-state, hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs).
  - *IPIP* — IP over IP (IPIP). Encapsulates IP packets to create tunnels between two routers. This ensures that IPIP tunnel appears as a single interface, rather than several separate interfaces. IPIP enables tunnel intranets to access the internet, and provides an alternative to source routing.
  - *PIM* — Matches the packet to Protocol Independent Multicast (PIM).
  - *L2TP*— Matches the packet to Layer 2 Internet Protocol (L2IP).
  - *ISIS* — Intermediate System - Intermediate System (ISIS). Distributes IP routing information throughout a single Autonomous System in IP networks.
  - *Any* — Matches the protocol to any protocol.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if 800/6-TCP or 800/17-UDP are selected in the Select from List drop-down menu. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if 800/6-TCP or 800/17-UDP are selected in the Select from List drop-down menu. The possible field range is 0 - 65535.
- **Source**
  - *IPv4 Address* — Matches the source port IPv4 address from which packets are addressed to the ACE.
  - *Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important.

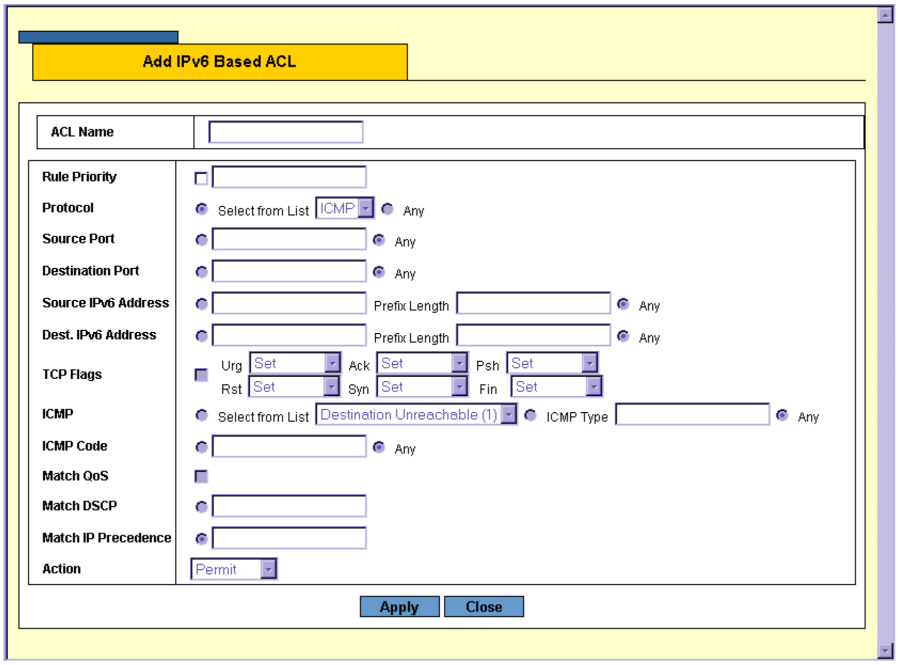
- **Destination**
  - *IPv4 Address* — Matches the destination port IPv4 address to which packets are addressed to the ACE.
  - *Mask* — Defines the destination IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important.
- **Flag Set** — Sets the indicated TCP flag that can be triggered. The possible values are:
  - *Urg, Ack, Psh, Rst, Syn,* and *Fin*.

  The indicated value setting is represented by one of the following:

  - *1* — Flag is set.
  - *0* — Flag is disabled.
  - *x* — Don't care.
- **ICMP Type** — Filters packets by ICMP message type. The field values are 0-255.
- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **IGMP Type** — Filters packets by IGMP message or message types.
- **DSCP** — Matches the packets DSCP value.
- **IP Prec.** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management Page*.
- **Delete** — To remove an ACE, click the ACE's checkbox and click the **Delete** button.

2. Click the **Add ACL** Button. The *Add IPv4 Based ACL Page* opens:

Figure 48: Add IPv4 Based ACL Page



Add IPv6 Based ACL

ACL Name	
Rule Priority	□
Protocol	● Select from List ICMP ○ Any
Source Port	○ ● Any
Destination Port	○ ● Any
Source IPv6 Address	○ Prefix Length ● Any
Dest. IPv6 Address	○ Prefix Length ● Any
TCP Flags	□ Urg Set Ack Set Psh Set Rst Set Syn Set Fin Set
ICMP	○ Select from List Destination Unreachable (1) ○ ICMP Type ● Any
ICMP Code	○ ● Any
Match QoS	□
Match DSCP	○
Match IP Precedence	●
Action	Permit

In addition to the *IPv4 Based ACL Page,* the *Add IPv4 Based ACL Page* contains the following fields:

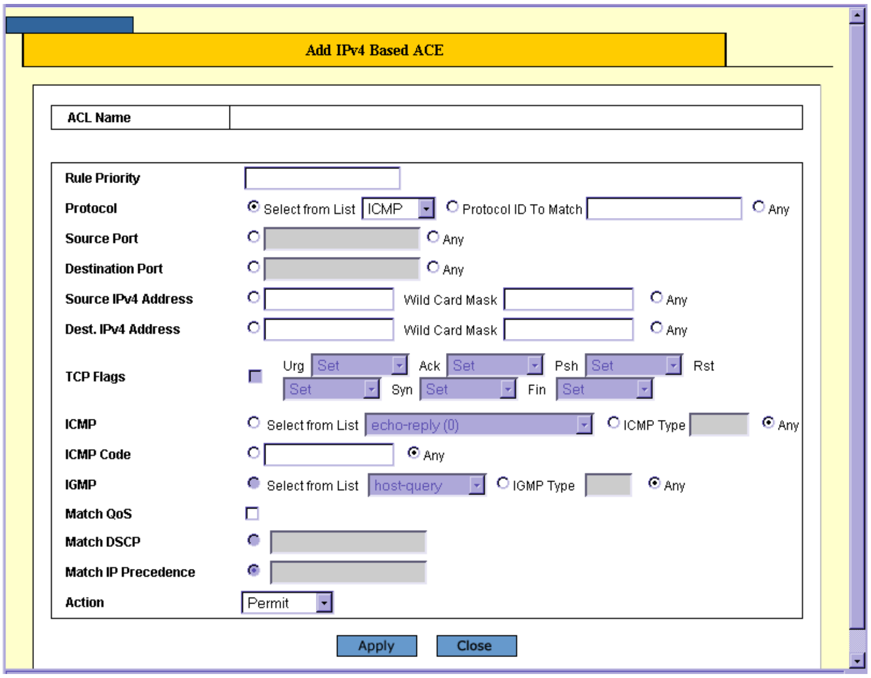
- **Match QoS** — Enables or disables the ACL classification to identify flows based on QoS values, such as DSCP or IP Precedence. The possible field values are:
  - *Checked* — Enables identification of flows based on QoS values. Selecting this option makes the **Match DSCP** and **Match IP Precedence** fields available.
  - *Unchecked* — Disables identification of flows based on QoS values.

3. Define the fields.
4. Click **Apply**. The IPv4-based ACL configuration is defined, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

Adding ACE Rules

1. Click **Network Security** > **IPv4 Based ACL**. The *IPv4 Based ACL Page* opens.
2. Click the **Add ACE** button. The *Add IPv4 Based ACE Page* opens.

Figure 49: Add IPv4 Based ACE Page



Add IPv4 Based ACE

ACL Name	

Rule Priority	
Protocol	● Select from List ICMP ○ Protocol ID To Match ○ Any
Source Port	○ ○ Any
Destination Port	○ ○ Any
Source IPv4 Address	○ Wild Card Mask ○ Any
Dest. IPv4 Address	○ Wild Card Mask ○ Any
TCP Flags	☐ Urg Set Ack Set Psh Set Rst Set Syn Set Fin Set
ICMP	○ Select from List echo-reply (0) ○ ICMP Type ● Any
ICMP Code	○ ● Any
IGMP	● Select from List host-query ○ IGMP Type ● Any
Match QoS	☐
Match DSCP	●
Match IP Precedence	●
Action	Permit

3. Define the fields.
4. Click **Apply**. The IPv4-based ACE rule is defined and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

To modify the IPv4-based ACL configuration:

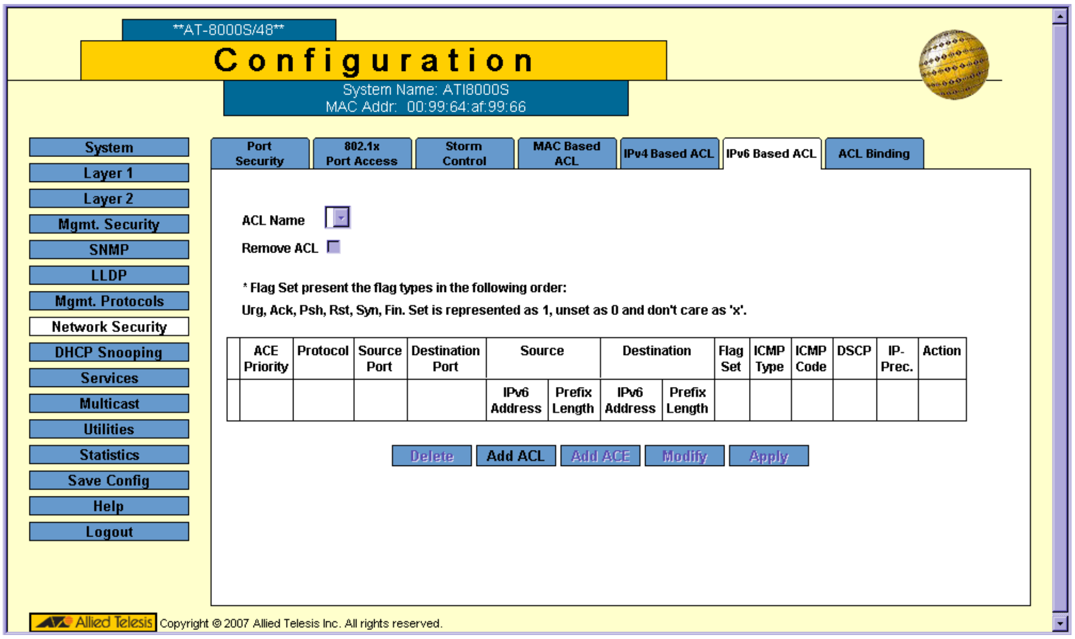
1. Click **Network Security > IPv4 Based ACL**. The *IPv4 Based ACL Page* opens.
2. Click **Modify**. The *IPv4 Based ACE Configuration Page* opens:
3. Define the fields.
4. Click **Apply**. The IPv4-based ACL configuration is defined, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

Defining IPv6 Based ACL

The *IPv6 Based ACL Page* contains information for defining IPv6-based ACLs, including defining the ACEs defined for IPv6-based ACLs.

1. Click **Network Security** > **IPv6 Based ACL**. The *IPv6 Based ACL Page* opens.

Figure 50: IPv6 Based ACL Page



ACL Name

Remove ACL □

* Flag Set present the flag types in the following order:
Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, unset as 0 and don't care as 'x'.

	ACE Priority	Protocol	Source Port	Destination Port	Source		Destination		Flag Set	ICMP Type	ICMP Code	DSCP	IP-Prec.	Action
					IPv6 Address	Prefix Length	IPv6 Address	Prefix Length						

The *IPv6 Based ACL Page* contains the following fields:

- **ACL Name** — Displays the specific IPv6-based ACLs.
- **Remove ACL** — Deletes the specified ACL. The possible field values are:
  - *Checked* — Deletes the ACL when user clicks the **Apply** button.
  - *Unchecked* — Maintains the ACL.
- **ACE Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. The available protocols are:
  - *ICMP* — Internet Control Message Protocol (ICMP). The ICMP allows the gateway or destination host to communicate with the source host. For example, reporting a processing error.
  - *TCP* — Transmission Control Protocol (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order they are sent.

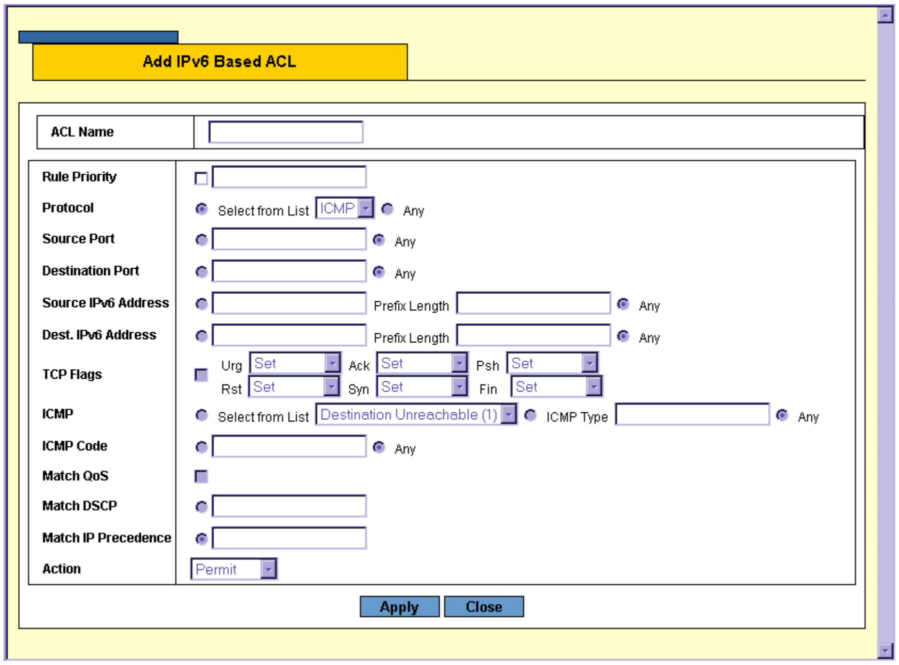
  - *UDP* — User Datagram Protocol (UDP). Communication protocol that transmits packets but does not guarantee their delivery.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if 800/6-TCP or 800/17-UDP are selected in the Select from List drop-down menu. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if 800/6-TCP or 800/17-UDP are selected in the Select from List drop-down menu. The possible field range is 0 - 65535.
- **Source**
  - *IPv6 Address* — Matches the source port IPv6 address from which packets are addressed to the ACE.
  - *Prefix Length* — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Destination**
  - *IPv6 Address* — Matches the destination port IPv6 address to which packets are addressed to the ACE.
  - *Prefix Length* — Defines the number of bits that comprise the destination IP address prefix, or the network mask of the destination IP address.
- **Flag Set** — Sets the indicated TCP flag that can be triggered. The possible values are:
  - *Urg, Ack, Psh, Rst, Syn,* and *Fin*.

  The indicated value setting is represented by one of the following:

  - *1* — Flag is set.
  - *0* — Flag is disabled.
  - *x* — Don't care.
- **ICMP Type** — Filters packets by ICMP message type. The field values are 0-255.
- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **DSCP** — Matches the packets DSCP value.
- **IP Prec.** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management Page*.
- **Delete** — To remove an ACE, click the ACE's checkbox and click the **Delete** button.

2. Click the **Add ACL** Button. The *Add IPv6 Based ACL Page* opens:

Figure 51: Add IPv6 Based ACL Page



Add IPv6 Based ACL

ACL Name	
Rule Priority	□
Protocol	● Select from List ICMP ○ Any
Source Port	○ ● Any
Destination Port	○ ● Any
Source IPv6 Address	○ Prefix Length ● Any
Dest. IPv6 Address	○ Prefix Length ● Any
TCP Flags	□ Urg Set Ack Set Psh Set Rst Set Syn Set Fin Set
ICMP	○ Select from List Destination Unreachable (1) ○ ICMP Type ● Any
ICMP Code	○ ● Any
Match QoS	□
Match DSCP	○
Match IP Precedence	●
Action	Permit

In addition to the *IPv6 Based ACL Page,* the *Add IPv6 Based ACL Page* contains the following fields:

- **Match QoS** — Enables or disables the ACL classification to identify flows based on QoS values, such as DSCP or IP Precedence. The possible field values are:
  - *Checked* — Enables identification of flows based on QoS values. Selecting this option makes the **Match DSCP** and **Match IP Precedence** fields available.
  - *Unchecked* — Disables identification of flows based on QoS values.

3. Define the fields.
4. Click **Apply**. The IPv6-based ACL configuration is defined, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

Adding ACE Rules

1. Click **Network Security** > **IPv6 Based ACL**. The *IPv6 Based ACL Page* opens.
2. Click the **Add ACE** button. The *Add IPv6 Based ACE Page* opens.
3. Define the fields.
4. Click **Apply**. The IPv6-based ACE rule is defined and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

To modify the IPv6-based ACL configuration:

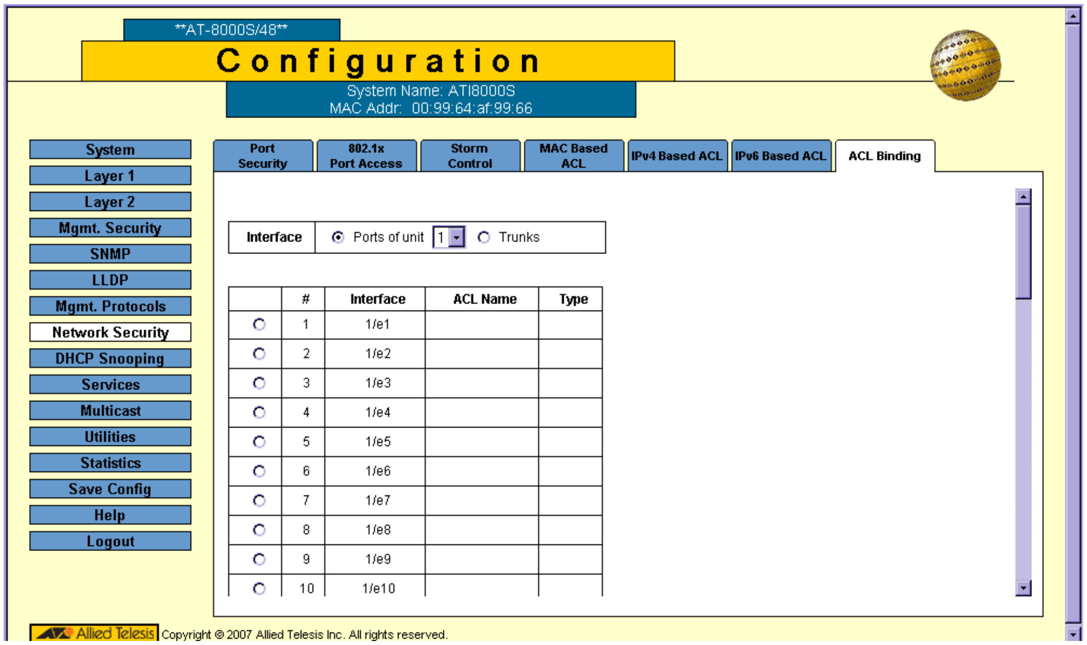
1. Click **Network Security > IPv6 Based ACL**. The *IPv6 Based ACL Page* opens.
2. Click **Modify**. The *IPv6 Based ACE Configuration Page* opens:
3. Define the fields.
4. Click **Apply**. The IPv6-based ACL configuration is defined, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

Defining ACL Binding

When an ACL is bound to an interface, all the ACE rules that have been defined are applied to the selected interface. Whenever an ACL is assigned on an interface, flows from that ingress interface that do not match the ACL are matched to the default rule, which is Drop unmatched packets.

1. Click **Network Security** > **ACL Binding**. The *ACL Binding Page* opens:

Figure 52: ACL Binding Page



Interface ● Ports of unit 1 ○ Trunks

	#	Interface	ACL Name	Type
○	1	1/e1		
○	2	1/e2		
○	3	1/e3		
○	4	1/e4		
○	5	1/e5		
○	6	1/e6		
○	7	1/e7		
○	8	1/e8		
○	9	1/e9		
○	10	1/e10		

The *ACL Binding Page* contains the following fields:

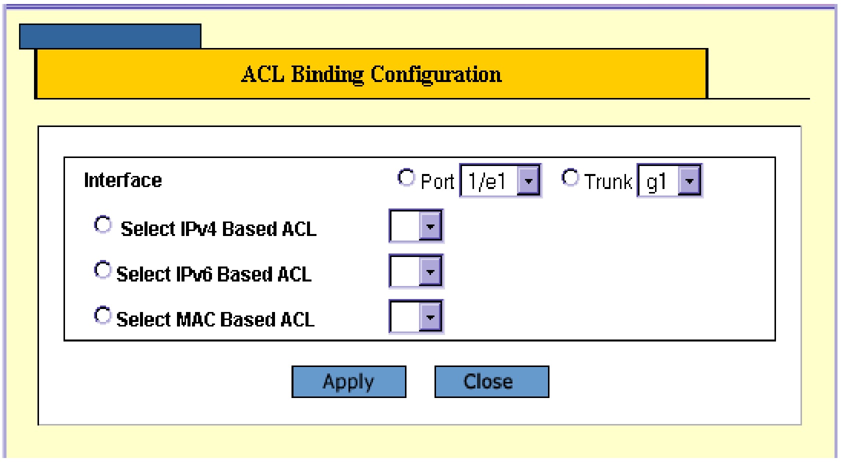
- **Interface** — Indicates the interface to which the ACL is bound. The possible values are:
  - *Unit* — Stacking member and port associated with the ACL.
  - *Trunk* — Trunk associated with the ACL.

For each entry, an interface has a bound ACL.

- **Interface** — Indicates the interface associated with the ACL.
- **ACL Name** — Indicates the ACL that is bound to the interface.
- **Type** — Indicates the type of access control:
  - *MAC-based ACL*
  - *IPv4-based ACL*
  - *IPv6-based ACL*

2. Click the **Modify** button. The *ACL Binding Configuration* opens:

Figure 53: ACL Binding Configuration



ACL Binding Configuration

Interface ○ Port 1/e1 ○ Trunk g1

○ Select IPv4 Based ACL

○ Select IPv6 Based ACL

○ Select MAC Based ACL

The *ACL Binding Configuration* contains the following fields:

- **Interface** — Choose the interface to which the ACL is bound. The possible values are:
  - *Port* — Port associated with the ACL.
  - *Trunk* — Trunk associated with the ACL.
- **Select IPv4 Based ACL**, **IPv6 Based ACL** or **MAC Based ACL** — Choose the ACL that is bound to the interface.

3. Define the fields.
4. Click **Apply.** ACL binding is defined, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

Chapter 6. Configuring DHCP Snooping

DHCP Snooping expands network security by providing an extra layer of security between untrusted interfaces and DHCP servers. By enabling DHCP Snooping network administrators can identify between trusted interfaces connected to end-users or DHCP Servers, and untrusted interface located beyond the network firewall.

DHCP Snooping filters untrusted messages. DHCP Snooping creates and maintains a DHCP Snooping Table which contains information received from untrusted packets. Interfaces are untrusted if the packet is received from an interface from outside the network or from a interface beyond the network firewall. Trusted interfaces receive packets only from within the network or the network firewall.

DHCP with Option 82 attaches authentication messages to the packets sent from the host. DHCP passes the configuration information to hosts on a TCP/IP network. This permits network administrators to limit address allocation authorized hosts. DHCP with Option 82 can be enabled only if DHCP snooping is enabled.

The *DHCP Snooping Table* contains the untrusted interfaces MAC address, IP address, Lease Time, VLAN ID, and interface information.

This section contains the following topics:

- Defining DHCP Snooping General Properties
- Defining DHCP Snooping on VLANs
- Defining Trusted Interfaces
- Binding Addresses to the DHCP Snooping Database

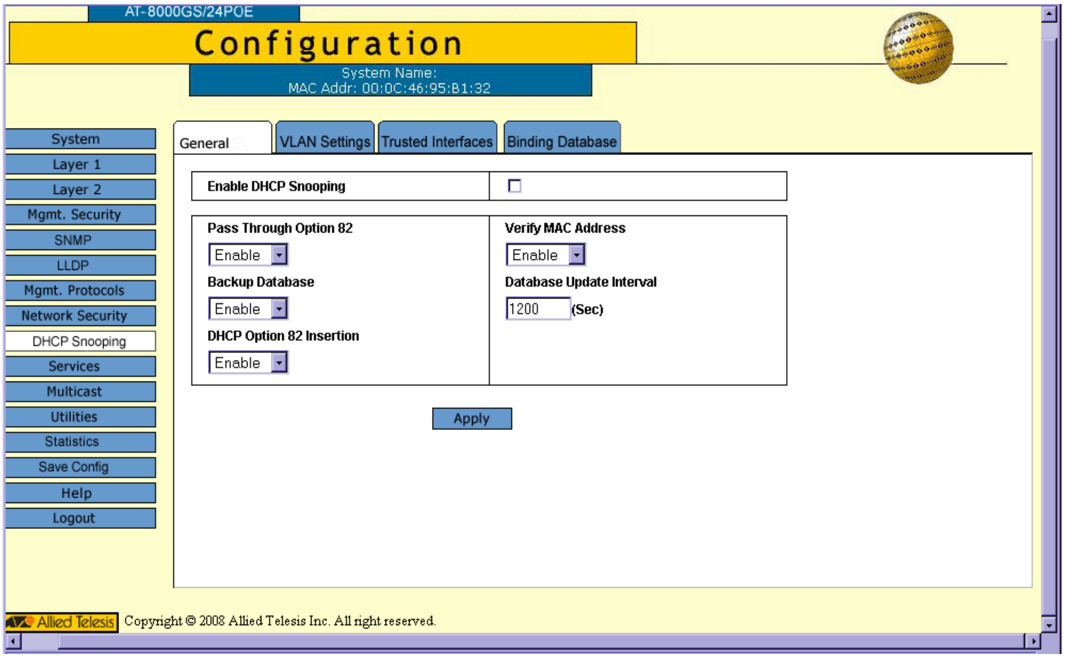
Defining DHCP Snooping General Properties

The *DHCP Snooping General Page* contains parameters for enabling DHCP Snooping on the device.

To define DHCP Snooping on the device:

1. Click **DHCP Snooping > General**. The *DHCP Snooping General Page* opens:

Figure 54: DHCP Snooping General Page



System Name:
MAC Addr: 00:0C:46:95:B1:32

Enable DHCP Snooping ☐

Pass Through Option 82: Enable

Verify MAC Address: Enable

Backup Database: Enable

Database Update Interval: 1200 (Sec)

DHCP Option 82 Insertion: Enable

The *DHCP Snooping General Page* contains the following fields:

- **Enable DHCP Snooping Status** — Indicates if DHCP Snooping is enabled on the device. The possible field values are:
  - *Checked* — Enables DHCP Snooping on the device.
  - *Unchecked* — Disables DHCP Snooping on the device. This is the default value.
- **Pass Through Option 82** — Indicates if DHCP Option 82 with data insertion is enabled on the device. The possible field values are:
  - *Enable* — If DHCP Option 82 with data insertion is enabled, the DHCP relay agent or DHCP Snooping switch can insert information into the DHCP DISCOVER message. The Relay agent information option specifies the port number from which the client's packet was received.
  - *Disable* — Disables DHCP Option 82 with data insertion on the device. This is the default value.
- **Verify MAC Address** — Indicates if MAC addresses are verified. The possible field values are:
  - *Enable* — Verifies that an untrusted port source MAC address matches the client's MAC address. This is the default value.

  - *Disable* — Disables verifying that an untrusted port source MAC address matches the client's MAC address.
- **Backup Database** — Indicates if the DHCP Snooping Database is enabled. The possible field values are:
  - *Enable* — Enables storing allotted IP addresses in the DHCP Snooping Database.
  - *Disable* — Disables storing allotted IP addresses in the DHCP Snooping Database. This is the default value.
- **Database Update Interval** — Indicates how often the DHCP Snooping Database is updated. The possible field range is 600 – 86400 seconds. The field default is 1200 seconds.
- **DHCP Option 82 Insertion** — DHCP Option 82 attaches authentication messages to the packets sent to DHCP Server via TCP/IP network. The option permits network administrators to limit address allocation to authorized hosts only. This permits network administrators to limit address allocation authorized hosts. The possible field values are:
  - *Enable* — Enables DHCP Option 82 Insertion on the device.
  - *Disable* — Disables DHCP Option 82 Insertion on the device. This is the default value.

2. Define the fields.
3. Click **Apply**. The DHCP Snooping configuration is defined and the device is updated.
4. Click **Save Config** on the menu to save the changes permanently.

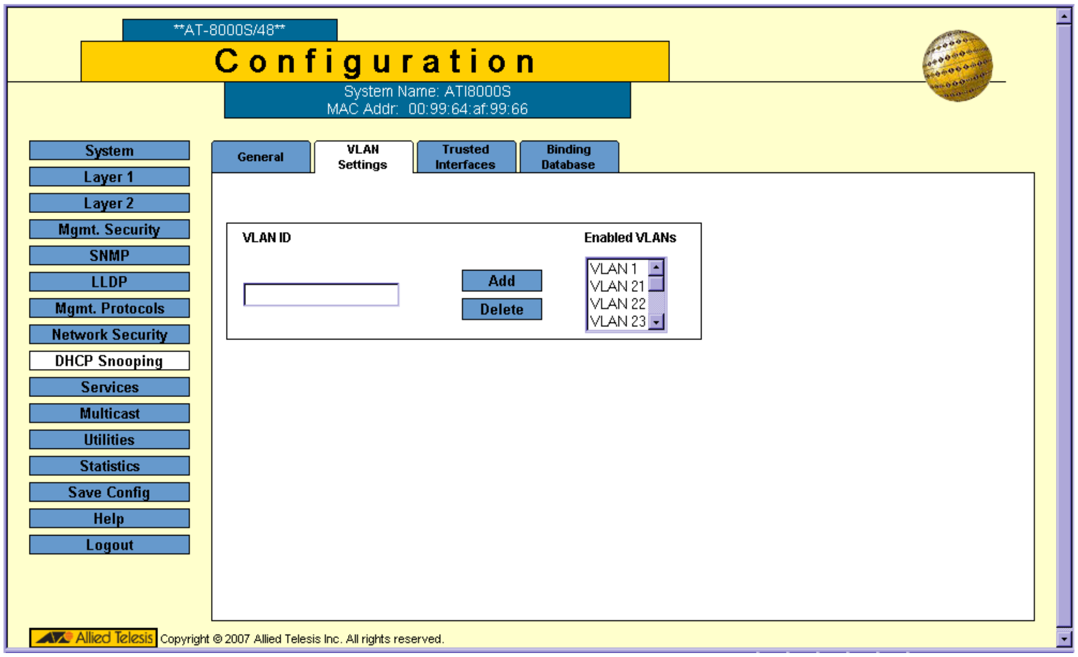
Defining DHCP Snooping on VLANs

The *VLAN Settings Page* allows network managers to enable DHCP snooping on VLANs. To enable DHCP Snooping on a VLAN, ensure DHCP Snooping is enabled on the device.

To define DHCP Snooping on VLANs:

1. Click **DHCP Snooping > VLAN Settings**. The *VLAN Settings Page* opens:

Figure 55: VLAN Settings Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Enabled VLANs: VLAN 1, VLAN 21, VLAN 22, VLAN 23

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *VLAN Settings Page* contains the following fields:

- **VLAN ID** — Indicates the VLAN to be added to the Enabled VLAN list.
- **Enabled VLANs** — Contains a list of VLANs for which DHCP Snooping is enabled.

2. Select the VLAN name from the VLAN ID list and click **Add**. This VLAN name then appears in the **Enabled VLANs** list.
3. Click **Save Config** on the menu to save the changes permanently.

Defining Trusted Interfaces

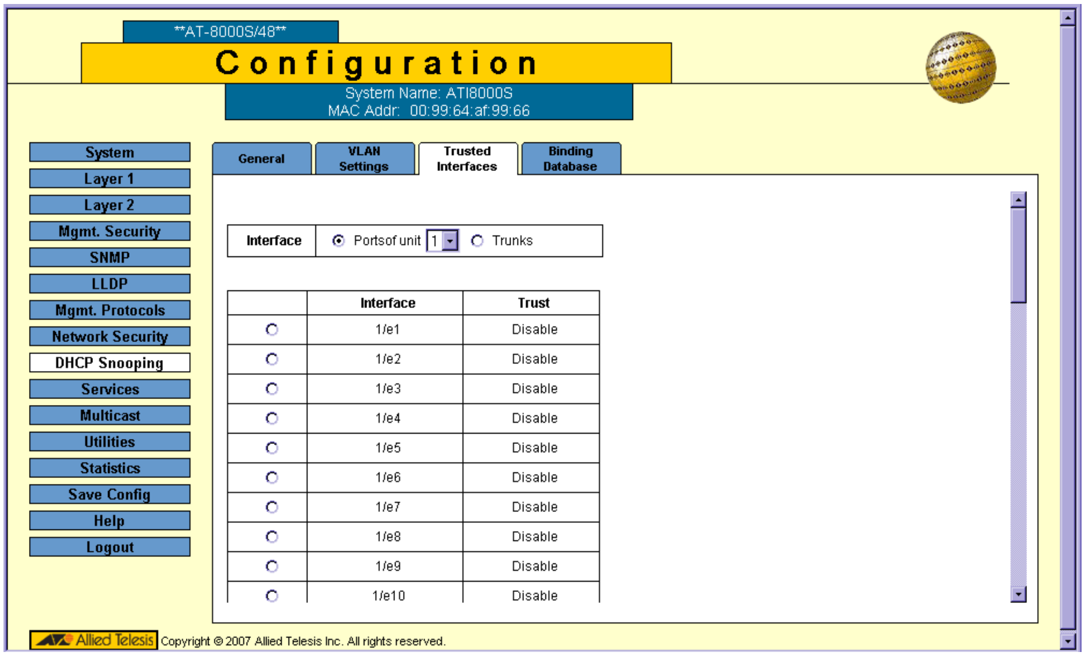
The *Trusted Interfaces Page* allows network manager to define Trusted interfaces. Trusted interfaces are connected to DHCP servers, switches, or hosts which do not require DHCP packet filtering. Trusted interfaces receive packets only from within the network or the network firewall, and are allowed to respond to DHCP requests. Packets sent from an interface outside the network, or from beyond the network firewall, are blocked by untrusted interfaces.

Conversely, untrusted interfaces can be configured to receive traffic from outside the network or the firewall.

To define trusted interfaces:

1. Click **DHCP Snooping > Trusted Interfaces**. The *Trusted Interfaces Page* opens:

Figure 56: Trusted Interfaces Page



AT-8000S/48

System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Interface ● Portsof unit 1 ○ Trunks

	Interface	Trust
○	1/e1	Disable
○	1/e2	Disable
○	1/e3	Disable
○	1/e4	Disable
○	1/e5	Disable
○	1/e6	Disable
○	1/e7	Disable
○	1/e8	Disable
○	1/e9	Disable
○	1/e10	Disable

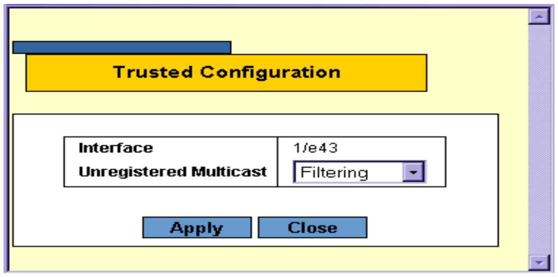
Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Trusted Interfaces Page* contains the following fields:

- Select the interfaces displayed in the table.
  - *Ports of Unit* — Displays the stacking member whose trusted interface configuration is displayed.
  - *Trunk* — Displays the trunks whose trusted interface configuration is displayed.
- **Interface** — Contains a list of existing interfaces.
- **Trust** — Indicates whether the interface is a Trusted interface

2. From the global Interface field, define the specific port or trunk.
3. In the table, select an interface and click **Modify**. The *Trusted Configuration Page* opens.

Figure 57: Trusted Configuration Page



Interface	1/e43
Unregistered Multicast	Filtering

4. Edit the following field:

- **Trusted Status** — Indicates whether the interface is a Trusted Interface.
  - *Enable* — Interface is a trusted interface.
  - *Disable* — Interface is an untrusted interface.

5. Click **Apply**. The Trusted Interfaces configuration is defined and the device is updated.
6. Click **Save Config** on the menu to save the changes permanently.

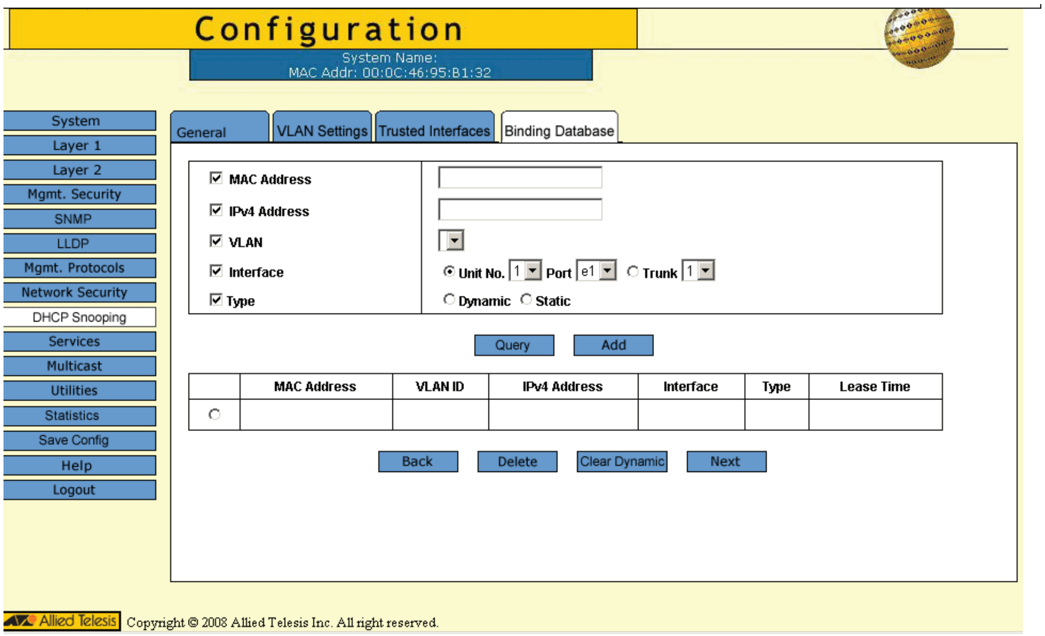
Binding Addresses to the DHCP Snooping Database

The *Binding Database Page* contains parameters for querying and adding IP addresses to the DHCP Snooping Database.

To bind addresses to the DHCP Snooping database:

1. Click **DHCP Snooping > Binding Database**. The *Binding Database Page* opens:

Figure 58: Binding Database Page



System Name:
MAC Addr: 00:0C:46:95:B1:32

☑ MAC Address

☑ IPv4 Address

☑ VLAN

☑ Interface ● Unit No. 1 Port e1 ○ Trunk 1

☑ Type ○ Dynamic ○ Static

	MAC Address	VLAN ID	IPv4 Address	Interface	Type	Lease Time
○						

Copyright © 2008 Allied Telesis Inc. All right reserved.

2. Define any of the following fields as a query filter:

Query Parameters

- **MAC Address** — Indicates the MAC addresses recorded in the DHCP Database. The Database can be queried by MAC address.
- **IPv4 Address** — Indicates the IPv4 addresses recorded in the DHCP Database The Database can be queried by IPv4 address.
- **VLAN** — Indicates the VLANs recorded in the DHCP Database. The Database can be queried by VLAN.
- **Interface** — Contains a list of interface by which the DHCP Database can be queried. The possible field values are:
  - *Unit No.* and *Port* — Queries the VLAN database by a specific stacking member and port number.
  - *Trunk* — Queries the VLAN database by trunk number.
- **Type** — Indicates the IP address binding type. The possible field values are:
  - *Static* — Indicates the IP address is static.
  - *Dynamic* — Indicates the IP address is dynamically defined by the DHCP server.

3. Click **Query**. The results appear in the Query Results table.

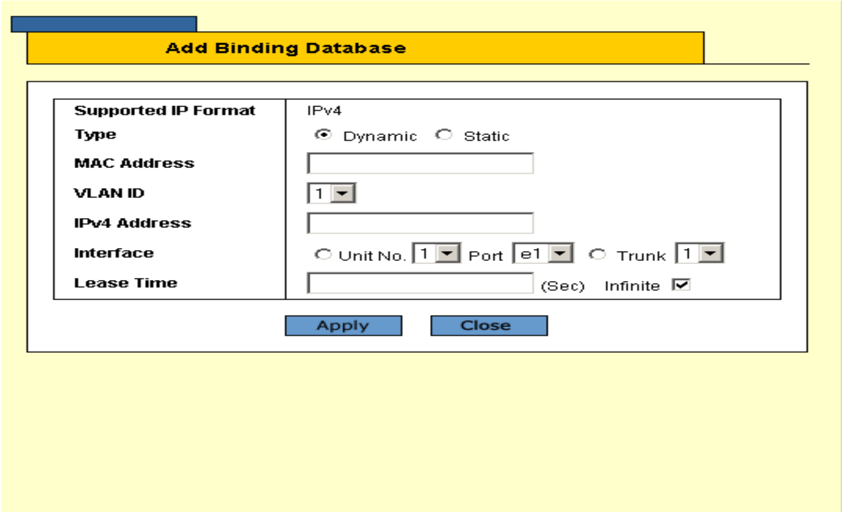
Query Results

The Query Results table contains the following fields:

- **MAC Address** — Indicates the MAC address found during the query.
- **VLAN ID** — Displays the VLAN ID to which the IP address is attached in the DHCP Snooping Database.
- **IPv4 Address** — Indicates the IPv4 address found during the query.
- **Interface** — Indicates the specific interface connected to the address found during the query.
- **Type** — Displays the IP address binding type. The possible field values are:
  - *Static* — Indicates the IP address is static.
  - *Dynamic* — Indicates the IP address is dynamically defined by the DHCP server.
- **Lease Time** — Displays the lease time. The Lease Time defines the amount of time the DHCP Snooping entry is active. Addresses whose lease times are expired are ignored by the switch. The possible values are 10 – 4294967295 seconds. In the *Add Binding Database Page*, select **Infinite** if the DHCP Snooping entry never expires.

4. Click **Create**. The *Add Binding Database Page* opens.

Figure 59: Add Binding Database Page



Supported IP Format	IPv4
Type	● Dynamic ○ Static
MAC Address	
VLAN ID	1
IPv4 Address	
Interface	○ Unit No. 1 Port e1 ○ Trunk 1
Lease Time	(Sec) Infinite ☑

5. Define the fields.
6. Click **Apply**. The bound address is added to the DHCP Snooping database, the *Add Binding Database Page* closes, and the device is updated.
7. To remove dynamic addresses from the Query Results table, click **Clear Dynamic**.
8. Click **Apply**. The addresses in the Query Results table are added to the DHCP Snooping Database.
9. Click **Save Config** on the menu to save the changes permanently.

Chapter 7. Configuring Ports

Port Configuration includes the following procedures for configuring ports and trunks on the device.

- Setting Ports Configurations
- Aggregating Ports

Setting Ports Configurations

This section contains the following topics:

- Defining Port Settings
- Configuring Port Mirroring

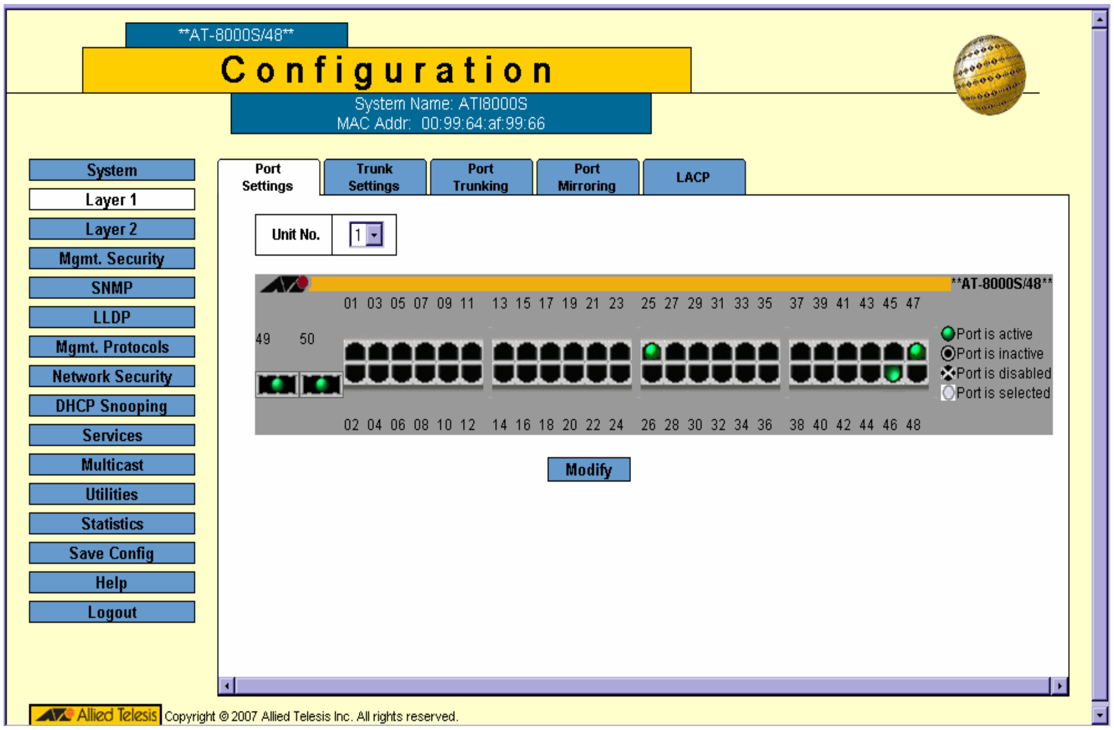
Defining Port Settings

The *Port Settings Page* contains fields for defining port parameters.

To define port general settings:

1. Click **Layer 1 > Port Settings**. The *Port Settings Page* opens:

Figure 60: Port Settings Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Unit No. 1

2. The *Port Settings Page* contains the Zoom View of the device ports. The possible port settings are::Select the

   ● *Port is active* — Indicates that the port is linked.

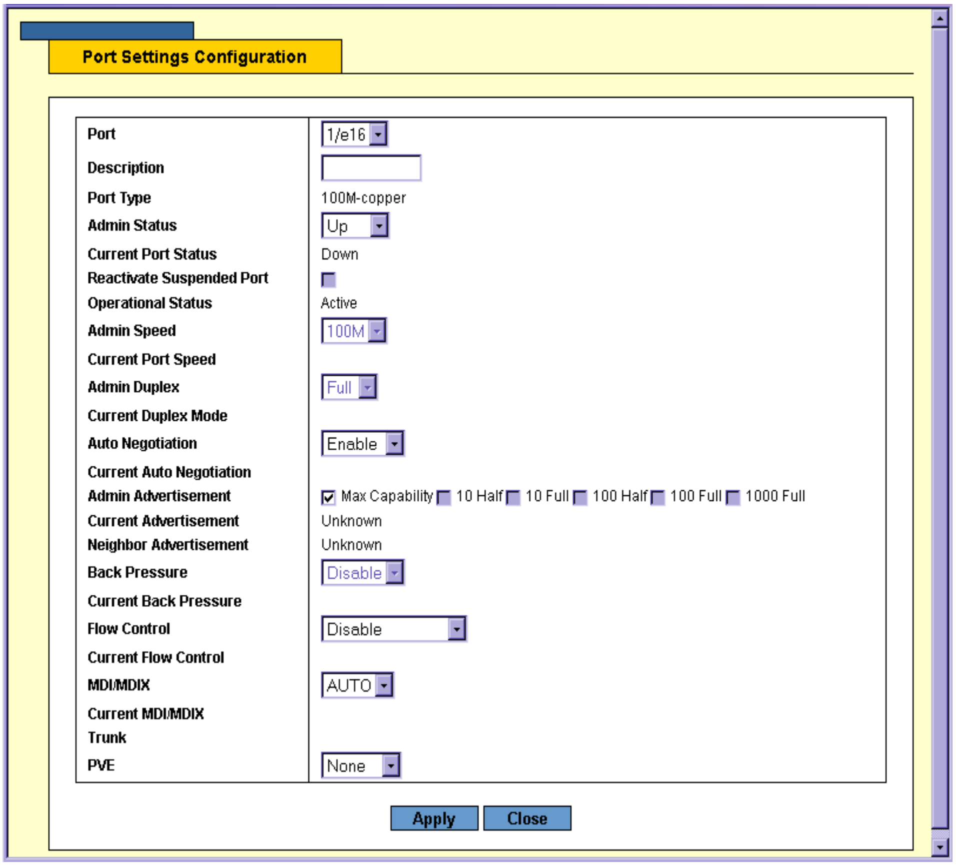
   ◙ *Port is inactive* — Indicates that the port is not linked.

   ☒ *Port is disabled* — Indicates that the port is disabled.

   ○ *Port is selected* — Indicates that the port is selected for modification.

   port(s). Clicking a port toggles it through the possible settings.
3. Click **Modify**. The *Port Setting Configuration Page* opens:

Figure 61: Port Setting Configuration Page



Port Settings Configuration

Port	1/e16
Description	
Port Type	100M-copper
Admin Status	Up
Current Port Status	Down
Reactivate Suspended Port	□
Operational Status	Active
Admin Speed	100M
Current Port Speed	
Admin Duplex	Full
Current Duplex Mode	
Auto Negotiation	Enable
Current Auto Negotiation	
Admin Advertisement	☑ Max Capability □ 10 Half □ 10 Full □ 100 Half □ 100 Full □ 1000 Full
Current Advertisement	Unknown
Neighbor Advertisement	Unknown
Back Pressure	Disable
Current Back Pressure	
Flow Control	Disable
Current Flow Control	
MDI/MDIX	AUTO
Current MDI/MDIX	
Trunk	
PVE	None

The *Port Setting Configuration Page* contains the following fields:

- **Port** — Lists the names of configured ports.
- **Description** — Provides a user-defined port description.
- **Port Type** — Indicates the port's maximum rate and connected media (copper or combo), for example, 1000M-ComboC.
- **Admin Status —** Displays the link administrative status. The possible field values are:
  - *Up* — Indicates that the port is currently operating.

  - *Down* — Indicates that the port is currently not operating.

Note

Admin settings, such as *Admin Status*, *Admin Speed* and so on, are settings made by an administrator and applied on the device. **Current** settings, such as *Current Port Status*, *Current Port Speed* and so on, are current operational settings received from the device and are read-only.

- **Current Port Status** — Indicates whether the port is currently operational or non-operational. The possible field values are:
  - *Up* — Indicates the port is currently operating.
  - *Down* — Indicates the port is currently not operating.
- **Reactivate Suspended Port** — Reactivates suspended ports. The possible field values are:
  - *Checked* — Reactivates the selected suspended port.
  - *Unchecked* — Maintains the port status. This is the default value.
- **Operational Status** — Indicates the port operational status. Possible field values are:
  - *Suspended* — The port is currently active, and is not receiving or transmitting traffic.
  - *Active* — Indicates the port is currently active and is receiving and transmitting traffic.
  - *Disable* — Indicates the port is currently disabled, and is not receiving or transmitting traffic.
  - *Unknown* — Indicates the port status is currently unknown.
- **Admin Speed** — Indicates the configured rate for the port. The port type determines what speed setting options are available. Admin speed can only be designated when auto-negotiation is disabled. The possible field values are:
  - *10M* — Indicates the port is currently operating at 10 Mbps.
  - *100M* — Indicates the port is currently operating at 100 Mbps.
  - *1000M* — Indicates the Giga port is currently operating at 1000 Mbps.
- **Current Port Speed** — Displays the rate of the port.
- **Admin Duplex** — Indicates the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on trunks. The possible field values are:
  - *Full* — The interface supports transmission between the device and its link partner in both directions simultaneously.
  - *Half* — The interface supports transmission between the device and the client in only one direction at a time.
- **Current Duplex Mode** — Displays the current duplex mode.
- **Auto Negotiation** — Defines the auto negotiation status on the port. Auto negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode, and flow control abilities to its partner.
- **Current Auto Negotiation** — Displays the current Auto Negotiation setting.

- **Admin Advertisement** — Defines the auto negotiation setting the port advertises. The possible field values are:
  - *Max Capability* — Indicates that all port speeds and duplex mode settings are accepted.
  - *10 Half* — Indicates that the port advertises for a 10 Mbps speed port and half duplex mode setting.
  - *10 Full* — Indicates that the port advertises for a 10 Mbps speed port and full duplex mode setting.
  - *100 Half* — Indicates that the port advertises for a 100 Mbps speed port and half duplex mode setting.
  - *100 Full* — Indicates that the port advertises for a 100 Mbps speed port and full duplex mode setting.
  - *1000 Full* — Indicates that the port advertises for a 1000 Mbps speed port and full duplex mode setting.
- **Current Advertisement** — Indicates the port advertises its speed to its neighbor port to start the negotiation process. The possible field values are those specified in the Admin Advertisement field.
- **Neighbor Advertisement** — Indicates the neighboring port's advertisement settings.
- **Back Pressure** — Displays the back pressure mode on the port. Back pressure mode is used to adjust the transmission speed to avoid losing data. The possible field values are:
  - *Enabled* — Indicates that back pressure is enabled for the selected port.
  - *Disabled* — Indicates that back pressure is currently disabled for the selected port. This is the default value.
- **Current Back Pressure** — Displays the current Back Pressure setting.
- **Flow Control** — Displays the flow control status on the port. Operates when the port is in full duplex mode.
  - *Enable* — Indicates that flow control is currently enabled for the selected port.
  - *Disable* — Indicates that flow control is currently disabled for the selected port. This is the default value.
- **Current Flow Control** — Displays the current Flow Control setting.
- **MDI/MDIX** — Defines the MDI/MDIX status on the port. Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to ensure that the correct pairs are connected. The possible field values are:
  - *Auto* — Use to automatically detect the cable type.
  - *MDI (Media Dependent Interface)* — Use for end stations.
  - *MDIX (Media Dependent Interface with Crossover)* — Use for hubs and switches.
- **Current MDI/MDIX** — Displays the current MDI/MDIX setting.
- **Trunk** — Defines if the port is a member of a trunk.
- **PVE** — Enables a port to be a *Private VLAN Edge* (PVE) port, which is isolated from other ports. When a port is defined as PVE, it bypasses the Forwarding Database (FDB), and forwards all Unicast, Multicast and Broadcast traffic to an uplink (except MAC-to-me packets). Traffic from the uplink is distributed to all interfaces.

  None indicates that the port is not defined as PVE.

  Only one uplink can be defined for a protected port. An IP address cannot be configured on the VLAN of which a protected port is a member.

4. Define the fields.
5. Click **Apply**. The port settings are saved and the device is updated. The *Port Settings Page* is displayed.
6. Click **Save Config** on the menu to permanently save the change.

Configuring Port Mirroring

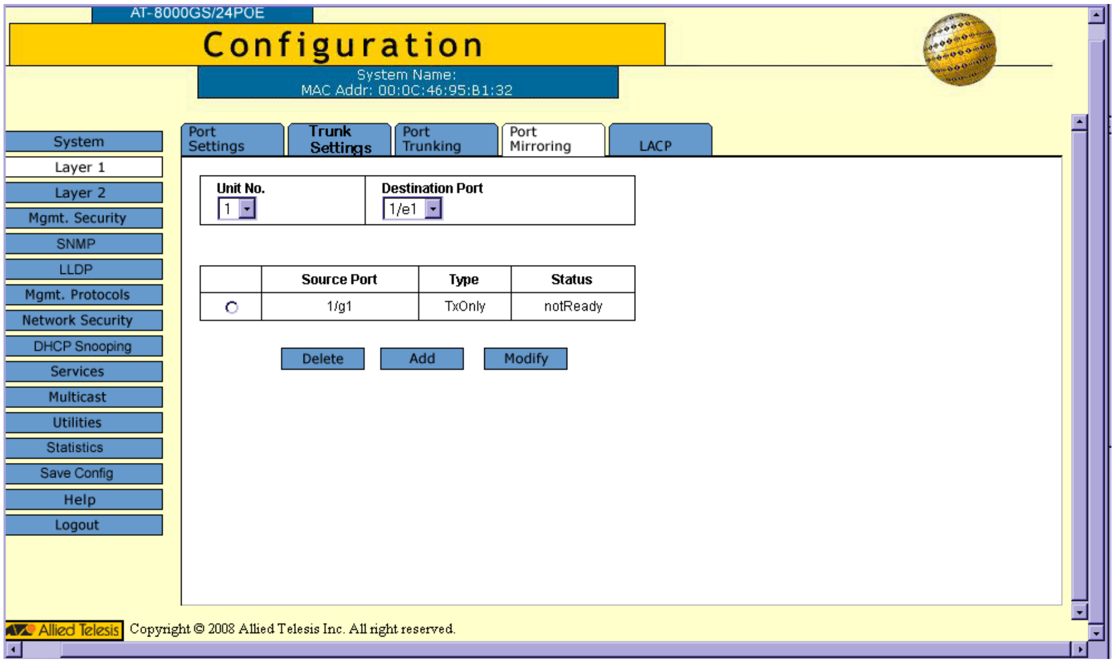
Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as a diagnostic tool as well as a debugging feature. Port mirroring also enables device performance monitoring.

Network administrators can configure port mirroring by selecting a specific port (called a destination port) to which packets are copied, and other ports (called source ports) from which packets are copied. The ratio is eight source ports to one destination port.

To define port mirroring:

1. Click **Layer 1 > Port Mirroring**. The *Port Mirroring Page* opens:

Figure 62: Port Mirroring Page



Unit No.	Destination Port
1	1/e1

	Source Port	Type	Status
○	1/g1	TxOnly	notReady

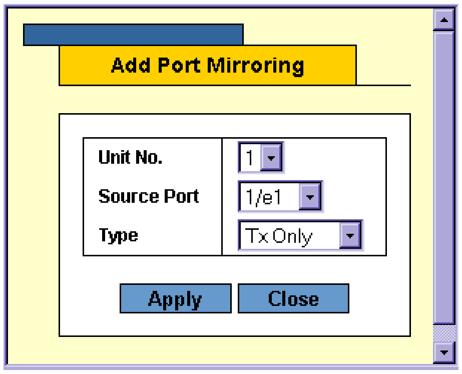
The *Port Mirroring Page* contains information about all port mirrors currently defined on the device. The following information is displayed:

- **Unit No.** — Indicates the stacking member’s unit number.
- **Destination Port** — Defines the port number to which port traffic is copied. Note that this port has to be detached from its VLAN before mirroring is configured. Only one destination port can be defined.
- **Source Port** — Indicates the port from which the packets are mirrored.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
  - *RX* — Defines that the port is monitored for traffic received on this port.
  - *TX* — Defines that the port is monitored for traffic transmitted on this port.
  - *Both* — Defines that the port is monitored for both transmitted and received traffic.

- **Status** — Indicates if the port is currently monitored. The possible field values are:
  - *Active* — Indicates the port is currently monitored.
  - *notReady* — Indicates the port is not currently monitored.

2. Click **Add**. The *Add Port Mirroring Page* opens:

Figure 63: Add Port Mirroring Page



Add Port Mirroring

Unit No.	1
Source Port	1/e1
Type	Tx Only

The *Add Port Mirroring Page* contains the following fields:

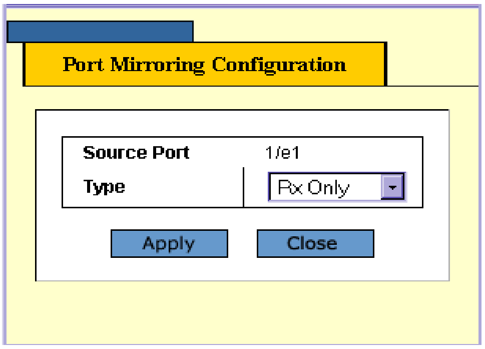
- **Unit Number**— Displays the stacking member for which the port is defined.
- **Source Port** — Defines the port from which traffic is to be analyzed.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
  - *Rx Only* — Defines the port mirroring on receiving ports.
  - *Tx Only* — Defines the port mirroring on transmitting ports. This is the default value.
  - *Tx and Rx* — Defines the port mirroring on both receiving and transmitting ports.

3. Click **Apply**. The port mirror status indicators are updated.
4. Click **Save Config** on the menu to permanently save the change.

To modify or delete a port mirror:

1. Click **Layer 1 > Port Mirroring**. The *Port Mirroring Page* opens.
2. Click **Modify**. The *Port Mirroring Configuration* opens.

Figure 64: Port Mirroring Configuration



Port Mirroring Configuration

Source Port	1/e1
Type	Rx Only

3. Define the *Type* field.
4. Click **Apply**. The Port mirroring is modified, and the device is updated.
5. Click **Save Config** on the menu to permanently save the change.

Aggregating Ports

Link Aggregation optimizes port usage by linking a group of ports together to form a single trunk. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy. The device supports both static trunks and *Link Aggregation Control Protocol* (LACP) trunks. LACP trunks negotiate aggregating port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a trunk between them.

Ensure the following:

- All ports within a trunk must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different trunk.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the trunk have the same ingress filtering and tagged modes.
- All ports in the trunk have the same back pressure and flow control modes.
- All ports in the trunk have the same priority.
- All ports in the trunk have the same transceiver type.
- The device supports up to eight trunks, and eight ports in each trunk.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured trunk.
- Ports added to a trunk lose their individual port configuration. When ports are removed from the trunk, the original port configuration is applied to the ports.

This section contains the following procedures for configuring static port trunks on the device.

- Defining Trunk Settings
- Defining Port Trunking
- Configuring LACP

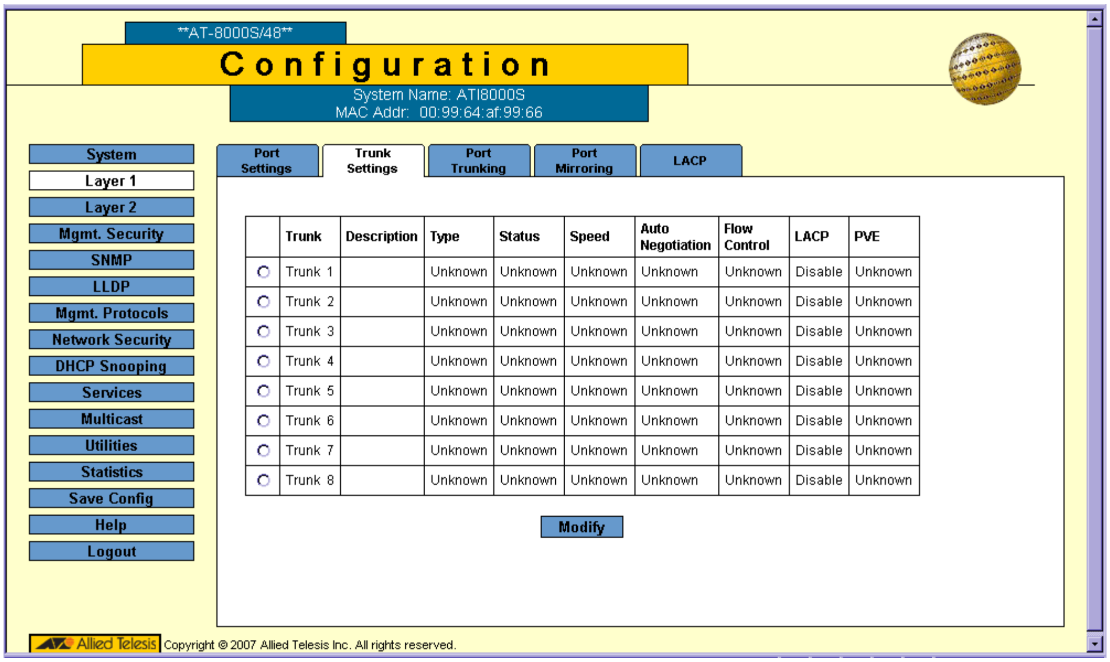
Defining Trunk Settings

The *Trunk Settings Page* contains parameters for defining Trunks.

To define a port trunk:

1. Click **Layer 1 > Trunk Settings**. The *Trunk Settings Page* opens:

Figure 65: Trunk Settings Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

	Trunk	Description	Type	Status	Speed	Auto Negotiation	Flow Control	LACP	PVE
○	Trunk 1		Unknown	Unknown	Unknown	Unknown	Unknown	Disable	Unknown
○	Trunk 2		Unknown	Unknown	Unknown	Unknown	Unknown	Disable	Unknown
○	Trunk 3		Unknown	Unknown	Unknown	Unknown	Unknown	Disable	Unknown
○	Trunk 4		Unknown	Unknown	Unknown	Unknown	Unknown	Disable	Unknown
○	Trunk 5		Unknown	Unknown	Unknown	Unknown	Unknown	Disable	Unknown
○	Trunk 6		Unknown	Unknown	Unknown	Unknown	Unknown	Disable	Unknown
○	Trunk 7		Unknown	Unknown	Unknown	Unknown	Unknown	Disable	Unknown
○	Trunk 8		Unknown	Unknown	Unknown	Unknown	Unknown	Disable	Unknown

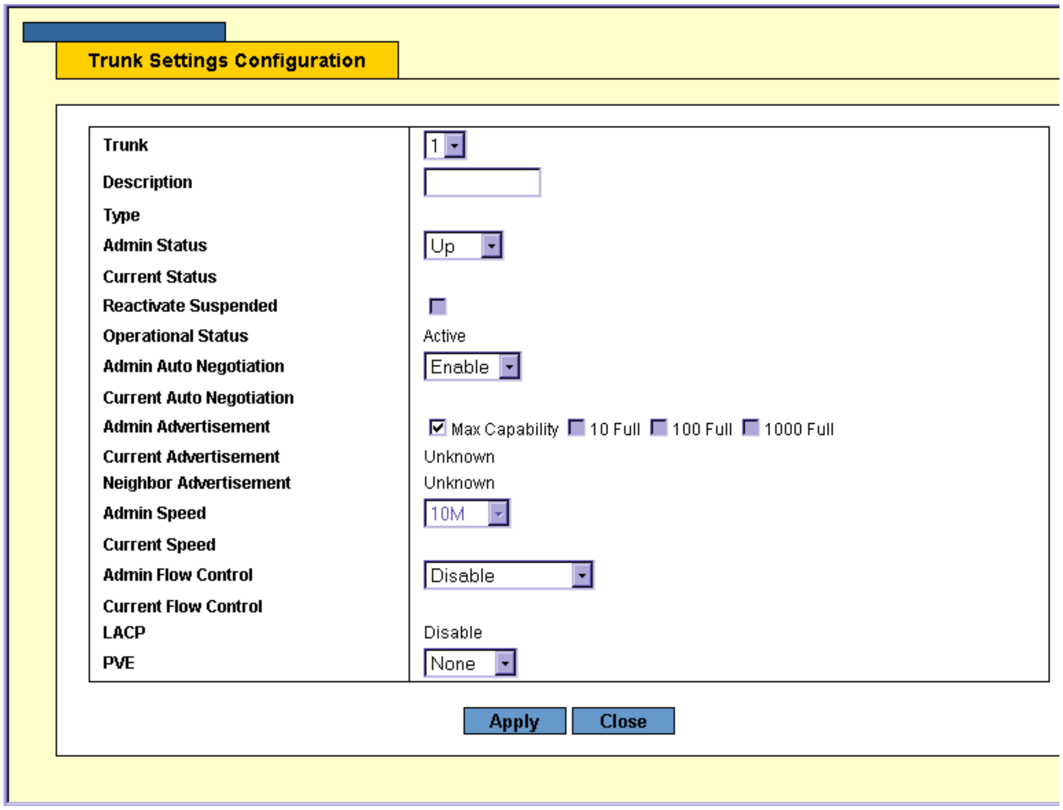
The *Trunk Settings Page* displays information about the currently defined trunks and contains the following fields:

- **Trunk** — Displays the trunk name.
- **Description** — Displays the user-defined trunk name and/or description.
- **Type** — Indicates the type of trunk defined by the first port assigned to the trunk. For example, 100-Copper, or 100-Fiber.
- **Status** — Indicates if the trunk is currently linked. The possible field values are:
  - *Up* — Indicates the trunk is currently linked, and is forwarding or receiving traffic.
  - *Down* — Indicates the trunk is not currently linked, and is not forwarding or receiving traffic.
- **Speed** — Displays the configured aggregated rate for the trunk. The possible field values are:
  - *10* — Indicates the trunk is currently operating at 10 Mbps.
  - *100* — Indicates the trunk is currently operating at 100 Mbps.
  - *1000* — Indicates the trunk is currently operating at 1000 Mbps.
- **Auto Negotiation** — Displays the auto negotiation status of the trunk. Auto negotiation is a protocol between two link partners that enables a port to advertise its transmission rate and flow control abilities to its partner.

- **Flow Control** — Displays the flow control status of the trunk.
- **LACP** — Indicates if LACP is enabled on the trunk. The possible values are:
  - *Enable* — LACP is enabled on the trunk.
  - *Disable* — LACP is disabled on the trunk.
- **PVE** — Enables a port to be a *Private VLAN Edge* (PVE) port. When a port is defined as PVE, it bypasses the Forwarding Database (FDB), and forwards all Unicast, Multicast and Broadcast traffic to an uplink (except MAC-to-me packets). Traffic from the uplink is distributed to all interfaces.

2. Click **Modify**. The *Trunk Setting Configuration Page* opens:

Figure 66: Trunk Setting Configuration Page



Trunk Settings Configuration

Trunk	1
Description	
Type	
Admin Status	Up
Current Status	
Reactivate Suspended	□
Operational Status	Active
Admin Auto Negotiation	Enable
Current Auto Negotiation	
Admin Advertisement	☑ Max Capability □ 10 Full □ 100 Full □ 1000 Full
Current Advertisement	Unknown
Neighbor Advertisement	Unknown
Admin Speed	10M
Current Speed	
Admin Flow Control	Disable
Current Flow Control	
LACP	Disable
PVE	None

The *Trunk Setting Configuration Page* contains the following fields:

- **Trunk—** Lists the names of configured trunks.
- **Description —** Provides a user-defined trunk description.
- **Type —** Indicates the type of trunk.
- **Admin Status** — Displays the link administrative status. Changes to the trunk state are active only after the device is reset. The possible field values are:
  - *Up* **—** Indicates that the trunk is currently operating.
  - *Down* **—** Indicates that the trunk is currently not operating.

- **Current Status —** Indicates whether the trunk is currently operational or non-operational. The possible field values are:
  - *Up* — Indicates the trunk is currently operating.
  - *Down* — Indicates the trunk is currently not operating.
- **Reactivate Suspended —** Reactivates suspended trunks. The possible field values are:
  - *Checked* **—** Reactivates the selected suspended trunk.
  - *Unchecked* **—** Maintains the trunk status. This is the default value.
- **Operational Status** — Indicates the trunk operational status. Possible field values are:
  - *Suspended* — The trunk is currently active, and is not receiving or transmitting traffic.
  - *Active* — Indicates the trunk is currently active and is receiving and transmitting traffic.
  - *Disable* — Indicates the trunk is currently disabled, and is not receiving or transmitting traffic.
- **Admin Auto Negotiation —** Displays the auto negotiation status of the trunk. Auto negotiation is a protocol between two link partners that enables a port to advertise its transmission rate and flow control abilities to its partner.
- **Current Auto Negotiation —** Displays the current Auto Negotiation setting.
- **Admin Advertisement —** Defines the auto negotiation setting the trunk advertises. The possible field values are:
  - *Max Capability* — Indicates trunk speeds.
  - *10 Full* — Indicates that the trunk advertises for a 10 Mbps speed trunk.
  - *100 Full* — Indicates that the trunk advertises for a 100 Mbps speed trunk.
  - *1000 Full* — Indicates that the trunk advertises for a 1000 Mbps speed trunk.
- **Current Advertisement —** Indicates the trunk advertises its speed to its neighbor trunk to start the negotiation process. The possible field values are those specified in the Admin Advertisement field.
- **Neighbor Advertisement** — Indicates the neighboring trunk's advertisement settings. The field values are identical to the Admin Advertisement field values.
- **Admin Speed —** Indicates the configured rate for the trunk. The trunk type determines the speed settings available. Trunk speeds can only be configured when auto-negotiation is disabled. The possible field values are:
  - *10M* — Indicates the trunk is currently operating at 10 Mbps.
  - *100M* — Indicates the trunk is currently operating at 100 Mbps.
  - *1000M* — Indicates the trunk is currently operating at 1000 Mbps.
- **Current Speed** — Displays the configured rate for the trunk.
- **Admin Flow Control —** Displays the flow control status on the trunk.
  - *Enable* — Indicates that flow control is currently enabled for the selected trunk.
  - *Disable* — Indicates that flow control is currently disabled for the selected trunk. This is the default value.
- **Current Flow Control** — Displays the current Flow Control setting.
- **LACP** — Indicates if LACP is enabled on the trunk. The possible values are:
  - *Enabled* — LACP is enabled on the trunk.
  - *Disabled* — LACP is disabled on the trunk.
- **PVE** — Enables a port to be a *Private VLAN Edge* (PVE) port. When a port is defined as PVE, it bypasses the Forwarding Database (FDB), and forwards all Unicast, Multicast and Broadcast traffic to an uplink (except MAC-to-me packets). Traffic from the uplink is distributed to all interfaces.

3. Modify the fields.
4. Click **Apply**. The Trunk settings are saved and the device is updated.

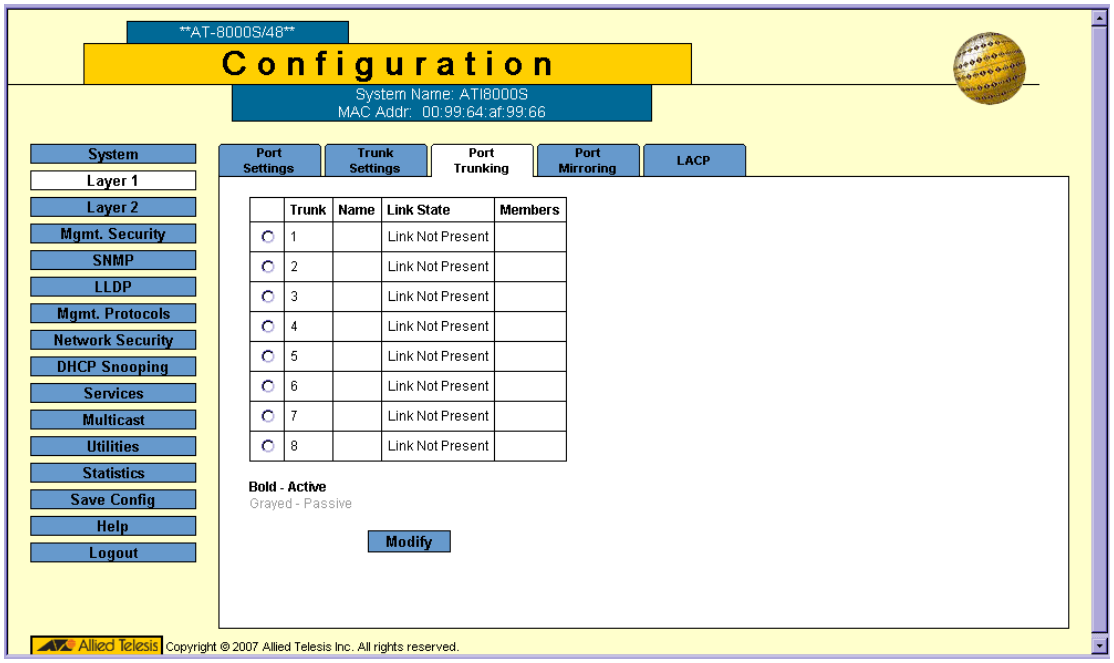
Defining Port Trunking

The *Port Trunking Page* contains information about all port trunks currently defined on the device.

To modify Port Trunking settings:

1. Click **Layer 1 > Port Trunking**. The *Port Trunking Page* opens:

Figure 67: Port Trunking Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

	Trunk	Name	Link State	Members
○	1		Link Not Present	
○	2		Link Not Present	
○	3		Link Not Present	
○	4		Link Not Present	
○	5		Link Not Present	
○	6		Link Not Present	
○	7		Link Not Present	
○	8		Link Not Present	

Bold - Active
Grayed - Passive

Copyright © 2007 Allied Telesis Inc. All rights reserved.

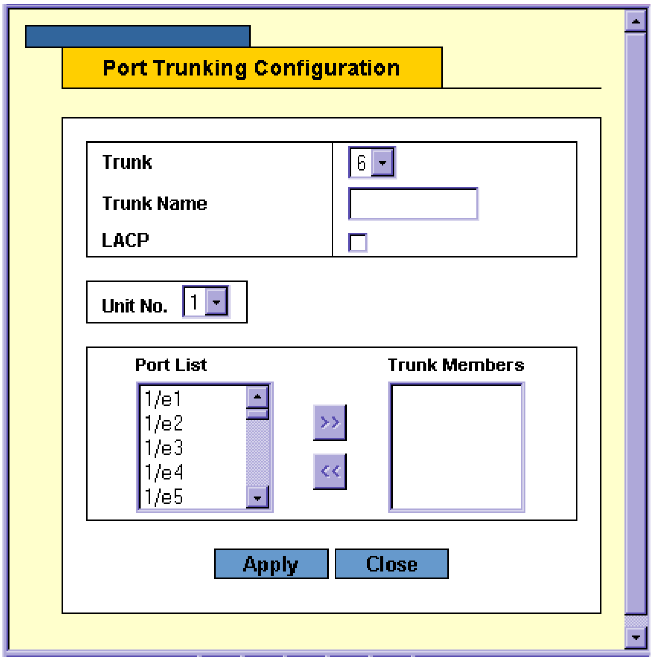
The following information is displayed:

- **Trunk** — Displays the ID number of the trunk.
- **Name** — Displays the name of the trunk. The name can be up to sixteen alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must be given a unique name.
- **Link State** — Indicates the current link status.
- **Members** — Indicates the ports which are defined for the trunk.

2. Select the trunk to modify.

3. Click **Modify**. The *Port Trunking Configuration Page* opens:

Figure 68: Port Trunking Configuration Page



Port Trunking Configuration

Trunk: 6
Trunk Name:
LACP: □

Unit No.: 1

Port List: 1/e1, 1/e2, 1/e3, 1/e4, 1/e5
Trunk Members:

In addition to the fields in the The *Port Trunking Page*, the *Port Trunking Configuration Page* contains the following additional field:

- **Unit Number** — Displays the stacking member for which the port trunking parameters are defined.
- **LACP** — Indicates if LACP is enabled on the trunk. The possible field values are:
  - *Checked* — Enables LACP on the trunk.
  - *Unchecked* — Disables LACP on the trunk. This is the default value.

4. Modify the *Trunk*, *LACP, Unit Number, and Trunk Name* fields.
5. Select the ports for the trunk from the *Port List* using the >> arrow. The selected ports are displayed as *Trunk Members*.
6. Click **Apply**. Trunking information is modified and the device is updated.
7. Click **Save Config** in the *Trunk Settings Page* menu to permanently save the changes.

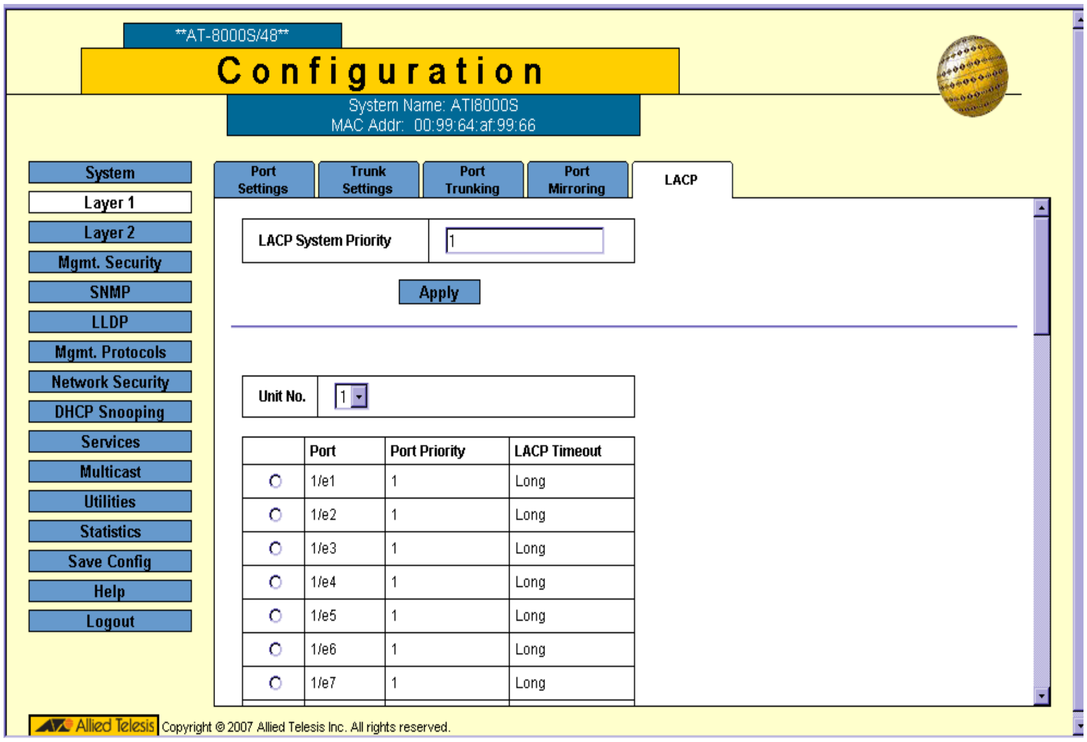
Configuring LACP

Trunk ports can contain different media types if the ports are operating at the same speed. Aggregated links can be set up manually or automatically established by enabling *Link Aggregation Control Protocol* (LACP) on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed. The *LACP Page* contains fields for configuring LACP trunks.

To configure LACP for trunks:

1. Click **Layer 1 > LACP**. The *LACP Page* opens:

Figure 69: LACP Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

LACP System Priority	1

Unit No.	1

	Port	Port Priority	LACP Timeout
○	1/e1	1	Long
○	1/e2	1	Long
○	1/e3	1	Long
○	1/e4	1	Long
○	1/e5	1	Long
○	1/e6	1	Long
○	1/e7	1	Long

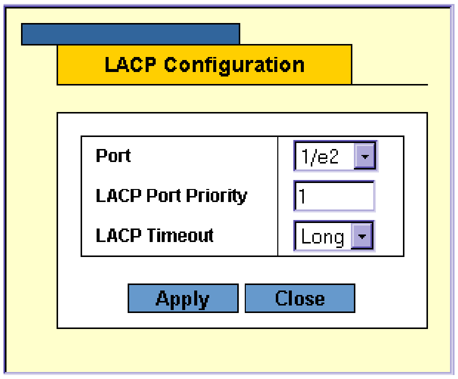
Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *LACP Page* contains the following fields:

- **LACP System Priority** — Specifies system priority value. The field range is 1-65535. The field default is 1.
- **Unit Number** — Displays the stacking member for which the trunk parameters are defined.
- **Port** — Displays the port number to which timeout and priority values are assigned.
- **Port Priority** — Displays the LACP priority value for the port. The field range is 1-65535.
- **LACP Timeout** — Displays the administrative LACP timeout. The following options are available: *Short* and *Long* (default).

2. Click **Modify**. the *LACP Configuration Page* opens:

Figure 70: LACP Configuration Page



LACP Configuration

Port	1/e2
LACP Port Priority	1
LACP Timeout	Long

3. Define the fields.
4. Click **Apply**. The LACP settings are saved and the device is updated.

Chapter 8. Configuring Interfaces

This section contains information on configuring the interfaces of the device.

This section describes the following topics:

- Defining MAC Addresses
- Configuring VLANs
- Defining MAC Based Groups

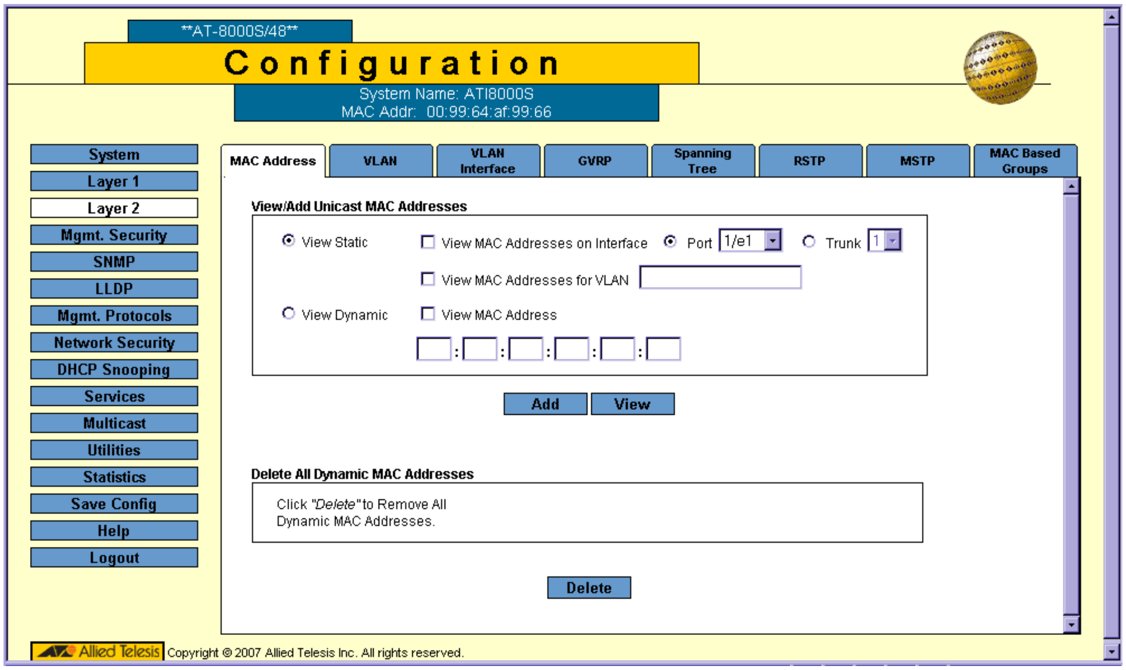
Defining MAC Addresses

The *MAC Address Page* contains parameters for querying information in the Static MAC Address Table and the Dynamic MAC Address Table, in addition to viewing and configuring Unicast addresses. The MAC Address tables contain address parameters by which packets are directly forwarded to the ports and can be sorted by interface, VLAN, and MAC Address.

To configure MAC addresses:

1. Click **Layer 2 > MAC Address**. The *MAC Address Page* opens:

Figure 71: MAC Address Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

● View Static
○ View Dynamic
□ View MAC Addresses on Interface ● Port 1/e1 ○ Trunk 1
□ View MAC Addresses for VLAN
□ View MAC Address

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

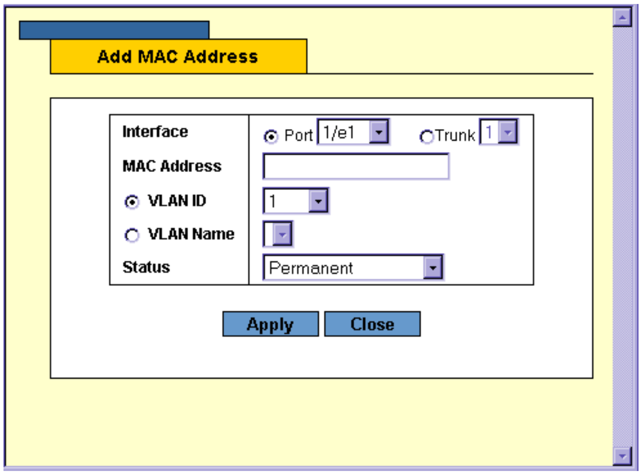
Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *MAC Address Page* contains the following fields:

- **View Static** — Displays the static addresses assigned to the ports on the device.
- **View Dynamic** — Displays the dynamic addresses learned on the ports on the device.
- **View MAC Addresses on Interface** — Displays the port's or trunk's dynamic or static MAC addresses.
- **View MAC Addresses for VLAN** — Displays the static or dynamic addresses learned on the tagged and untagged ports of a specific VLAN. You specify the VLAN by entering the VLAN ID. Only one VLAN at one time can be defined.
- **View MAC Address** — Displays the number of the port on which a MAC address was assigned or learned. To find out on which port a particular MAC address was learned, even if the device is part of a large network, specify the MAC address. The system automatically locates the port that is connected to the device.
- **Delete All Dynamic MAC Addresses** — Clicking **Delete** removes all dynamic addresses from the MAC Address Table.

2. Define the fields for the Unicast or Multicast MAC addresses to add.
3. Click **Add**. The *Add MAC Address Page* opens:

Figure 72: Add MAC Address Page



Add MAC Address

Interface ● Port 1/e1 ○ Trunk 1
MAC Address
● VLAN ID 1
○ VLAN Name
Status Permanent

The *Add MAC Address Page* contains the following fields:

- **Interface** — Indicates the port or trunk on which the address was learned or assigned.
- **MAC Address** —Defines the static Unicast MAC address.
- **VLAN ID** — Displays the VLAN ID number to which the entry refers.
- **VLAN Name** — Displays the VLAN name to which the entry refers.
- **Status** — Indicates the current status of the address. The possible values are:
  - *Permanent* — The MAC address is permanent.
  - *Delete on Reset* — The MAC address is deleted when the device is reset.
  - *Delete on Timeout* — The MAC address is deleted when a timeout occurs.
  - *Secure Options* — The MAC Address is defined for locked ports.

Note

When viewed, the information also includes the *Type* of the address: static or dynamic.

4. Click **Apply**. The new MAC address is added to the addresses table and the device information is updated.

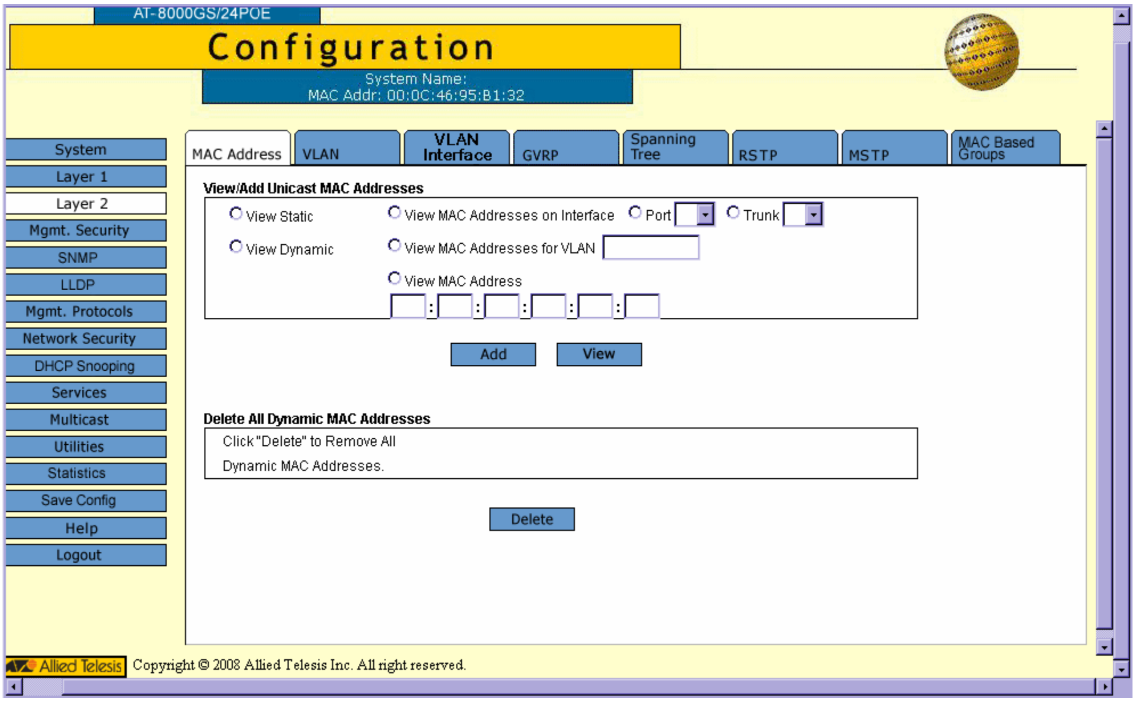
To delete all MAC addresses:

1. Click **Layer 2 > MAC Address**. The *MAC Address Page* opens.
2. Click **Delete** in the *Delete All MAC Address*s section of the *MAC Address Page*. All addresses are cleared from the Dynamic MAC Address Table and the device begins to learn new addresses as packets arrive on the ports.

To view or remove static MAC addresses:

1. Click **Layer 2 > MAC Address**. The *MAC Address Page* opens.
2. Click **View**. Depending on whether View Static or View Dynamic is chosen, the *View Static MAC Address Table Page* or *View Dynamic MAC Address Table Page* opens:

Figure 73: View Static MAC Address Table Page



Click "Delete" to Remove All Dynamic MAC Addresses.

Copyright © 2008 Allied Telesis Inc. All right reserved.

The *View Static MAC Address Table Page* and or *View Dynamic MAC Address Table Page* display all static or dynamic MAC addresses, respectively.

3. Click the radio button to select a *VLAN ID*.
4. Click **Delete**. The MAC Address is deleted from the list (applicable to Static addresses only).
5. Click **Refresh**. The MAC Address information is updated.
6. Click **Close**. The *MAC Address Page* is displayed.

Configuring VLANs

This section describes how to create and configure Virtual LANs (VLANs).

VLANs are logical subgroups within a Local Area Network (LAN) which combine user stations and network devices into a single unit, regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs use software to reduce the amount of time it takes for network changes, additions, and moves to be implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, or through any other logical connection combination, since they are software-based and not defined by physical attributes.

VLANs function at Layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router working at a protocol level is required to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are Broadcast and Multicast domains. Broadcast and Multicast traffic is transmitted only in the VLAN in which the traffic is generated. VLAN tagging provides a method of transferring VLAN information between VLAN-aware devices. VLAN tagging attaches a 4-byte tag to frame headers. The VLAN tag indicates to which VLAN the frames belong. VLAN tags are attached to the VLAN by either the end station or the network device. VLAN tags also contain VLAN network priority information.

Combining VLANs and *Generic Attribute Registration Protocol* (GARP) allows network managers to define network nodes into Broadcast domains.

When configuring VLANs ensure the following:

- When using this feature, the management VLAN must exist on each AT-S94 Series device that you want to manage.
- The uplink and downlink ports on each device that are functioning as the tagged or untagged data links between the devices must be either tagged or untagged members of the management VLAN.
- The port on the device to which the management station is connected must be a member of the management VLAN.

This section contains the following topics:

- Defining VLAN Properties
- Defining VLAN Interface Settings
- Defining GVRP

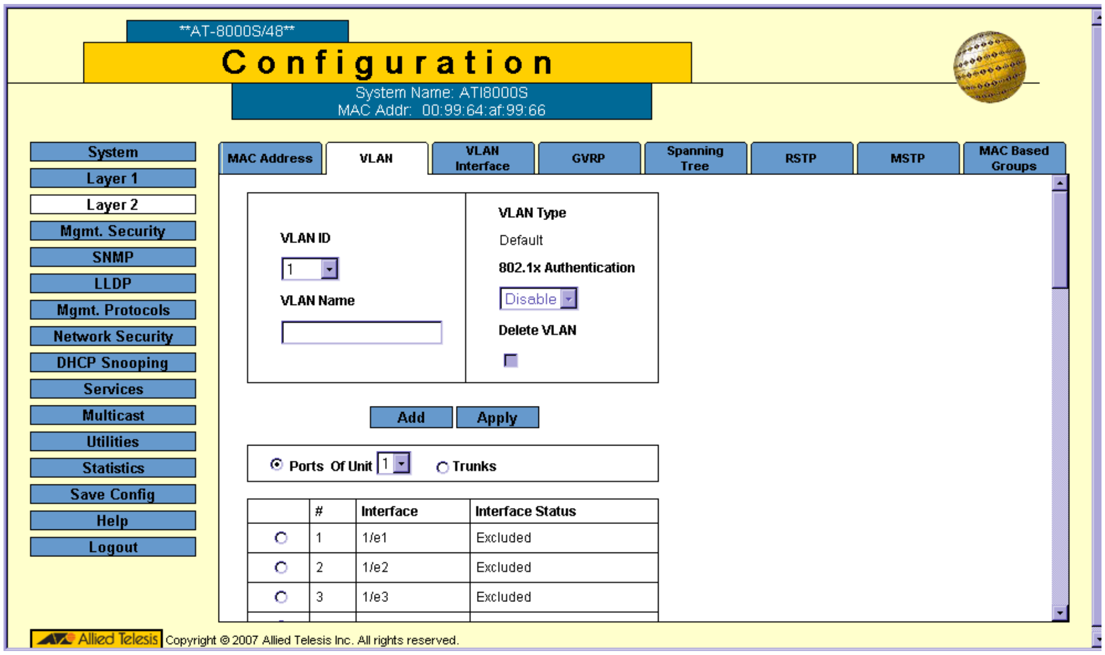
Defining VLAN Properties

The *VLAN Page* provides information and global parameters for configuring and working with VLANs.

To configure a VLAN:

1. Click **Layer 2 > VLAN**. The *VLAN Page* opens:

Figure 74: VLAN Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

VLAN ID: 1

VLAN Name:

VLAN Type: Default

802.1x Authentication: Disable

Delete VLAN ☐

● Ports Of Unit 1 ○ Trunks

	#	Interface	Interface Status
○	1	1/e1	Excluded
○	2	1/e2	Excluded
○	3	1/e3	Excluded

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *VLAN Page* is divided into two sections. The first section contains the following fields:

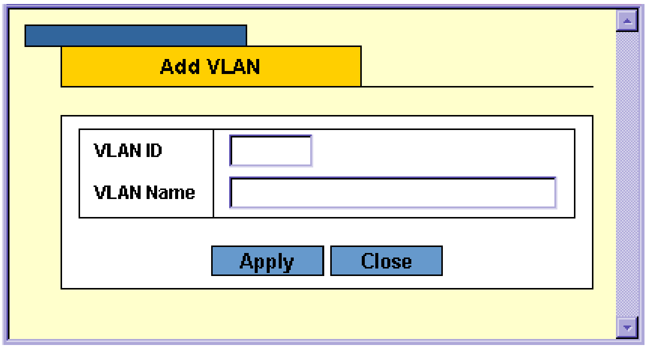
- **VLAN ID** — Defines the VLAN ID. Possible VLAN IDs are 1-4095, in which “1” is reserved for the default VLAN, and “4095” is reserved as the “discard” VLAN.
- **VLAN Name** — Displays the user-defined VLAN name.
- **VLAN Type** — Displays the VLAN type. The possible field values are:
  - *Dynamic* — Indicates the VLAN was dynamically created through GARP.
  - *Static* — Indicates the VLAN is user-defined.
  - *Default* — Indicates the VLAN is the default VLAN.
- **802.1x Authentication** — Enables the 802.1x authentication method on the VLAN. The possible field values are:
  - *Enable* — Enables 802.1x authentication.
  - *Disable* — Disables 802.1x authentication. This is the default value.
- **Delete VLAN** — Removes the specified VLAN. The possible field values are:
  - *Checked* — Deletes the specified VLAN.
  - *Unchecked* — Maintains the specified VLAN.

The second section contains a table that maps VLAN parameters to ports.

- Select the interfaces displayed in the table.
  - *Ports of Unit* — Specifies the port and stacking member for which the VLAN mapping is displayed.
  - *Trunks* — Specifies the trunk for which the VLAN mapping is displayed.
- **Interface Status** — Indicates the interface's membership status in the VLAN. The possible field values are:
  - *Tagged* — Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
  - *Untagged* — Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged. In the default VLAN, this is the default value for all interfaces.
  - *Excluded* — Indicates that the port is excluded from the VLAN.
  - *Forbidden* — Indicates that the port cannot be included in the VLAN.

2. Click the **Add** button. The *Add VLAN Page* opens:

Figure 75: Add VLAN Page



Add VLAN

VLAN ID

VLAN Name

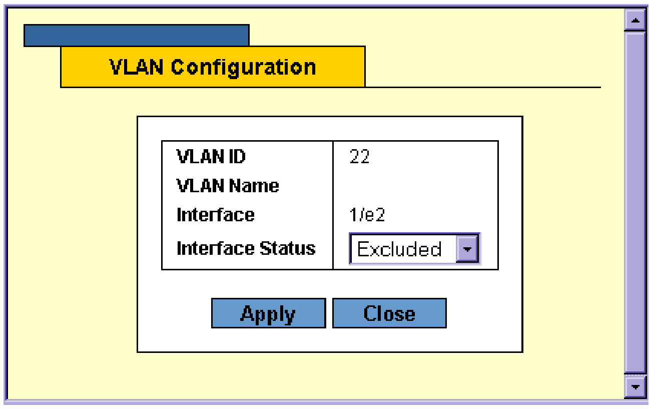
3. Define the fields.
4. Click **Apply**. The VLAN is created, and the device is updated.

To modify VLAN settings:

1. Click **Layer 2 > VLAN**. The *VLAN Page* opens:
2. Select a VLAN from the table.

3. Click **Modify**. The *VLAN Configuration* opens.

Figure 76: VLAN Configuration



VLAN ID	22
VLAN Name	
Interface	1/e2
Interface Status	Excluded

4. Change the **Interface Status** setting.
5. Click **Apply**. The VLAN configuration is modified, and the device is updated.
6. Click **Save Config** on the menu to permanently save the change.

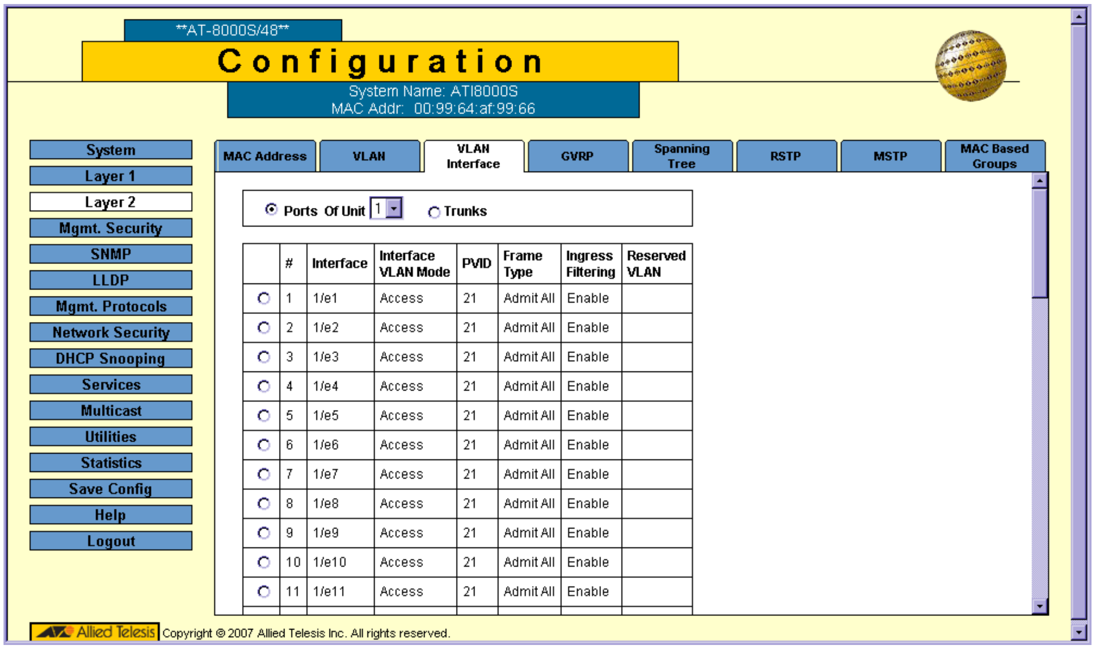
Defining VLAN Interface Settings

The *VLAN Interface Page* contains fields for managing ports that are part of a VLAN.

To define a VLAN interface:

1. Click **Layer 2 > VLAN Interface**. The *VLAN Interface Page* opens:

Figure 77: VLAN Interface Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

● Ports Of Unit 1 ○ Trunks

	#	Interface	Interface VLAN Mode	PVID	Frame Type	Ingress Filtering	Reserved VLAN
○	1	1/e1	Access	21	Admit All	Enable	
○	2	1/e2	Access	21	Admit All	Enable	
○	3	1/e3	Access	21	Admit All	Enable	
○	4	1/e4	Access	21	Admit All	Enable	
○	5	1/e5	Access	21	Admit All	Enable	
○	6	1/e6	Access	21	Admit All	Enable	
○	7	1/e7	Access	21	Admit All	Enable	
○	8	1/e8	Access	21	Admit All	Enable	
○	9	1/e9	Access	21	Admit All	Enable	
○	10	1/e10	Access	21	Admit All	Enable	
○	11	1/e11	Access	21	Admit All	Enable	

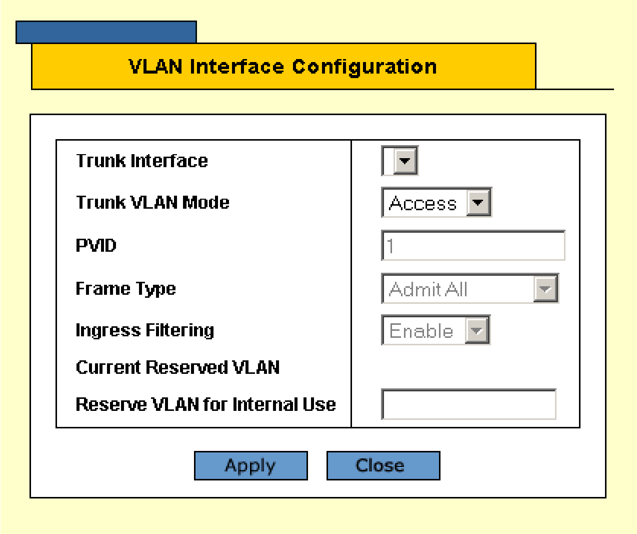
The *VLAN Interface Page* displays the VLAN interface information for a selected Port/Unit or Trunk:

- Select the interfaces displayed in the table.
  - *Ports of Unit* — Specifies the port and stacking member for which the VLAN mapping is displayed.
  - *Trunk* — Specifies the trunk for which the VLAN mapping is displayed.
- **Interface** — Displays the port or trunk number.
- **Interface VLAN Mode** — Indicates the port (or trunk) mode in the VLAN. The possible values are:
  - *General* — Indicates the port belongs to VLANs, and each VLAN's interface is user-defined as tagged or untagged (full IEEE802.1q mode).
  - *Access* — Indicates a port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port cannot be designated. Ingress filtering is always enabled for ports in Access mode.

   - *Trunk* — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that is untagged.
- **PVID** — Port Default VLAN ID. Assigns a VLAN ID to untagged packets. The possible values are 1-4094. VLAN 4095 is defined as per standard and industry practice as the Discard VLAN. Packets classified to the Discard VLAN are dropped.
- **Frame Type** — Specifies the packet type accepted on the port. The possible field values are:
   - *Admit Tag Only* — Only tagged packets are accepted on the port.
   - *Admit All* — Both tagged and untagged packets are accepted on the port.
- **Ingress Filtering** — Indicates whether ingress filtering is enabled on the port. The possible field values are:
   - *Enable* — Enables ingress filtering on the device. Ingress filtering discards packets that are defined to VLANs of which the specific port is not a member.
   - *Disable* — Disables ingress filtering on the device.
- **Reserved VLAN** — Indicates the VLAN that is currently reserved for internal use by the system.

2. Select an interface from the table.
3. Click **Modify**. The *VLAN Interface Configuration Page* opens:

Figure 78: VLAN Interface Configuration Page



Trunk Interface	
Trunk VLAN Mode	Access
PVID	1
Frame Type	Admit All
Ingress Filtering	Enable
Current Reserved VLAN	
Reserve VLAN for Internal Use	

In addition to the *VLAN Interface Page*, the *VLAN Interface Configuration Page* contains the following field:

- **Reserve VLAN for Internal Use** — Indicates which VLAN is reserved for internal use by the system. One VLAN must be reserved.

4. Define the fields.
5. Click **Apply**. The VLAN interface configuration is saved and the device is updated.
6. Click **Save Config** on the menu to permanently save the change.

Defining GVRP

The *GVRP Page* enables users to configure *GARP VLAN Registration Protocol* (GVRP) on the device. GVRP is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge and register VLAN membership.

In the *GVRP Page*, users can do the following tasks:

- Configuring GVRP
- Enabling/Disabling GVRP on a Port

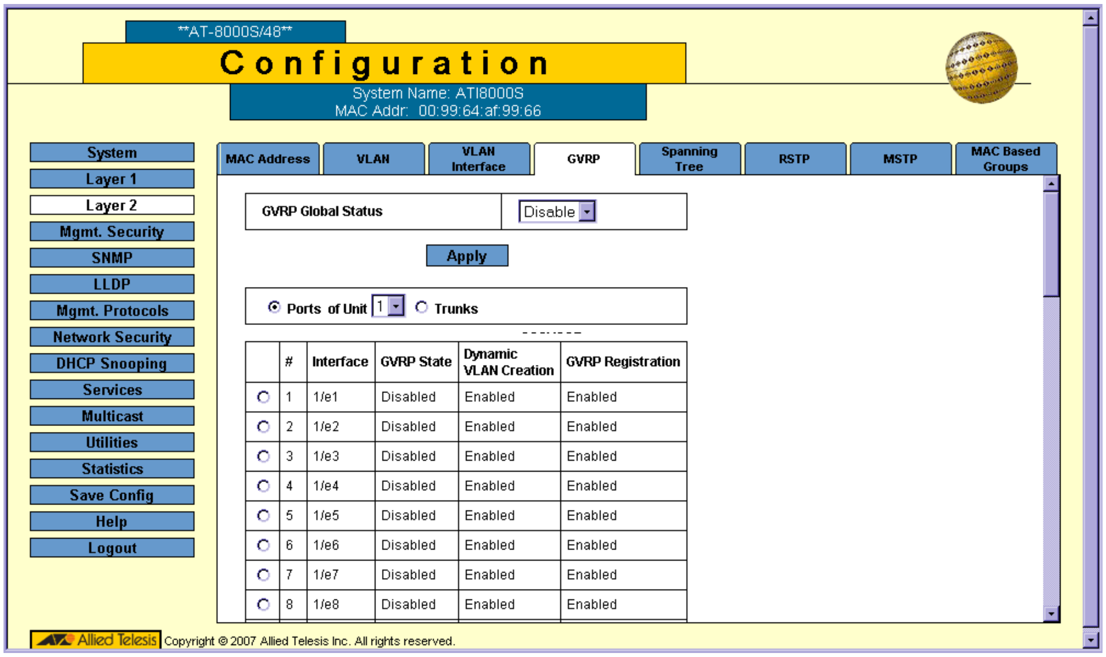
The settings for the three GVRP timers must be the same on all GVRP-active devices in your network. This is configurable only in the CLI, using the config-if **garp timer** command.

Configuring GVRP

To define GVRP on the device:

1. Click **Layer 2 > GVRP**. The *GVRP Page* opens:

Figure 79: GVRP Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

GVRP Global Status: Disable

● Ports of Unit 1 ○ Trunks

	#	Interface	GVRP State	Dynamic VLAN Creation	GVRP Registration
○	1	1/e1	Disabled	Enabled	Enabled
○	2	1/e2	Disabled	Enabled	Enabled
○	3	1/e3	Disabled	Enabled	Enabled
○	4	1/e4	Disabled	Enabled	Enabled
○	5	1/e5	Disabled	Enabled	Enabled
○	6	1/e6	Disabled	Enabled	Enabled
○	7	1/e7	Disabled	Enabled	Enabled
○	8	1/e8	Disabled	Enabled	Enabled

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *GVRP Page* contains the following fields:

- **GVRP Global Status** — Indicates if GVRP is enabled on the device. The possible field values are:
  - *Enable* — Enables GVRP on the selected device.
  - *Disable* — Disables GVRP on the selected device. This is the default value.
- Select the interfaces displayed in the table.
  - *Ports of Unit* — Specifies the port and stacking member for which the GVRP settings are displayed.

  - *Trunk* — Specifies the trunk for which the GVRP settings are displayed.
- **Interface** — Displays the port or trunk name on which GVRP is enabled.
- **GVRP State** — Indicates if GVRP is enabled on the port. The possible field values are:
  - *Enable* — Enables GVRP on the interface.
  - *Disable* — Disables GVRP on the interface.
- **Dynamic VLAN Creation —** Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
  - *Enable* — Enables Dynamic VLAN creation on the interface.
  - *Disable* — Disables Dynamic VLAN creation on the interface.
- **GVRP Registration —** Indicates if VLAN registration through GVRP is enabled on the interface. The possible field values are:
  - *Enable* — Enables GVRP registration on the device.
  - *Disable* — Disables GVRP registration on the device.

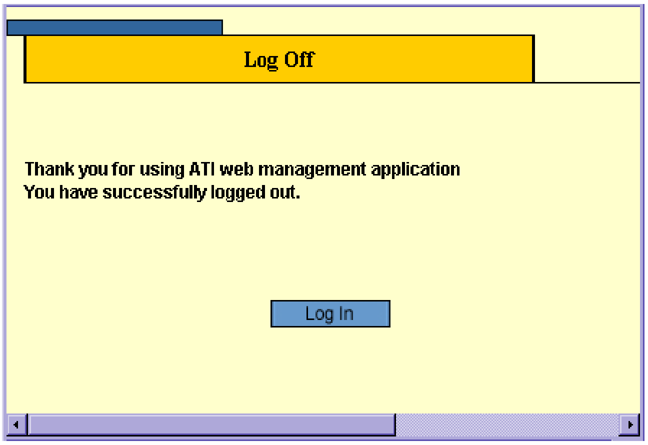
2. Select **Enable GVRP**.
3. Define the GVRP parameters.
4. Click **Apply**. The global GVRP parameters are saved and the device is updated.
5. Click **Save Config** on the menu to permanently save the change.

Enabling/Disabling GVRP on a Port

To enable or disable GVRP on ports:

1. Click **Layer 2 > GVRP**. The *GVRP Page* opens.
2. Select a *Port on Unit* or *Trunk*.
3. Click **Modify**. The *GVRP Configuration Page* opens:

Figure 80: GVRP Configuration Page



Log Off

Thank you for using ATI web management application
You have successfully logged out.

4. Select the interface (Port or Trunk).
5. Define the fields.
6. Click **Apply**. The change to the GVRP mode is activated on the selected interface.

Defining MAC Based Groups

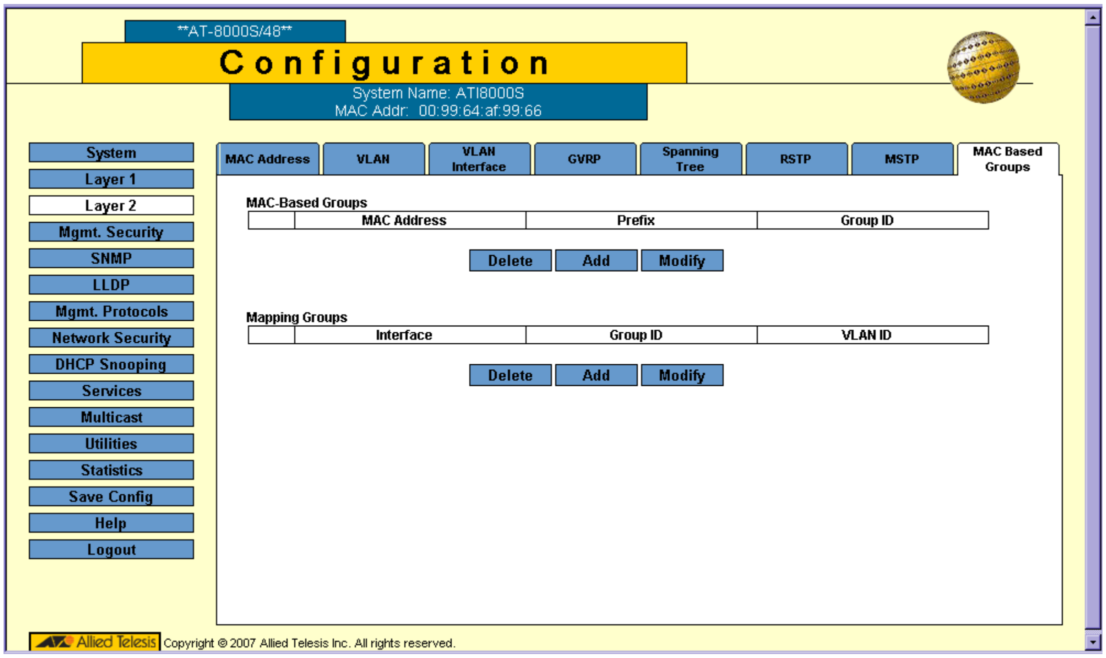
The *MAC Based Groups Page* allows network managers to group VLANs based on the VLAN MAC address, and to map groups to VLANs. For these purposes, the page contains two tables:

- MAC-Based Groups table
- Mapping Groups table

To define MAC Based Groups:

1. Click **Layer 2 > MAC Based Groups**. The *MAC Based Groups Page* opens:

Figure 81: MAC Based Groups Page



MAC-Based Groups

	MAC Address	Prefix	Group ID

Mapping Groups

	Interface	Group ID	VLAN ID

The *MAC Based Groups Page* contains the following fields:

MAC-Based Groups

In the MAC-Based Groups table, network managers group VLANs based on the VLAN MAC address.

- **MAC Address** — Displays the MAC address associated with the VLAN group.
- **Prefix** — Displays the MAC prefix associated with the MAC group.
- **Group ID** — Displays the VLAN Group ID.

Mapping Groups

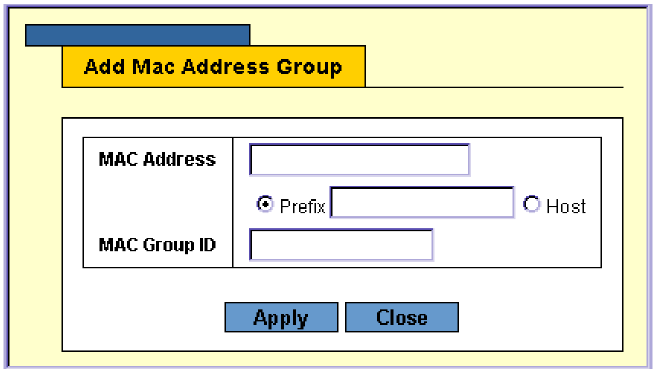
In the Mapping Groups table, network managers assign MAC groups to interfaces.

- **Interface** — Indicates the interface type to add to the VLAN group. The possible field values are:
  - *Port* — Indicates the specific port added to the VLAN group.

  - *Trunk* —Indicates the specific trunk added to the VLAN group.
- **Group ID** — Defines the MAC group ID to which the interface is added.
- **VLAN ID** — Attaches the interface to a user-defined VLAN ID. VLAN group ports can be attached to a VLAN ID. The possible field range is 1-4093, and 4095 (4094 is not available for configuration).

2. Below the MAC-Based Groups table, click the **Add** button. The *Add MAC Address Group Page* opens:

Figure 82: Add MAC Address Group Page



Add Mac Address Group

MAC Address ____

● Prefix ____ ○ Host

MAC Group ID ____

In addition to the fields in the *MAC Based Groups Page*, the *Add MAC Address Group Page* contains the following additional fields:

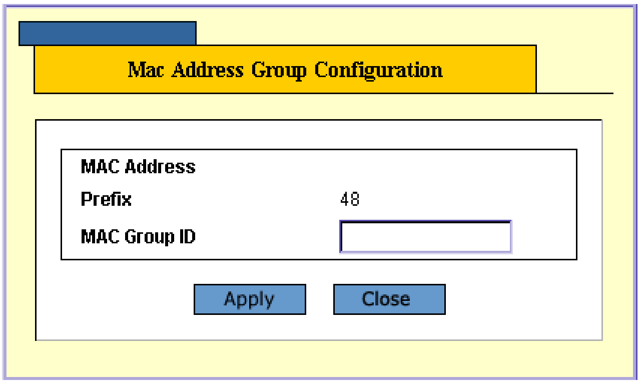
- **Host** — Defines the specified MAC address as the only address associated with the VLAN group.

3. Define the fields.
4. Click **Apply**. The MAC based VLAN group is defined, and the device is updated.

To modify MAC based group settings:

1. Click **Layer 2 > MAC Based Groups**. The *MAC Based Groups Page* opens:
2. Click **Modify**. The *MAC Address Group Configuration* opens.

Figure 83: MAC Address Group Configuration



Mac Address Group Configuration

MAC Address

Prefix 48

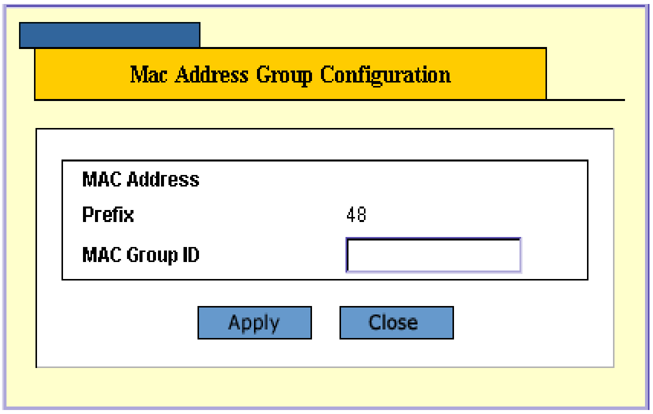
MAC Group ID ____

3. Modify the fields.
4. Click **Apply**. The MAC based VLAN group is modified, and the device is updated.
5. Click **Save Config** on the menu to permanently save the change.

To add a mapped group:

1. Click **Layer 2 > MAC Based Groups**. The *MAC Based Groups Page* opens:
2. Below the Mapping Group table, click the **Add** button. The *Add MAC Address Group Mappings Page* opens:

Figure 84: Add MAC Address Group Mappings Page



MAC Address
Prefix 48
MAC Group ID

In addition to the fields in the *MAC Based Groups Page*, the *Add MAC Address Group Mappings Page* contains the following additional fields:

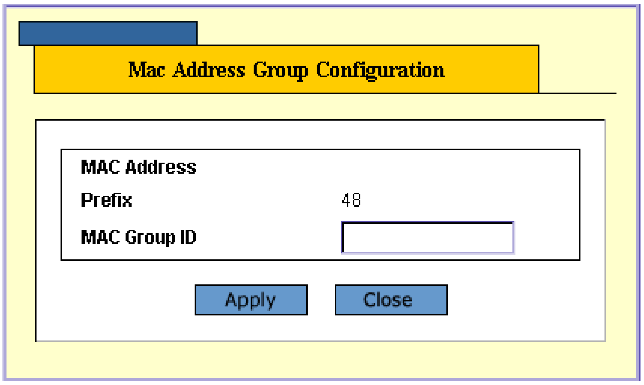
- **Group Type** – Indicates the VLAN Group to which interfaces are mapped. The possible field value is:
  – *MAC-based* – Indicates that interfaces are mapped to MAC based VLAN groups.

3. Select a VLAN to map with the group (*VLAN ID*).
4. Click **Apply**. The mapping group is added, and the device is updated.

To modify mapping group settings:

1. Click **Layer 2 > MAC Based Groups**. The *MAC Based Groups Page* opens:
2. Click **Modify**. The *MAC Address Group Mappings Configuration Page* opens.

Figure 85: MAC Address Group Mappings Configuration Page



MAC Address
Prefix 48
MAC Group ID

3. Change the mapped VLAN (*VLAN ID*).
   – Click **Apply**. The mapping group is modified, and the device is updated.

Chapter 9. Configuring System Logs

This section provides information for managing system logs. System logs enable viewing device events in real time and recording the events for later usage. System Logs record and manage events, and report errors and informational messages.

This section includes the following topics:

- Defining Log Settings
- Viewing Temporary and Flash Logs

Defining Log Settings

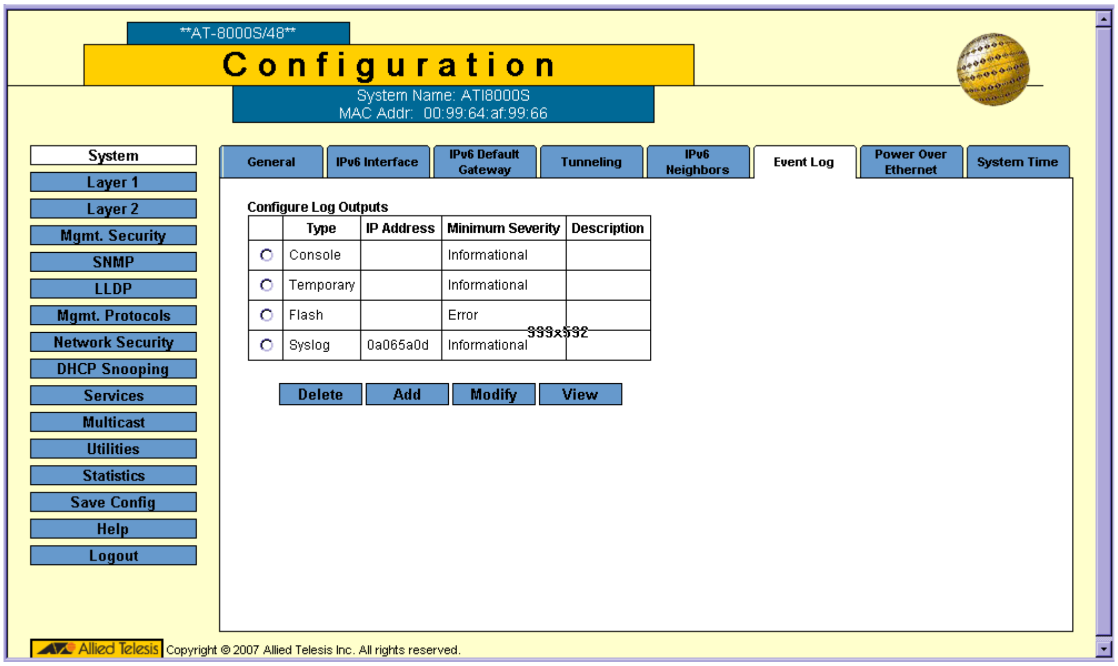
Event messages have a unique format, which is the Syslog protocols recommended message format for all error reporting. For example, Syslog and local device reporting messages are assigned a severity code and include a message mnemonic which identifies the source application generating the message. This allows messages to be filtered based on their urgency or relevancy. The message severity determines the set of event logging devices that are sent for each event message. The default severity for all logs is *Informational*, with the exception of logs in the Remote Log Server, which are *Error.*

The *Event Log Page* contains fields for defining which events are recorded to which logs. It contains fields for enabling logs globally and parameters for defining logs.

To view system log parameters:

1. Click **System > Event Log**. The *Event Log Page* opens:

Figure 86: Event Log Page



Configure Log Outputs

	Type	IP Address	Minimum Severity	Description
○	Console		Informational	
○	Temporary		Informational	
○	Flash		Error	
○	Syslog	0a065a0d	Informational	

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Configure Log Outputs* table displays the following log information:

- **Type** — Indicates the log type included in the output. The possible values are:
  - *Console* — Indicates that the output is of a console log.
  - *Temporary* — Indicates that the output is of the temporary memory log. *Temporary* logs are not available after reset.
  - *Flash* — Indicates that the output is of a Flash memory log. *Flash* logs are available after reset.
- **IP Address** — Displays the defined IP address of the syslog server.
- **Minimum Severity** — Indicates the defined minimum severity level.
- **Description** — Provides additional information about the syslog server.

Clearing Event Logs

To clear all events from the log:

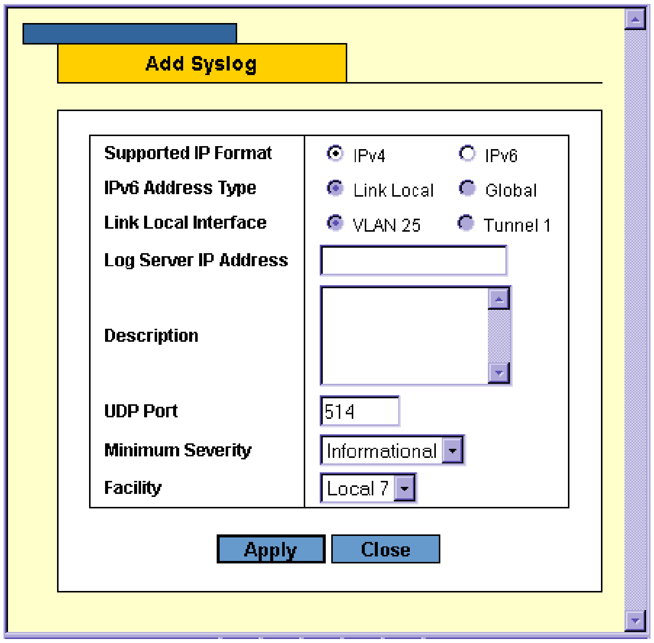
1. Click **System > Event Log**. The *Event Log Page* opens:
2. Click **Clear Logs**. The stored logs are cleared. If logging is enabled, the system begins to log new events.

Adding Log Servers

To add a log server:

1. Click **System > Event Log**. The *Event Log Page* opens.
2. Select a Log Type in the Configure Log Outputs table.
3. Click **Add**. The *Add Syslog Page* opens:

Figure 87: Add Syslog Page



Add Syslog

Supported IP Format	● IPv4	○ IPv6
IPv6 Address Type	● Link Local	○ Global
Link Local Interface	● VLAN 25	○ Tunnel 1
Log Server IP Address		
Description		
UDP Port	514	
Minimum Severity	Informational	
Facility	Local 7	

The *Add Syslog Page* contains the following fields:

- **Supported IP Format** — Indicates the supported Internet Protocol on the device. The possible field values are:
  - *IPv4* — Indicates that IPv4 is supported.
  - *IPv6* — Indicates that IPv6 is supported.
- **IPv6 Address Type** — Defines the type of configurable static IPv6 IP address for an interface. The possible values are:
  - *Link Local* — Defines a Link Local address; non routable and can be used for communication on the same network only. A Link Local address has a prefix of 'FE80'.
  - *Global* — Defines a globally unique IPv6 address; visible and reachable from different subnets.
- **Link Local Interface** — Indicates the type of Link Local interface. The possible values are:
  - *VLAN*
  - *Tunnel*
- **Log Server IP Address** — Defines the log server IP address.
- **Description** — Provides any additional information about the syslog server, for example, its location.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1-65535. The default value is 514.
- **Minimum Severity** — Indicates the minimum severity level to be included in the log output. All logs that have the severity higher than the minimum severity are also included in the output. When the minimum severity level is defined, logs of all higher severity levels are selected automatically.
- **Facility** — Defines an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are Local 0 - Local 7.

4. Define the fields.
5. Click **Apply**. The Log server is defined and the device is updated.

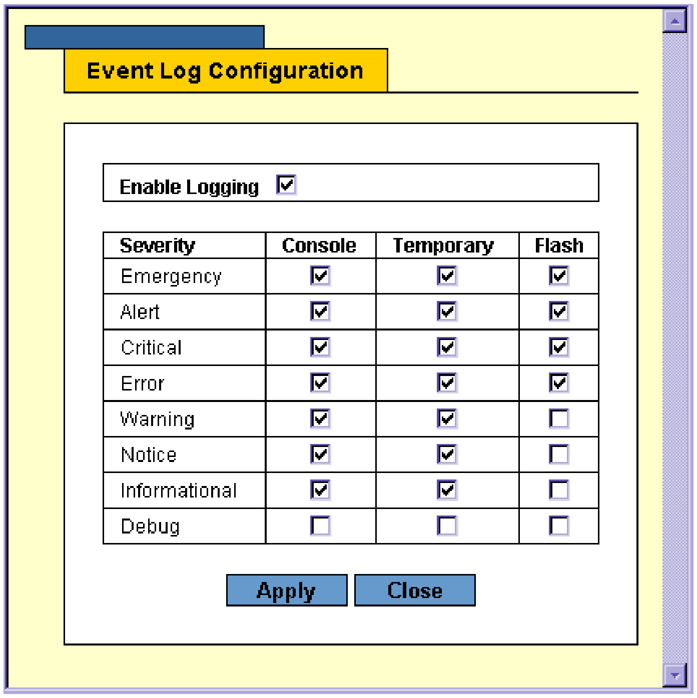
Modifying Log Servers

Clicking **Modify** opens the *Event Log Configuration Page*, in which administrators can modify Server Log entries.

To modify a Server Log entry:

1. Select the entry in the Log Table and click **Modify**. The *Event Log Configuration Page* opens.

Figure 88: Event Log Configuration Page



Enable Logging ☑

Severity	Console	Temporary	Flash
Emergency	☑	☑	☑
Alert	☑	☑	☑
Critical	☑	☑	☑
Error	☑	☑	☑
Warning	☑	☑	☐
Notice	☑	☑	☐
Informational	☑	☑	☐
Debug	☐	☐	☐

The *Event Log Configuration Page* contains the following fields:

- **Enable Logging** — Enables logging or disables event logging.
- **Severity** — Lists the minimum severity level per device or system-wide. The default severity for logging terminal, temporary and remote server is **Informational**. The default severity for logging to file is **Error**.
- **Console**, **Temporary** and/or **Flash** — Enables or disables device event logging to the severity indicated.

2. Define the relevant fields.
3. Click **Apply**. The Server Log configuration is updated in the Log Table. The device is updated.
4. Click **Save Config** in the *Event Log Page* menu to save the changes permanently.

Viewing Temporary and Flash Logs

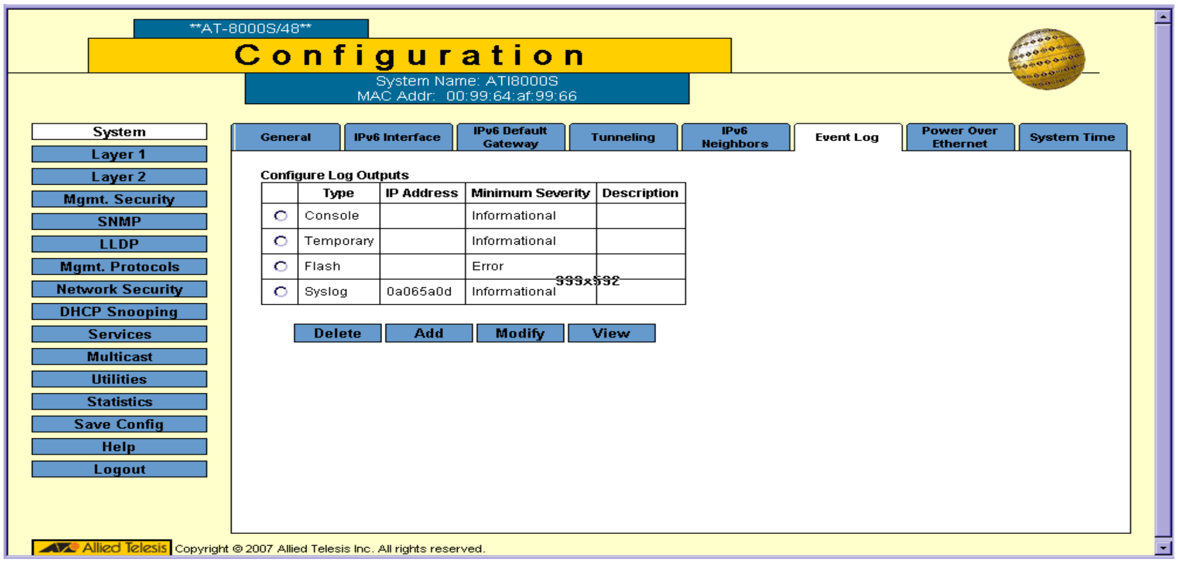
The *Temporary Log* and *View Flash Log Pages* contain information about log entries saved to the respective log files, including the time the log was generated, the log severity, and a description of the log message. The Flash log is available after reboot, but the Temporary log is deleted during reboot.

To display Flash logs:

1. Click **System > Event Log**. The *Event Log Page* opens.
2. In the **Configure Log Outputs** table, select a Temporary or Flash entry.

3. Click **View.** The selected log page opens:

Figure 89: View Flash Log Page



Configure Log Outputs

	Type	IP Address	Minimum Severity	Description
○	Console		Informational	
○	Temporary		Informational	
○	Flash		Error	
○	Syslog	0a065a0d	Informational	

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *View Flash Log Page* and *View Temporary Log Page* list the following information:

- **Log Index** —The log index number.
- **Log Time** — The date and time that the log was entered.
- **Severity** — The severity of the event for which the log entry was created.
- **Description** — The event details.

To clear memory logs:

1. Click **Clear Logs**. Logs are removed from the table.
2. Click **Close**. The *Event Log Page* is displayed.

Chapter 10.Configuring Spanning Tree

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides a single path between end stations on a network, eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The device supports the following STP versions:

- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops. For more information on configuring Classic STP, see *Configuring Classic Spanning Tree*.
- **Rapid STP** — Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops. For more information on configuring Rapid STP, see *Configuring Rapid Spanning Tree*.
- **Multiple STP** — Provides various load balancing scenarios. For example, if port A is blocked in one STP instance, the same port can be placed in the *Forwarding State* in another STP instance. For more information on configuring Multiple STP, see *Configuring Multiple Spanning Tree*.

This section contains the following topics:

- Configuring Classic Spanning Tree
- Configuring Rapid Spanning Tree
- Configuring Multiple Spanning Tree

Configuring Classic Spanning Tree

This section contains the following topics:

- Defining STP Properties
- Defining STP Interfaces

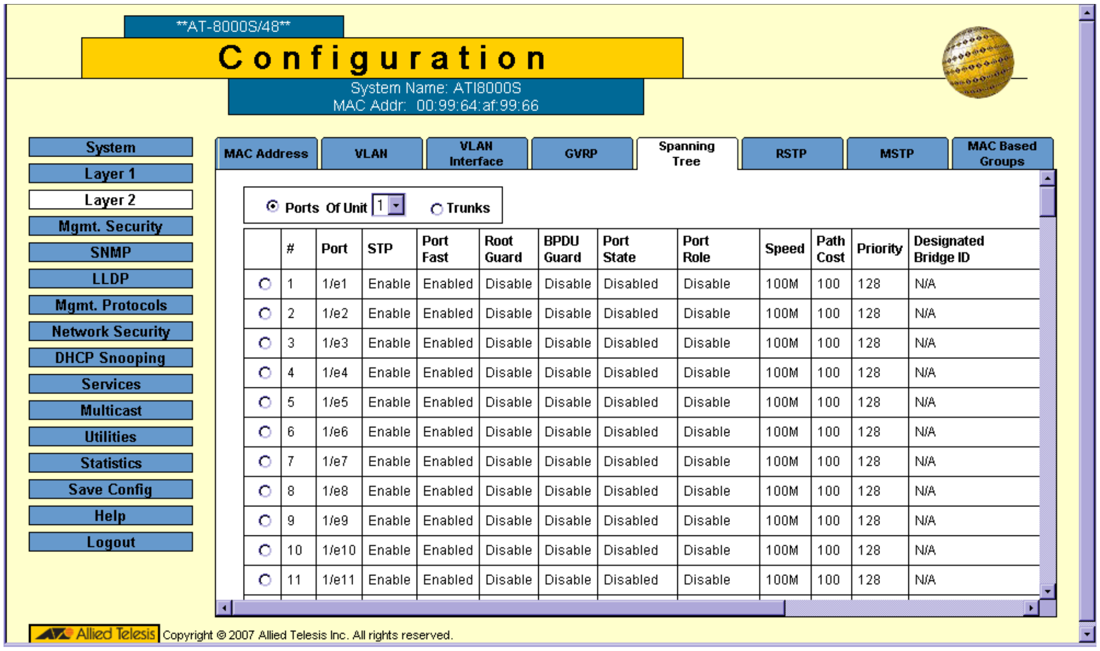
Defining STP Properties

The *Spanning Tree Page* contains parameters for enabling and configuring STP on the device.

To enable STP on the device:

1. Click **Layer 2 > Spanning Tree**. The *Spanning Tree Page* opens:

Figure 90: Spanning Tree Page



AT-8000S/48

Configuration

System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

● Ports Of Unit 1 ○ Trunks

	#	Port	STP	Port Fast	Root Guard	BPDU Guard	Port State	Port Role	Speed	Path Cost	Priority	Designated Bridge ID
○	1	1/e1	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	2	1/e2	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	3	1/e3	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	4	1/e4	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	5	1/e5	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	6	1/e6	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	7	1/e7	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	8	1/e8	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	9	1/e9	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	10	1/e10	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A
○	11	1/e11	Enable	Enabled	Disable	Disable	Disabled	Disable	100M	100	128	N/A

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *STP General* section of the *Spanning Tree Page* contains the following fields:

- **Spanning Tree State** — Indicates whether STP is enabled on the device. The possible field values are:
  - *Enable* — Enables STP on the device.
  - *Disable* — Disables STP on the device.
- **STP Operation Mode** — Specifies the STP mode that is enabled on the device.
  The possible field values are:
  - *Classic STP* — Enables Classic STP on the device.
  - *Rapid STP* — Enables Rapid STP on the device.
  - *Multiple STP* — Enables Multiple STP on the device.
- **BPDU Handling** — Determines how BPDU packets are managed when STP is disabled on the port or device. BPDUs are used to transmit spanning tree information. The possible field values are:
  - *Filtering* — Filters BPDU packets when spanning tree is disabled on an interface.
  - *Flooding* — Floods BPDU packets when spanning tree is disabled on an interface. This is the default value.

- **Path Cost Default Values** — Specifies the method used to assign default path cost to STP ports. The possible field values are:
  - *Short* — Specifies 1 through 65,535 range for port path cost. This is the default value.
  - *Long* — Specifies 1 through 200,000,000 range for port path cost.

The *Bridge Settings* section of the *Spanning Tree Page* contains the following fields:

- **Priority** — Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The default value is 32768. The port priority value is provided in increments of 4096; the value range is 0-65535.
- **Hello Time** — Specifies the device Hello Time, in seconds. The Hello Time is the time interval during which a Root Bridge waits between configuration messages. The value range is 1-10 seconds; the default value is 2 seconds.
- **Max Age** — Specifies the device Maximum Age Time, in seconds. The Maximum Age Time is the time interval during which a bridge waits before sending configuration messages. The value range is 6-40 seconds; the default value is 20 seconds.
- **Forward Delay** — Specifies the device Forward Delay Time, in seconds. The Forward Delay Time is the time interval during which a bridge remains in the listening-and-learning state before forwarding packets. The value range is 4-30 seconds; the default value is 15 seconds.

The *Designated Root* section of the *Spanning Tree Page* contains the following fields:

- **Bridge ID** — Identifies the Bridge priority and MAC address.
- **Root Bridge ID** — Identifies the Root Bridge priority and MAC address.
- **Root Port** — Indicates the port number that offers the lowest cost path from this bridge to the Root Bridge. This field is significant when the bridge is not the Root Bridge. The default is zero.
- **Root Path Cost** — The cost of the path from this bridge to the Root Bridge.
- **Topology Changes Counts** — Specifies the total amount of STP state changes that have occurred.
- **Last Topology Change** — Indicates the time interval that has elapsed since the bridge was initialized or reset, and the last topographic change that occurred. The time is displayed in a day-hour-minute-second format, such as 2 days 5 hours 10 minutes and 4 seconds.

2. Complete the *STP General* and *Bridge Settings* fields.
3. Click **Apply**. The new STP definition is added and device information is updated.
4. Click **Save Config** on the menu to save the settings permanently.

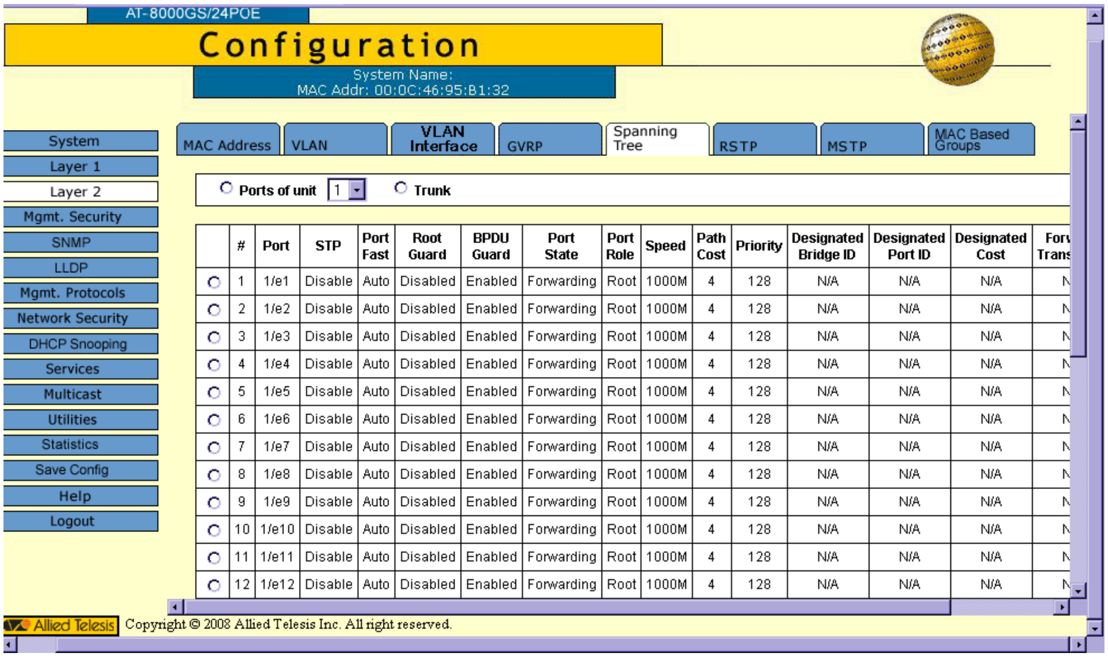
Defining STP Interfaces

Network administrators can assign STP settings to a specific interface (port or trunk) using the *STP Interface Configuration Page*. The Global trunks section displays the STP information for Link Aggregated Groups.

To assign STP settings to an interface (port or trunk):

1. Click **Layer 2 > Spanning Tree**. The *Spanning Tree Page* opens.
2. Click **Configure**. The *STP Interface Configuration Page* opens:

Figure 91: STP Interface Configuration Page



○ Ports of unit 1 ○ Trunk

	#	Port	STP	Port Fast	Root Guard	BPDU Guard	Port State	Port Role	Speed	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost	Forv Trans
○	1	1/e1	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	2	1/e2	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	3	1/e3	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	4	1/e4	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	5	1/e5	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	6	1/e6	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	7	1/e7	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	8	1/e8	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	9	1/e9	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	10	1/e10	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	11	1/e11	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N
○	12	1/e12	Disable	Auto	Disabled	Enabled	Forwarding	Root	1000M	4	128	N/A	N/A	N/A	N

The *STP Interface Configuration Page* contains the following sections:

- STP Port Parameters table
- Global System Trunk table

The parameters listed in both tables are identical.

The *STP Interface Configuration Page* contains the following fields:

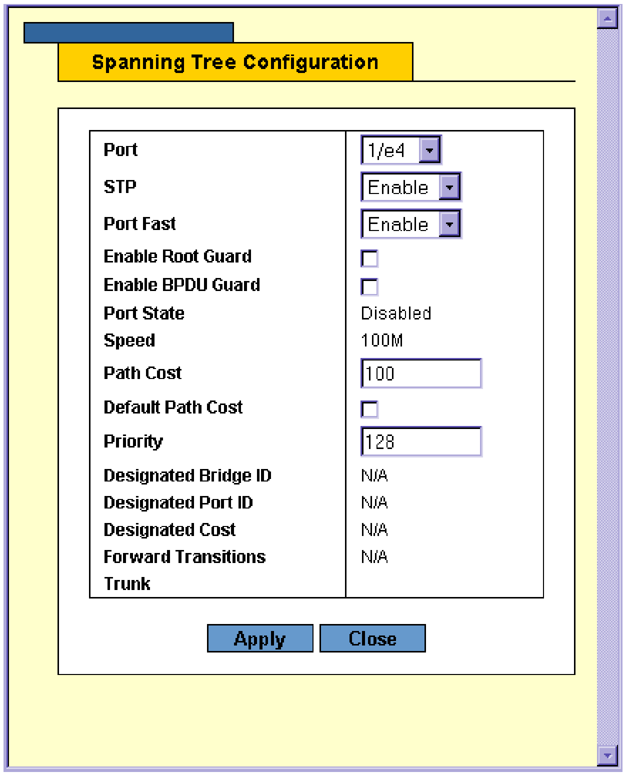
- Select the interfaces displayed in the table.
  - *Ports of Unit* — Specifies the port and stacking member for which the STP settings are displayed.
  - *Trunk* — Specifies the trunk for which the STP settings are displayed.
- **Port/Trunks** — Indicates the port or trunk number.
- **STP** — Indicates if STP is enabled on the port. The possible field values are:
  - *Enabled* — Indicates that STP is enabled on the port.
  - *Disabled* — Indicates that STP is disabled on the port.

- **Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the *Port State* is automatically placed in the *Forwarding* state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks. The possible field values are:
  - *Enable* — Enables Port Fast.
  - *Disable* — Disables Port Fast.
  - *Auto* — Indicates that Port Fast mode is enabled a few seconds after the interface becomes active.
- **Root Guard** — Prevents devices outside the network core from being assigned the spanning tree root. The possible field values are:
  - *Enable* — Enables Root Guard.
  - *Disable* — Disables Root Guard.
- **BPDU Guard** — Protects the network from invalid configurations by shutting down an interface when a BPDU message is received. The possible field values are:
  - *Enable* — Enables BPDU Guard.
  - *Disable* — Disables BPDU Guard.
- **Port State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
  - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
  - *Listening* — Indicates that the port is currently in the listening mode. The interface cannot forward traffic nor can it learn MAC addresses.
  - *Learning* — Indicates the port is currently in the learning mode. The interface cannot forward traffic; however, it can learn new MAC addresses.
  - *Forwarding* — Indicates the port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses. The interface can forward traffic and learn new MAC addresses.
- **Port Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to the root switch.
  - *Designated* — The port or trunk through which the designated switch is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root switch from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
  - *Disabled* — The port is not participating in the Spanning Tree.
- **Speed** — Indicates the speed at which the port is operating.
- **Path Cost** — Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is rerouted.
- **Priority** — Indicates the priority value of the port connected to the selected port. A lower priority increases the probability of connecting to a root port. The priority value is between 0-240. The priority value is determined in increments of 16.
- **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — Indicates the designated port priority and interface.
- **Designated Cost** — Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

- **Forward Transitions** — Indicates the number of times the port has changed from *Forwarding* state to *Blocking* state.
- **Trunk** — Indicates the trunk to which the port belongs.

3. Select the Unit, in the STP Interface Configuration section.
4. Click **Modify**. The *Spanning Tree Configuration Page* for ports or for trunks opens:

Figure 92: Spanning Tree Configuration Page



Port	1/e4
STP	Enable
Port Fast	Enable
Enable Root Guard	□
Enable BPDU Guard	□
Port State	Disabled
Speed	100M
Path Cost	100
Default Path Cost	□
Priority	128
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A
Trunk	

In addition to the *STP Interface Configuration Page*, the port-level *Spanning Tree Configuration Page* contains the following fields:

- **Default Path Cost** — Select if the default path cost of the port is automatically set by the port speed and the default path cost method.

5. Select *Enable* in the *STP* field.
6. Define the *Port Fast*, *Enable Root Guard*, *Path Cost*, *Default Path Cost*, and *Priority* fields.
7. Click **Apply**. STP is enabled on the interface, and the device is updated.

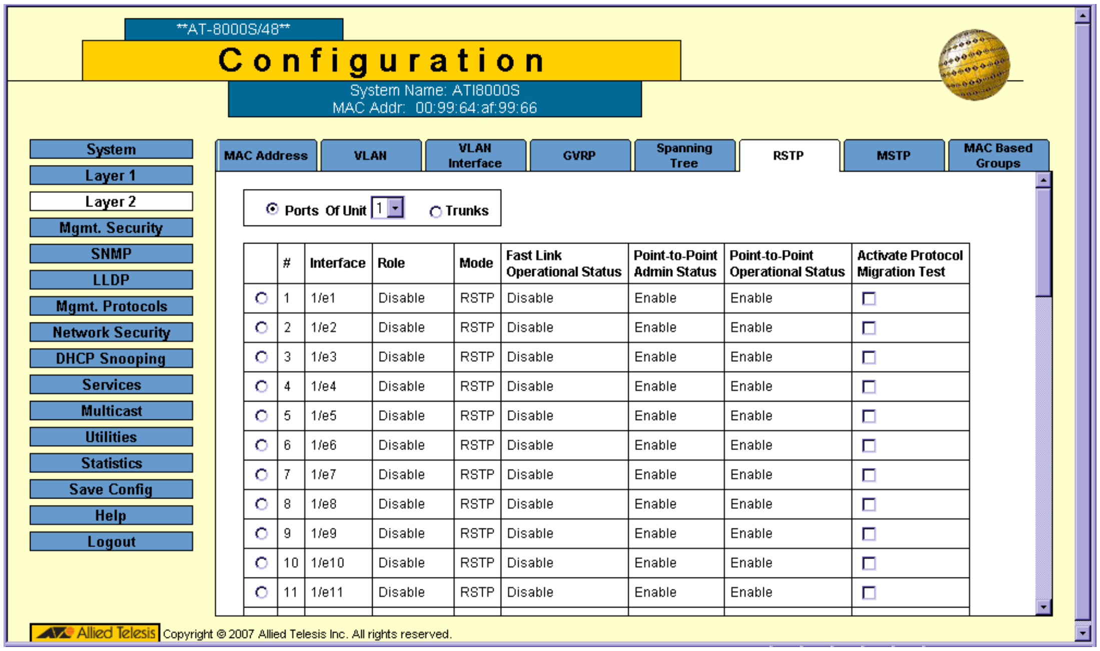
Configuring Rapid Spanning Tree

While Classic STP prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. This time may delay detecting possible loops and propagating status topology changes. *Rapid Spanning Tree Protocol* (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops.

To define RSTP on the device:

1. Click **Layer 2 > RSTP**. The *RSTP Page* opens:

Figure 93: RSTP Page



● Ports Of Unit 1 ○ Trunks

	#	Interface	Role	Mode	Fast Link Operational Status	Point-to-Point Admin Status	Point-to-Point Operational Status	Activate Protocol Migration Test
○	1	1/e1	Disable	RSTP	Disable	Enable	Enable	□
○	2	1/e2	Disable	RSTP	Disable	Enable	Enable	□
○	3	1/e3	Disable	RSTP	Disable	Enable	Enable	□
○	4	1/e4	Disable	RSTP	Disable	Enable	Enable	□
○	5	1/e5	Disable	RSTP	Disable	Enable	Enable	□
○	6	1/e6	Disable	RSTP	Disable	Enable	Enable	□
○	7	1/e7	Disable	RSTP	Disable	Enable	Enable	□
○	8	1/e8	Disable	RSTP	Disable	Enable	Enable	□
○	9	1/e9	Disable	RSTP	Disable	Enable	Enable	□
○	10	1/e10	Disable	RSTP	Disable	Enable	Enable	□
○	11	1/e11	Disable	RSTP	Disable	Enable	Enable	□

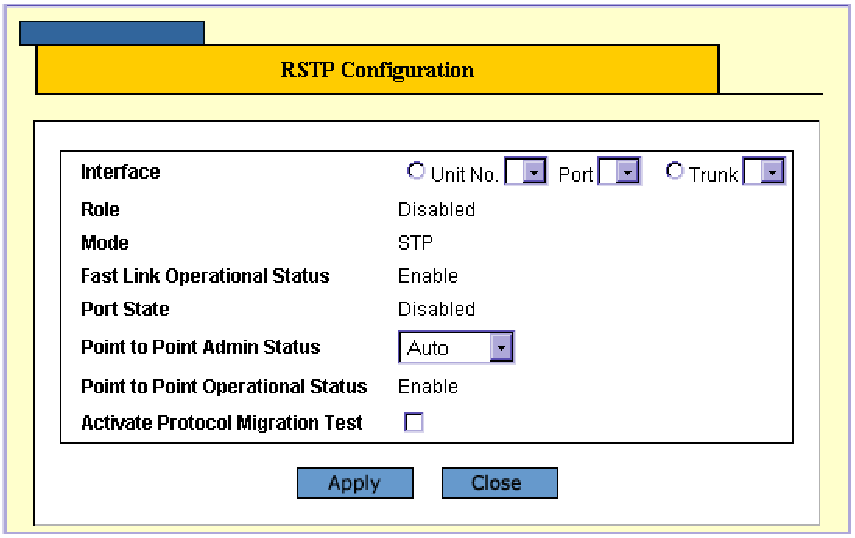
The *RSTP Page* contains the following fields:

- Select the interfaces displayed in the table.
  - *Ports of Unit* — Specifies the port and stacking member for which the RSTP settings are displayed.
  - *Trunks* — Specifies the trunk for which the RSTP settings are displayed.
- **Interface** — Displays the port or trunk on which Rapid STP is enabled.
- **Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to the root switch.
  - *Designated* — The port or trunk through which the designated switch is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root switch from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections to a shared segment.
  - *Disabled* — The port is not participating in the Spanning Tree.

- **Mode** — Displays the current STP mode. The STP mode is selected in the *Spanning Tree Page*. The possible field values are:
  - *STP* — Classic STP is enabled on the device.
  - *Rapid STP* — Rapid STP is enabled on the device.
- **Fast Link Operational Status** — Indicates whether Fast Link is enabled or disabled for the port or trunk. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
- **Point-to-Point Admin Status** — Indicates whether a point-to-point link is established on the port. Ports defined as Full Duplex are considered Point-to-Point port links. The possible field values are:
  - *Enable* — Enables the device to establish point-to-point links.
  - *Disable* — Device establishes shared, half duplex links.
  - *Auto* — Device automatically determines the state.
- **Point-to-Point Operational Status** — Displays the point-to-point operating state.
- **Activate Protocol Migration Test** — Select to run a Protocol Migration Test. The test identifies the STP mode of the interface connected to the selected interface.
  - *Checked* — Runs a Protocol Migration Test on the interface after the user clicks the **Apply** button.
  - *Unchecked* — Does not run a Protocol Migration Test.

2. Click **Modify**. The *Modify RSTP Page* opens:

Figure 94: Modify RSTP Page



RSTP Configuration

Interface	○ Unit No. ▾ Port ▾ ○ Trunk ▾
Role	Disabled
Mode	STP
Fast Link Operational Status	Enable
Port State	Disabled
Point to Point Admin Status	Auto ▾
Point to Point Operational Status	Enable
Activate Protocol Migration Test	□

In addition to the *RSTP Page*, the *Modify RSTP Page* contains the following fields:

- **Port State** — Displays the current STP state of a port. If STP is enabled, the port state determines what action is taken on traffic. Possible port states are:
  - *Forwarding* — Indicates that the port forwards packets.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
  - *Listening* — Indicates that the port is currently in the listening mode. The interface cannot forward traffic nor can it learn MAC addresses.

   - *Learning* — Indicates the port is currently in the learning mode. The interface cannot forward traffic however it can learn new MAC addresses
   - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.

3. Define the *Interface*, *Point to Point Admin Status*, and *Activate Protocol Migration Test* fields.
4. Click **Apply**. RSTP is defined for the selected interface, and the device is updated.
5. Click **Save Config** on the menu, to save changes permanently.

Configuring Multiple Spanning Tree

Multiple Spanning Tree Protocol (MSTP) provides differing load balancing scenarios. For example, while port A is blocked in one STP instance, the same port can be placed in the *Forwarding* state in another STP instance.

This section contains the following topics:

- Defining MSTP Properties
- Defining MSTP Interfaces
- Defining MSTP Instance Mappings
- Defining MSTP Instance Settings

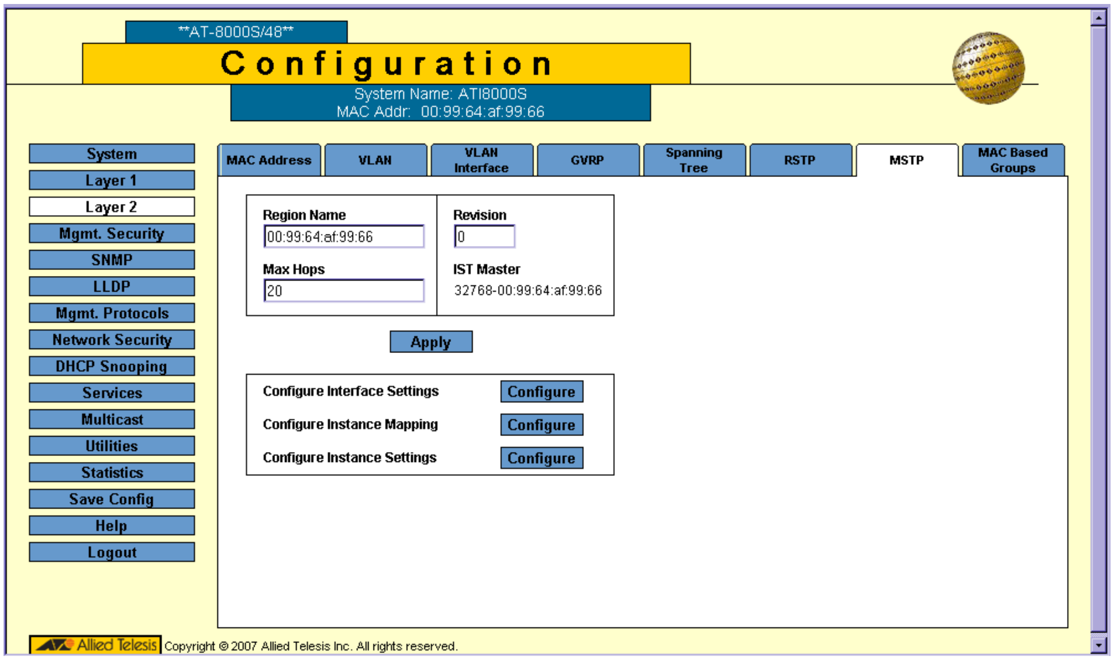
Defining MSTP Properties

The *MSTP Page* contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops.

To define MSTP:

1. Click **Layer 2 > MSTP**. The *MSTP Page* opens:

Figure 95: MSTP Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Region Name: 00:99:64:af:99:66
Revision: 0
Max Hops: 20
IST Master: 32768-00:99:64:af:99:66

Configure Interface Settings
Configure Instance Mapping
Configure Instance Settings

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *MSTP Page* contains the following fields:

- **Region Name** — User-defined STP region name.
- **Revision** — An unsigned 16-bit number that identifies the revision of the current MSTP configuration. The revision number is required as part of the MSTP configuration. The possible field range is 0-65535.
- **Max Hops** — Specifies the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The possible field range is 1-40. The field default is 20 hops.
- **IST Master** — Identifies the Spanning Tree Master instance. The IST Master is the specified instance root.
- **Configure Interface Settings** — Click **Configure** to assign MSTP settings to a specific interface.
- **Configure Instance Mapping** — Click **Configure** to assign MSTP mapping to a specific instance.
- **Configure Instance Settings** — Click **Configure** to define MSTP Instances settings.

2. Define the *Region Name*, *Revision*, and *Max Hops* fields.
3. Click **Apply**. The MSTP properties are defined, and the device is updated.

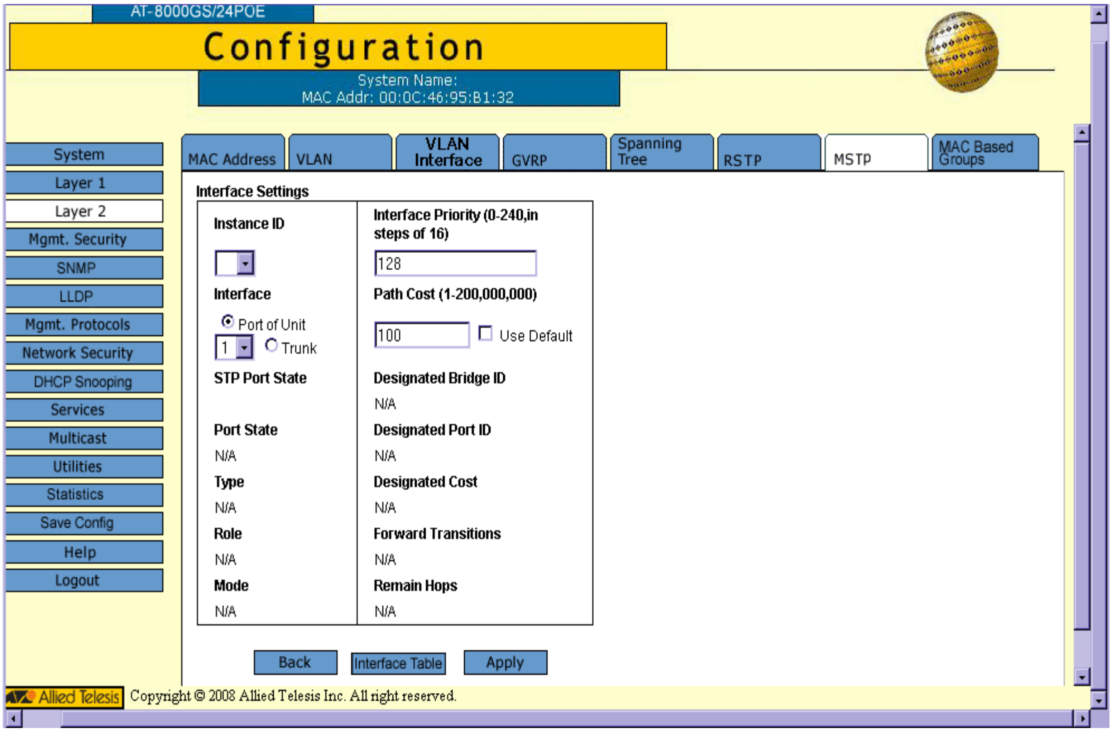
Defining MSTP Interfaces

Network administrators can assign MSTP settings to a specific interface (port or trunk) using the *MSTP Interface Settings Page*.

To define MSTP interface settings:

1. Click **Layer 2 > MSTP**. The *MSTP Page* opens.
2. Click **Configure** next to the *Configure Interface Settings* option. The *MSTP Interface Settings Page* opens:

Figure 96: MSTP Interface Settings Page



Interface Settings

Instance ID

Interface

● Port of Unit
1 ○ Trunk

STP Port State

Port State
N/A

Type
N/A

Role
N/A

Mode
N/A

Interface Priority (0-240,in steps of 16)
128

Path Cost (1-200,000,000)
100 □ Use Default

Designated Bridge ID
N/A

Designated Port ID
N/A

Designated Cost
N/A

Forward Transitions
N/A

Remain Hops
N/A

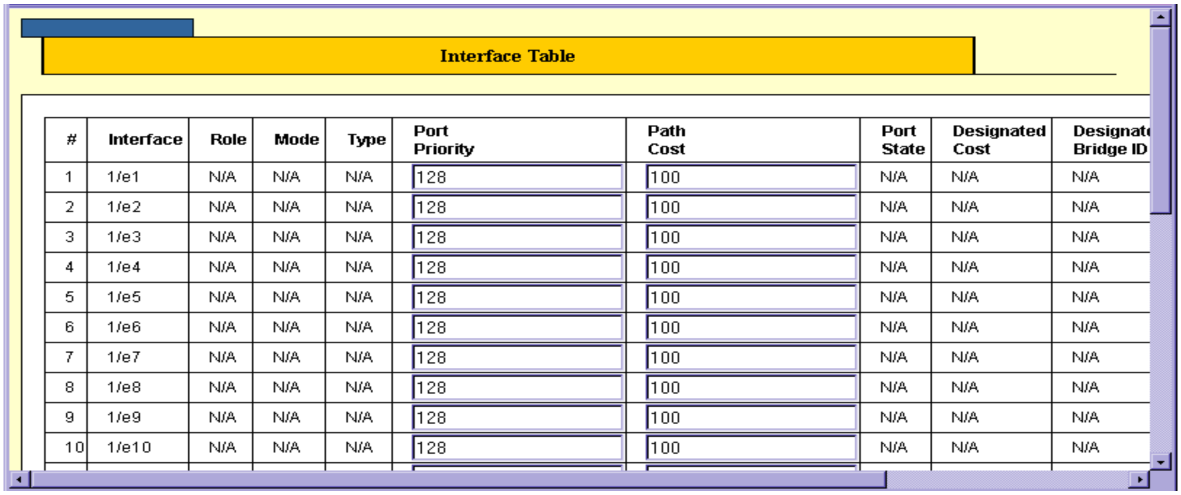
Copyright © 2008 Allied Telesis Inc. All right reserved.

The *MSTP Interface Settings Page* contains the following fields:

- **Instance ID** — Lists the MSTP instances configured on the device. The possible field range is 1-7.
- **Interface** — Displays the specific interface for this page's MSTP setting. The possible field values are:
  - *Port of Unit* — Specifies the port for which the MSTP settings are displayed.
  - *Trunk* — Specifies the trunk for which the MSTP settings are displayed.
- **STP Port State** — Indicates if STP is enabled on the port. The possible field values are:
  - *Enabled* — Indicates that STP is enabled on the port.
  - *Disabled* — Indicates that STP is disabled on the port.
- **Port State** — Indicates whether the port is enabled for the specific instance. The possible field values are:
  - *Forwarding* — Indicates that the port forwards packets.
  - *Discarding* — Indicates that the port discards packets.
  - *Disabled* — Indicates that STP is disabled on the port.
  - *N/A* — Indicates that the port is not available for STP; for example, if the port belongs to a trunk.
- **Type** — Indicates whether the port is a Boundary or Master port. The possible field values are:
  - *Boundary* — Indicates that the port attaches MST bridges to LANs in an outlying region. If the port is a Boundary port, this field also indicates whether the device on the other side of the link is working in RSTP or STP mode.
  - *Internal* — Indicates the port provides connectivity within the same region.
- **Role** — Indicates the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to the root device.
  - *Designated* — Indicates the port or trunk through which the designated device is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root device from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link or when a LAN has two or more connections to a shared segment.
  - *Disabled* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the STP mode by which STP is enabled on the device. The possible field values are:
  - *Classic STP* — Classic STP is enabled on the device. This is the default value.
  - *Rapid STP* — Rapid STP is enabled on the device.
- **Interface Priority (0-240,in steps of 16)** — Indicates the priority value of the port connected to the selected port for the specified instance. A lower priority increases the probability of connecting to a root port. The possible field values are 0-240, in multiples of 16. The default value is 128.
- **Path Cost (1-200,000,000)** — Indicates the port contribution to the Spanning Tree instance. The field range is 1-200,000,000.
  - *Use Default* — Defines the default path cost as the Path Cost field setting.
- **Designated Bridge ID** — Displays the ID of the bridge that connects the link or shared LAN to the root.
- **Designated Port ID** — Displays the ID of the port on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost** — Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings.
- **Forward Transitions** — Indicates the number of times the Trunk State has changed from a *Forwarding* state to a *Blocking* state.
- **Remain Hops** — Indicates the hops remaining in the region before the BPDU is discarded.

3. Define the fields.
4. Click **Apply**. MSTP is defined for the selected interface.
5. Click **Save Config** on the menu, to save changes permanently.
6. To view the MSTP configurations of all interfaces, click Interface Table. The *MSTP Interface Table* is displayed. In the *MSTP Interface Table*, administrators can modify the Interface Priority and Path Cost of any interface.

Figure 97: MSTP Interface Table



Interface Table

#	Interface	Role	Mode	Type	Port Priority	Path Cost	Port State	Designated Cost	Designat Bridge ID
1	1/e1	N/A	N/A	N/A	128	100	N/A	N/A	N/A
2	1/e2	N/A	N/A	N/A	128	100	N/A	N/A	N/A
3	1/e3	N/A	N/A	N/A	128	100	N/A	N/A	N/A
4	1/e4	N/A	N/A	N/A	128	100	N/A	N/A	N/A
5	1/e5	N/A	N/A	N/A	128	100	N/A	N/A	N/A
6	1/e6	N/A	N/A	N/A	128	100	N/A	N/A	N/A
7	1/e7	N/A	N/A	N/A	128	100	N/A	N/A	N/A
8	1/e8	N/A	N/A	N/A	128	100	N/A	N/A	N/A
9	1/e9	N/A	N/A	N/A	128	100	N/A	N/A	N/A
10	1/e10	N/A	N/A	N/A	128	100	N/A	N/A	N/A

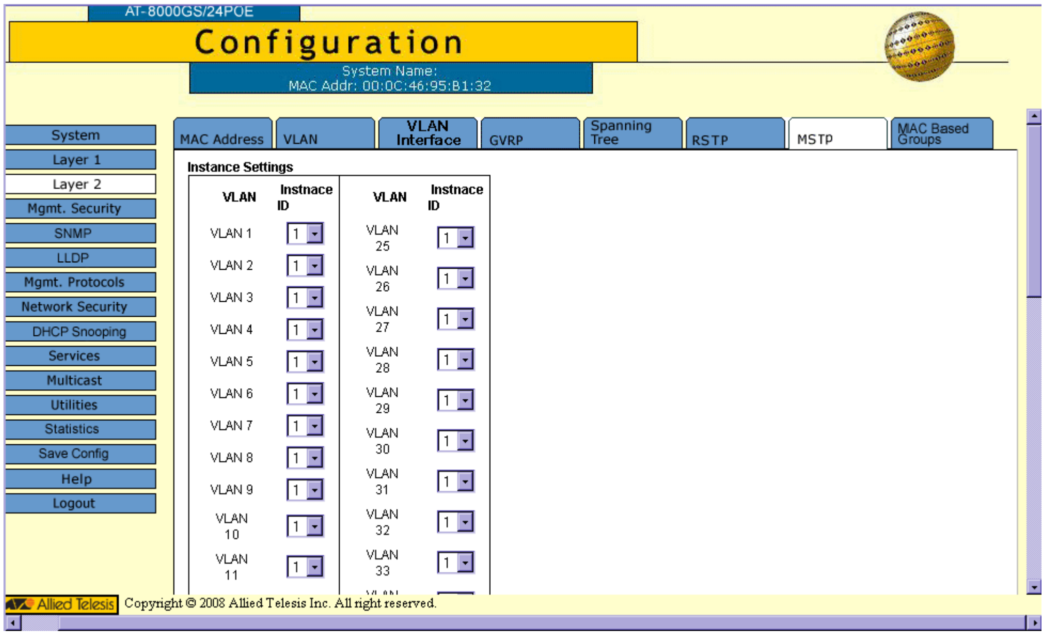
Defining MSTP Instance Mappings

Network administrators can assign MSTP mapping to a specific instance (port or trunk) using the *MSTP Instance Mapping Page*.

To define MSTP interface mapping:

1. Click **Layer 2 > MSTP**. The *MSTP Page* opens.
2. Click **Configure** next to the *Configure Instance Mapping* option. The *MSTP Instance Mapping Page* opens:

Figure 98: MSTP Instance Mapping Page



Instance Settings

VLAN	Instnace ID	VLAN	Instnace ID
VLAN 1	1	VLAN 25	1
VLAN 2	1	VLAN 26	1
VLAN 3	1	VLAN 27	1
VLAN 4	1	VLAN 28	1
VLAN 5	1	VLAN 29	1
VLAN 6	1	VLAN 30	1
VLAN 7	1	VLAN 31	1
VLAN 8	1	VLAN 32	1
VLAN 9	1	VLAN 33	1
VLAN 10	1		
VLAN 11	1		

The *MSTP Instance Mapping Page* contains the following fields:

- **VLAN** — Displays the VLAN ID.
- **Instance ID** — Defines the mapped MSTP instance. The possible field range is 1-7.

3. Map the VLANs to Instance IDs.
4. Click **Apply** to implement the mapping.
5. Click **Save Config** on the menu, to save changes permanently.

Defining MSTP Instance Settings

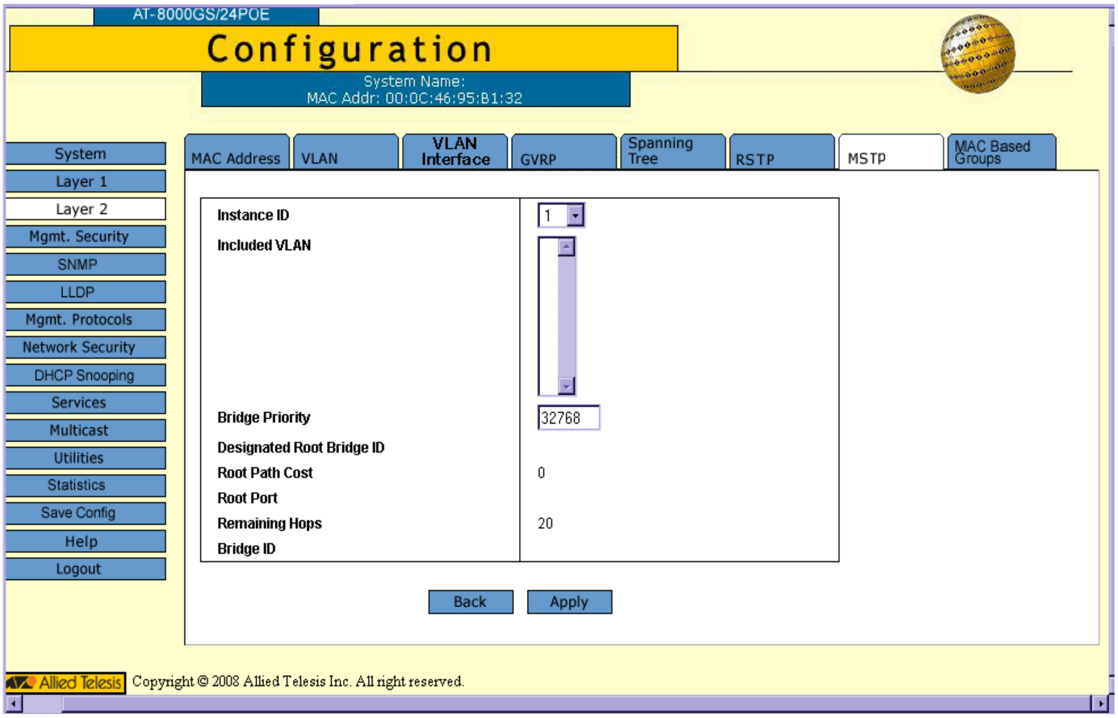
MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within *Multiple Spanning Tree Regions* (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MSTP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and VLANs that belong to an instance. To configure devices in the same region, the three components must be the same for all the devices.

Network Administrators can define MSTP Instances settings using the *MSTP Instance Settings Page*.

To define MSTP interface settings:

1. Click **Layer 2 > MSTP**. The *MSTP Page* opens.
2. Click **Configure** next to the *Configure Instance Settings* option. The *MSTP Instance Settings Page* opens:

Figure 99: MSTP Instance Settings Page



Instance ID	1
Included VLAN	
Bridge Priority	32768
Designated Root Bridge ID	
Root Path Cost	0
Root Port	
Remaining Hops	20
Bridge ID	

The *MSTP Instance Settings Page* contains the following fields:

- **Instance ID** — Defines the VLAN group to which the interface is assigned. The possible field range is 1-15.
- **Included VLAN** — Maps the selected VLAN to the selected instance. Each VLAN belongs to one instance.
- **Bridge Priority** — Specifies the selected spanning tree instance device priority. The possible field range is 0-61440 in multiples of 4096.
- **Designated Root Bridge ID** — Indicates the ID of the bridge with the lowest path cost to the instance ID.
- **Root Path Cost** — Indicates the selected instance’s path cost.
- **Root Port** — Indicates the selected instance’s root port.
- **Remaining Hops** — Indicates the number of hops remaining in the region until the BPDU is discarded.
- **Bridge ID** — Indicates the bridge ID of the selected instance.

3. Define the fields.
4. Click **Apply**. MSTP is defined for the selected instance, and the device is updated. The *MSTP Page* is displayed.
5. Click **Save Config** on the menu, to save changes permanently.

Chapter 11.Configuring Multicast Forwarding

Multicast forwarding allows a single packet to be forwarded to multiple destinations. Layer 2 Multicast service is based on a Layer 2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports. The Internet Group Management Protocol (IGMP) allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific Multicast group.

Multicast forwarding enables transmitting packets from either a specific Multicast group to a source, or from a non-specific source to a Multicast group.

The device supports IGMPv1, IGMPv2, and IGMPv3.

This section contains the following topics:

- Configuring IGMP Snooping
- Defining Multicast Bridging Groups
- Defining Multicast Forward All Settings
- Defining Unregistered Multicast Settings

Configuring IGMP Snooping

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines:

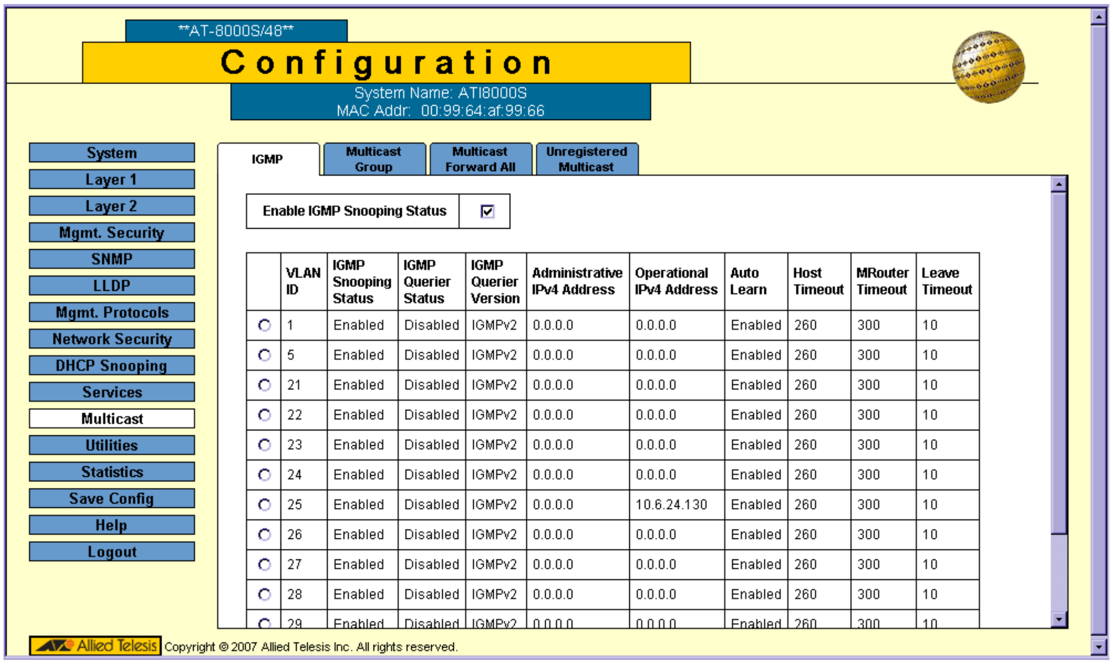
- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.
- Which routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that Multicast group is accepting members. This results in the creation of the Multicast filtering database.

To configure IGMP Snooping:

1. Click **Multicast** > **IGMP**. The *IGMP Page* opens:

Figure 100: IGMP Page



Enable IGMP Snooping Status ☑

	VLAN ID	IGMP Snooping Status	IGMP Querier Status	IGMP Querier Version	Administrative IPv4 Address	Operational IPv4 Address	Auto Learn	Host Timeout	MRouter Timeout	Leave Timeout
○	1	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10
○	5	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10
○	21	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10
○	22	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10
○	23	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10
○	24	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10
○	25	Enabled	Disabled	IGMPv2	0.0.0.0	10.6.24.130	Enabled	260	300	10
○	26	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10
○	27	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10
○	28	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10
○	29	Enabled	Disabled	IGMPv2	0.0.0.0	0.0.0.0	Enabled	260	300	10

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *IGMP Page* contains the following fields:

- **Enable IGMP Snooping Status** — Indicates if IGMP Snooping is enabled on the device. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled. The possible field values are:
  - *Checked* — Enables IGMP Snooping on the device.
  - *Unchecked* — Disables IGMP Snooping on the device.
- **VLAN ID** — Specifies the VLAN ID.
- **IGMP Snooping Status** — Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:
  - *Enable* — Enables IGMP Snooping on the VLAN.
  - *Disable* — Disables IGMP Snooping on the VLAN.

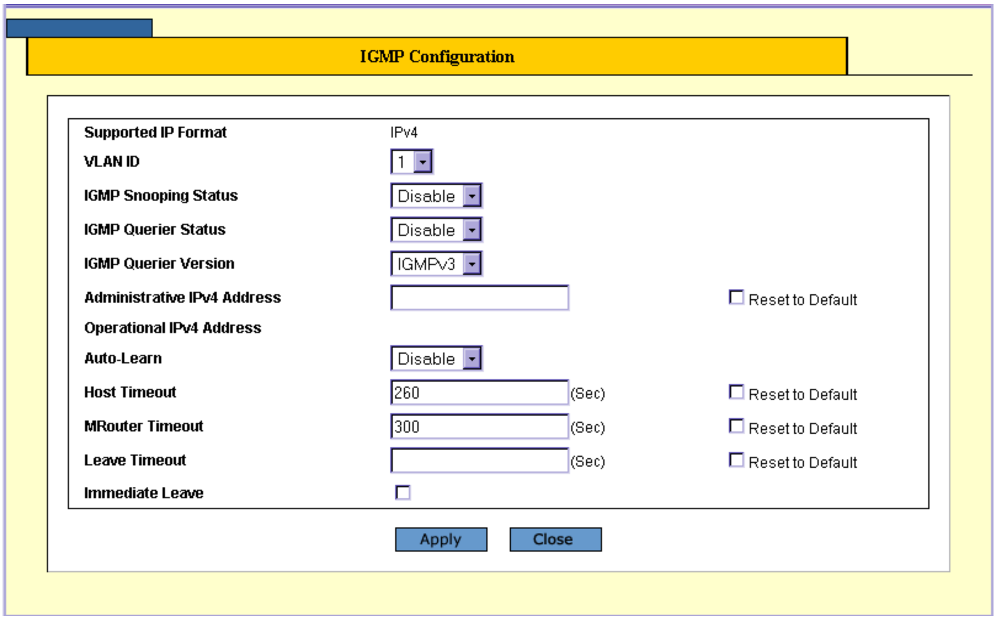
- **IGMP Querier Status** — Indicates if the specific VLAN can operate as an IGMP Querier. The possible field values are:
  - *Enable* — Enables IGMP Querying on the VLAN.
  - *Disable* — Disables IGMP Querying on the VLAN.
- **IGMP Querier Version** — Displays the IGMP Snooping version enabled on the device which functions as an IGMP Snooper of the selected VLAN. The possible field values are:
  - *IGMPv2* — Indicates that IGMP version 2 is enabled on the device.
  - *IGMPv3* — Indicates that IGMP version 3 is enabled on the device.
- **Administrative IPv4 Address** — The configured IPv4 address of the IGMP Querier interface on the VLAN. The VLAN’s IP address is the default address for the IGMP Querier.
- **Operational IPv4 Address** — The current IPv4 address of the IGMP Querier interface on the VLAN.
- **Auto Learn** — Indicates if Auto Learn is enabled on the device. If Auto Learn is enabled, the devices automatically learns where other Multicast groups are located. Enables or disables Auto Learn on the Ethernet device.The possible field values are:
  - *Enable* — Enables auto learn
  - *Disable* — Disables auto learn.
- **Host Timeout** — Indicates the amount of time host waits to receive a message before timing out. The default time is 260 seconds.
- **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.
- **Leave Timeout** — Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic The Leave Timeout value is either user-defined, or an immediate leave value. The default timeout is 10 seconds.

2. Click the *Enable IGMP Snooping Status* checkbox. IGMP Snooping is enabled on the device.

To modify the IGMP Snooping configuration:

1. Click **Multicast** > **IGMP**. The *IGMP Page* opens.
2. Click **Modify**. The *IGMP Configuration Page* opens:

Figure 101:IGMP Configuration Page



IGMP Configuration

Supported IP Format	IPv4		
VLAN ID	1		
IGMP Snooping Status	Disable		
IGMP Querier Status	Disable		
IGMP Querier Version	IGMPv3		
Administrative IPv4 Address			□ Reset to Default
Operational IPv4 Address			
Auto-Learn	Disable		
Host Timeout	260	(Sec)	□ Reset to Default
MRouter Timeout	300	(Sec)	□ Reset to Default
Leave Timeout		(Sec)	□ Reset to Default
Immediate Leave	□		

In addition to the *IGMP Page*, the *IGMP Configuration Page* contains the following fields:

- **Supported IP Format** — Indicates that IPv4 is supported.
- **Immediate Leave** — Host immediately times out after requesting to leave the IGMP group and not receiving a Join message from another station.
  - *Checked* — Host immediately times out.
  - *Unchecked* — Host times out as specified in the **Leave Timeout** field.

3. Define the fields. Select **Reset as Default** to use the default value.
4. Click **Apply**. The IGMP Snooping global parameters are modified, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

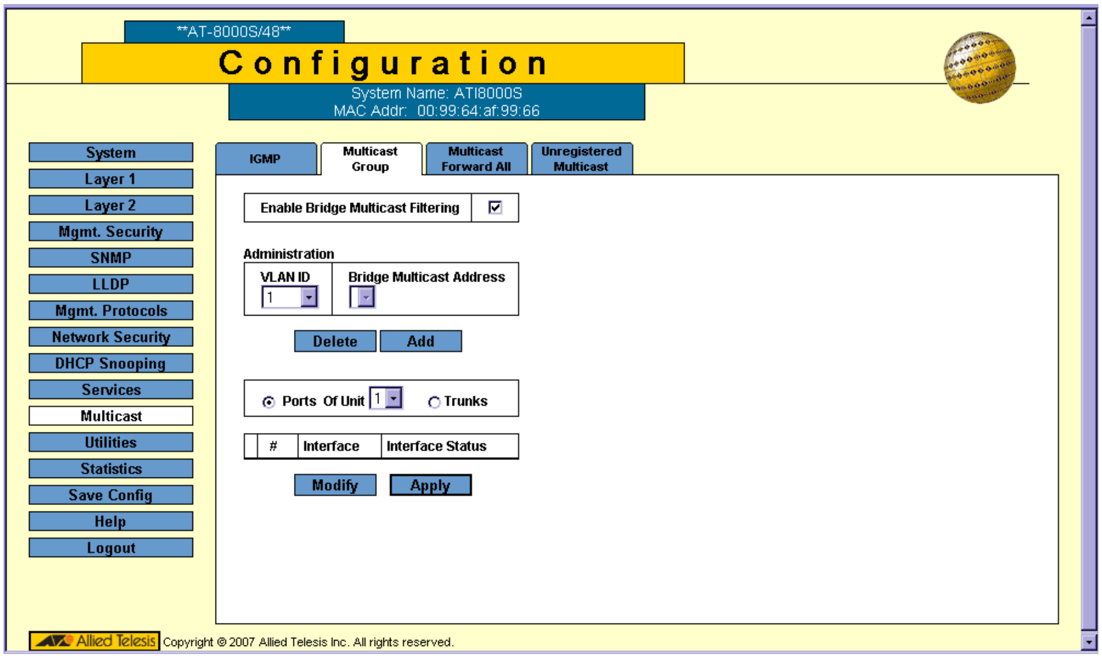
Defining Multicast Bridging Groups

The *Multicast Group Page* displays the ports and trunks attached to the Multicast service group in the Ports and Trunks tables. The Port and Trunk tables also reflect the manner in which the port or trunks joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. New Multicast service groups can be created and ports can be assigned to a specific Multicast service address group.

To define Multicast Groups:

1. Click **Multicast > Multicast Group**. The *Multicast Group Page* opens:

Figure 102: Multicast Group Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Enable Bridge Multicast Filtering ☑

Administration

VLAN ID	Bridge Multicast Address
1	

● Ports Of Unit 1 ○ Trunks

#	Interface	Interface Status

Copyright © 2007 Allied Telesis Inc. All rights reserved.

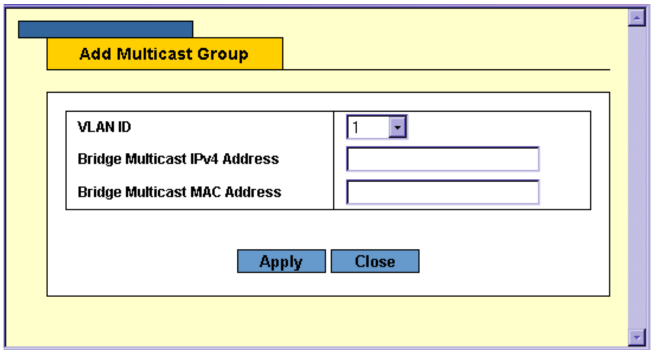
The *Multicast Group Page* contains the following fields:

- **Enable Bridge Multicast Filtering** — Indicates if bridge Multicast filtering is enabled on the device. The possible field values are:
  - *Checked* — Enables Multicast filtering on the device.
  - *Unchecked* — Disables Multicast filtering on the device. If Multicast filtering is disabled, Multicast frames are flooded to all ports in the relevant VLAN. Disabled is the default value.
- **VLAN ID** — Displays the VLAN for which Multicast parameters are displayed.
- **Bridge Multicast Address** — Identifies the Multicast group MAC address/IP address.
- Select the interfaces displayed in the table.
  - *Ports of Unit* — Specifies the port and stacking member for which the Multicast group settings are displayed.
  - *Trunk* — Specifies the trunk for which the Multicast group settings are displayed.
- **Interface** — Displays the currently defined interface.
- **Interface Status** — Displays the current interface status. Available options are: *excluded*, *forbidden*, *static* and *dynamic*.

2. Check the **Enable Bridge Multicast Filtering** checkbox.

3. Click **Add**. The *Add Multicast Group Page* opens:

Figure 103: Add Multicast Group Page



Add Multicast Group

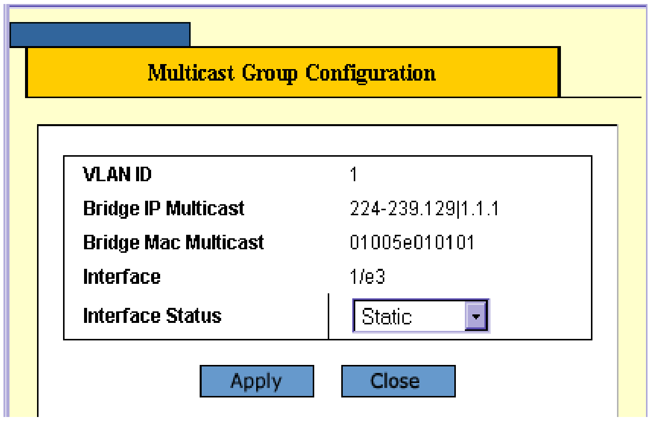
VLAN ID	1
Bridge Multicast IPv4 Address	
Bridge Multicast MAC Address	

4. Select the *VLAN ID*.
5. Enter the *Bridge Multicast MAC Address* and the *Bridge Multicast IPv4 Address*.
6. Click **Apply**. The new Multicast group is saved and the device is updated.

To modify a Multicast group:

1. Click **Modify**. The *Multicast Group Configuration Page* opens:

Figure 104: Multicast Group Configuration Page



Multicast Group Configuration

VLAN ID	1
Bridge IP Multicast	224-239.129|1.1.1
Bridge Mac Multicast	01005e010101
Interface	1/e3
Interface Status	Static

2. Define the fields.
3. Click **Apply**. The Multicast Group is saved and the device is updated.

Defining Multicast Forward All Settings

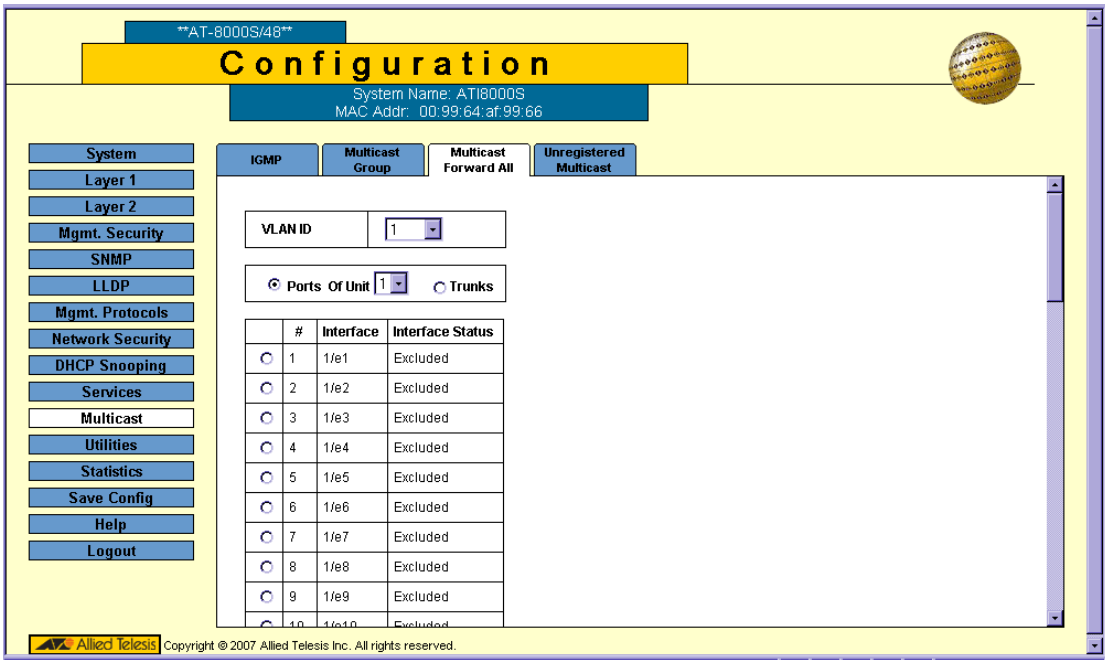
Multicast forwarding enables transmitting packets from either a specific Multicast group to a source, or from a non-specific source to a Multicast group.

The *Bridge Multicast Forward All Page* contains fields for attaching ports or trunks to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port or VLAN. Unless trunks are defined, only a Multicast Forward All table displays.

To define Multicast forward all settings:

1. Click **Multicast > Multicast Forward All**. The *Multicast Forward All Page* opens:

Figure 105: Multicast Forward All Page



AT-8000S/48

Configuration

System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

VLAN ID: 1

● Ports Of Unit 1 ○ Trunks

	#	Interface	Interface Status
○	1	1/e1	Excluded
○	2	1/e2	Excluded
○	3	1/e3	Excluded
○	4	1/e4	Excluded
○	5	1/e5	Excluded
○	6	1/e6	Excluded
○	7	1/e7	Excluded
○	8	1/e8	Excluded
○	9	1/e9	Excluded
○	10	1/e10	Excluded

Allied Telesis Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Multicast Forward All Page* contains the following fields:

- **VLAN ID** — Displays the VLAN for which Multicast parameters are displayed.
- Select the interfaces displayed in the table.
  - *Ports of Unit* — Specifies the port and stacking member for which the Multicast Forward All settings are displayed.
  - *Trunk* — Specifies the trunk for which the Multicast Forward All settings are displayed.

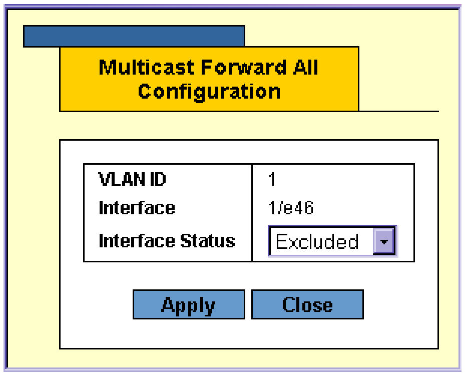
The Multicast Forward All table displays the following information, identical for ports and trunks.

- **Interface** — Displays the interface ID.
- **Interface Status** — Indicates the forwarding status of the selected interface. The possible values are:
  - *Static* — Attaches the port to the Multicast router or switch as a static port.
  - *Excluded* — The port is not attached to a Multicast router or switch.
  - *Forbidden* — Indicates that the port is forbidden for forward all.

2. Select interfaces to modify.

3. Click **Modify**. The *Multicast Forward All Configuration Page* opens:

Figure 106: Multicast Forward All Configuration Page



VLAN ID	1
Interface	1/e46
Interface Status	Excluded

4. Define the *Interface Status* field.
5. Click **Apply**. The Multicast Forward All settings are saved and the device is updated.

Defining Unregistered Multicast Settings

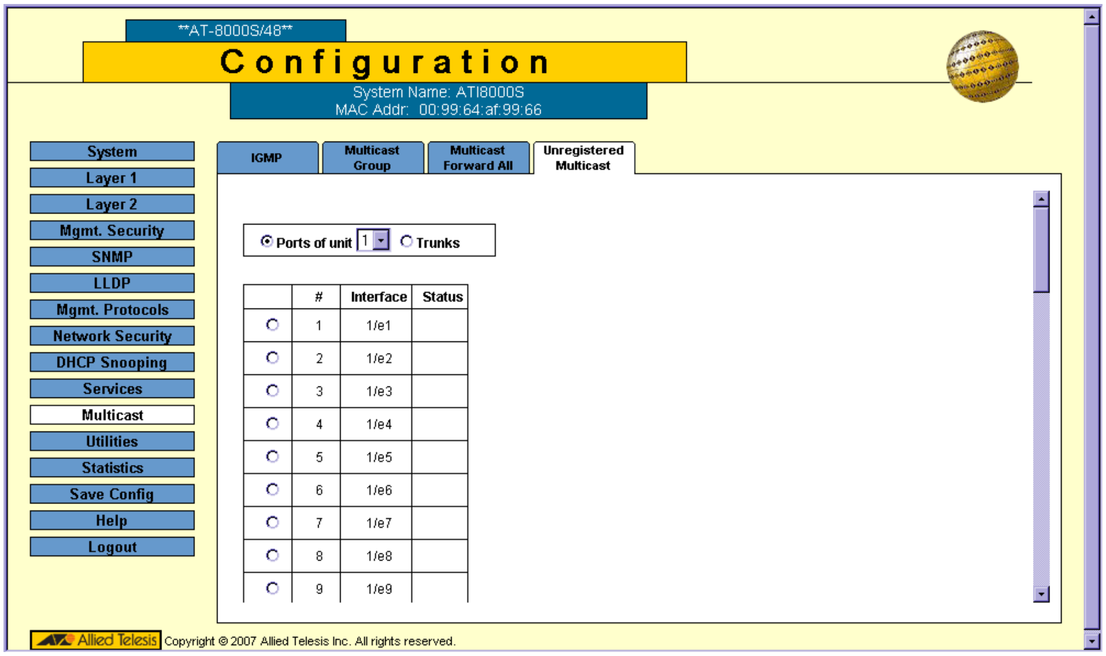
Multicast frames are generally forwarded to all ports in the VLAN. If IGMP Snooping is enabled, the device learns about the existence of Multicast groups and monitors which ports have joined what Multicast group. Multicast groups can also be statically enabled. This enables the device to forward the Multicast frames (from a registered Multicast group) only to ports that are registered to that Multicast group.

The *Unregistered Multicast Page* contains fields to handle Multicast frames that belong to Unregistered Multicast groups. Unregistered Multicast groups are the groups that are not known to the device. All Unregistered Multicast frames are still forwarded to all ports on the VLAN. After a port has been set to Forwarding/Filtering, then this port's configuration is valid for any VLAN it is a member of (or will be a member of).

To define unregistered Multicast settings:

1. Click **Multicast > Unregistered Multicast**. The *Unregistered Multicast Page* opens:

Figure 107: Unregistered Multicast Page



AT-8000S/48

System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

● Ports of unit 1 ○ Trunks

	#	Interface	Status
○	1	1/e1	
○	2	1/e2	
○	3	1/e3	
○	4	1/e4	
○	5	1/e5	
○	6	1/e6	
○	7	1/e7	
○	8	1/e8	
○	9	1/e9	

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Unregistered Multicast Page* contains the following fields:

Select the interfaces displayed in the table.

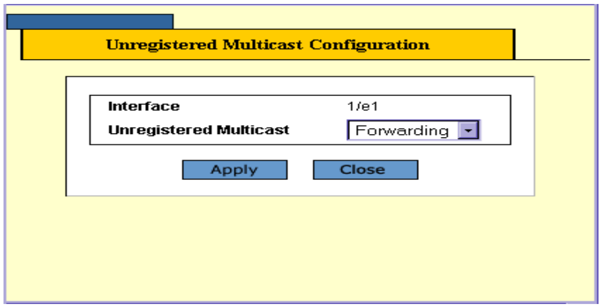
- **Ports of Unit** — Indicates the stacking member ports for which the unregistered Multicast parameters are displayed.
- **Trunk** — Specifies the trunk for which the Unregistered Multicast settings are displayed.

The Unregistered Multicast table displays the following information for ports:

- **Interface** — Displays the interface ID.
- **Unregistered Multicast** — Indicates the forwarding status of the selected interface. The possible values are:
  - *Forwarding* — Enables forwarding of Unregistered Multicast frames to the selected VLAN interface. This is the default setting.
  - *Filtering* — Enables filtering of Unregistered Multicast frames to the selected VLAN interface.

2. Click **Modify**. The *Unregistered Multicast Configuration Page* opens:

Figure 108: Unregistered Multicast Configuration Page



Unregistered Multicast Configuration

Interface	1/e1
Unregistered Multicast	Forwarding

3. Define the *Unregistered Multicast* field. The.
4. Click **Apply**. The Multicast Forward All settings are saved and the device is updated.

Chapter 12.Configuring SNMP

Simple Network Management Protocol (SNMP) provides a method for managing network devices. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. Access to the agent using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Access to the switch using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having its own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to “groups” that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as “views.”

The device has a default view (all MIB objects) and default groups defined for security models v1 and v2c. The following table shows the security models and levels available and the system default settings.

The SNMP agents maintain a list of variables, which are used to manage the device. The variables are defined in the *Management Information Base* (MIB). The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings.

The device is SNMP-compliant and contains an SNMP agent that supports a set of standard and private MIB variables. Developers of management stations require the exact structure of the MIB tree and receive the complete private MIBs information before being able to manage the MIBs.

All parameters are manageable from any SNMP management platform, except the SNMP management station IP address and community (community name and access rights). The SNMP management access to the device is disabled if no community strings exist.

This section contains the following topics:

- Enabling SNMP
- Defining SNMP Communities
- Defining SNMP Groups
- Defining SNMP Users
- Defining SNMP Views
- Defining Notification Recipients
- Defining Notification Filters

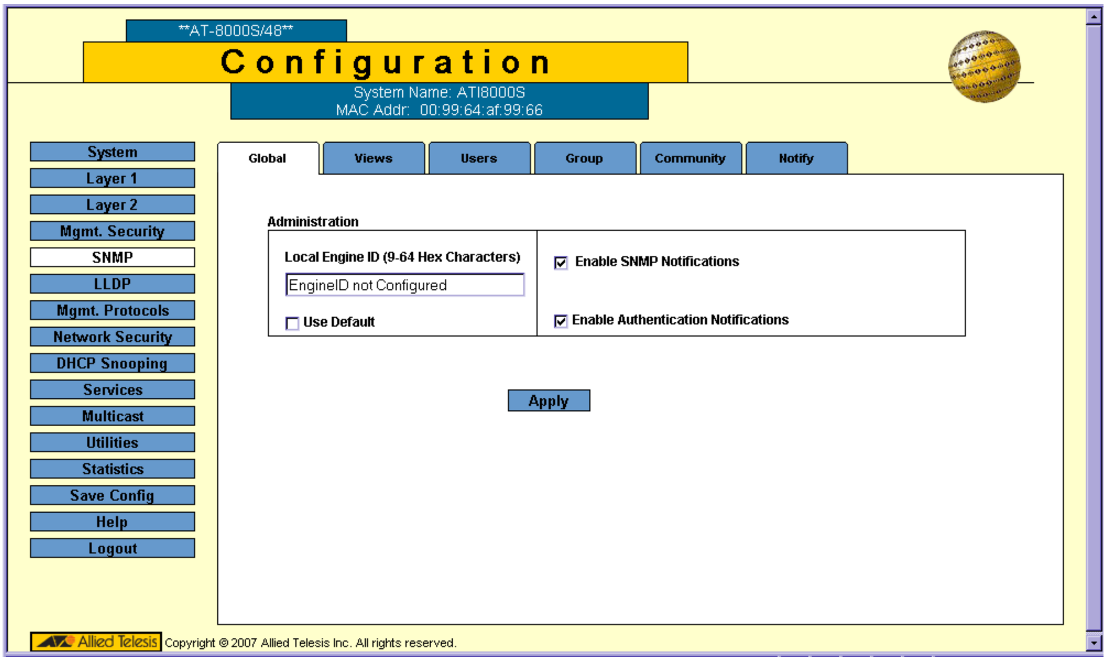
Enabling SNMP

The *SNMP Global Page* provides fields for globally enabling and configuring SNMP on the device.

To enable SNMP:

1. Click **SNMP > Global**. The *SNMP Global Page* opens:

Figure 109: SNMP Global Page



Administration

Local Engine ID (9-64 Hex Characters): EngineID not Configured

□ Use Default

☑ Enable SNMP Notifications

☑ Enable Authentication Notifications

The *SNMP Global Page* contains the following fields:

- **Local Engine ID (9-64 Hex Characters)** — Displays the engine number.
- **Use Default** — Restores default SNMP settings, using the Local Engine ID.
- **Enable SNMP Notifications** — Indicates if SNMP traps are enabled for the device. The possible values are:
  - *Checked* — Traps are enabled.
  - *Unchecked* — Traps are disabled.
- **Enable Authentication Notifications** — Indicates if notification messages are issued if unauthorized connection attempts occur. The possible values are:
  - *Checked* — Notifications are issued.
  - *Unchecked* — Notifications are not issued.

2. Define the fields.
3. Click **Apply**. The global SNMP settings are saved and the device is updated.

Defining SNMP Communities

Access rights are managed by defining communities in the *SNMP Community Page*. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMPv1 and SNMPv2c.

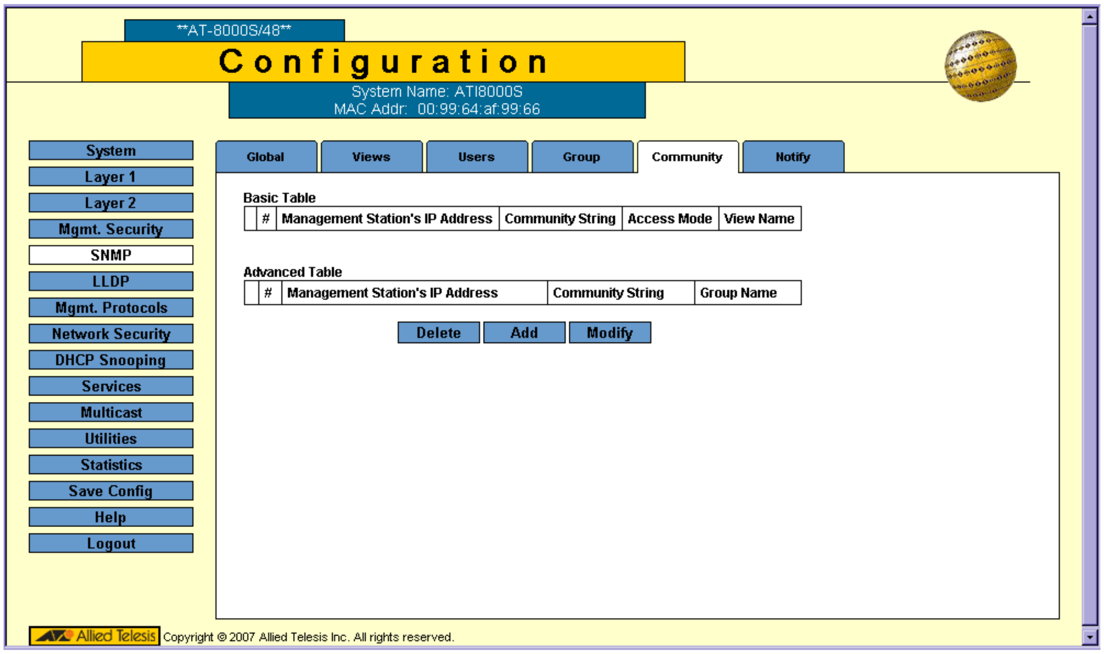
Note

The device switch is delivered with no community strings configured.

To define SNMP communities:

1. Click **SNMP > Community**. The *SNMP Global Page* opens. The *SNMP Community Page* opens:

Figure 110: SNMP Community Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Basic Table

	#	Management Station's IP Address	Community String	Access Mode	View Name

Advanced Table

	#	Management Station's IP Address	Community String	Group Name

The *SNMP Community Page* contains the Basic and the Advanced Table:

SNMP Communities Basic Table

The *SNMP Communities Basic Table* contains the following fields:

- **Management Station's IP Address** — Displays the management station IP address for which the basic SNMP community is defined. A value of *All* indicates all management station IP addresses.
- **Community String** — Defines the community name used to authenticate the management station to the device.

- **Access Mode** — Defines the access rights of the community. The possible field values are:
  - *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
  - *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
  - *SNMP Admin* — User has access to all device configuration options, as well as permissions to modify the community.
- **View Name** — Contains a list of user-defined SNMP views in addition to the Default and DefaultSuper views.

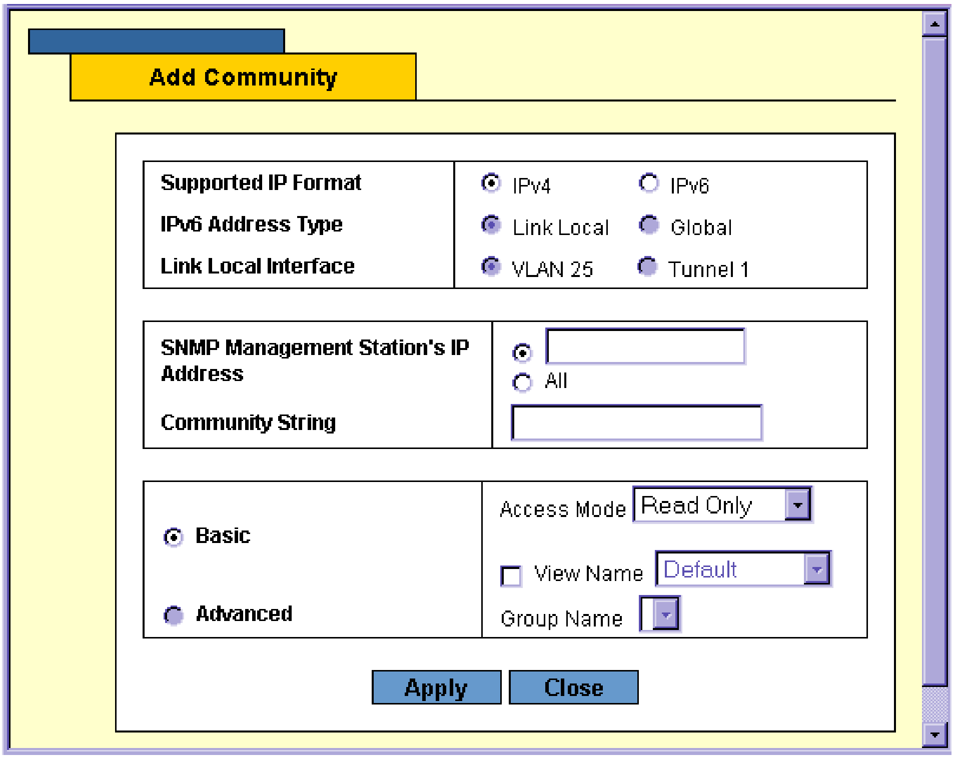
SNMP Communities Advanced Table

The *SNMP Communities Advanced Table* contains the following fields:

- **Management Station's IP Address** — Displays the management station IP address for which the advanced SNMP community is defined. A value of *0.0.0.0* indicates all management station IP addresses.
- **Community String** — Defines the community name used to authenticate the management station to the device.
- **Group Name** — Indicates the group that was assigned to the community.

2. Click the **Add** button. The *Add SNMP Community Page* opens.

Figure 111: Add SNMP Community Page



Add Community

Supported IP Format	● IPv4 ○ IPv6
IPv6 Address Type	● Link Local ● Global
Link Local Interface	● VLAN 25 ● Tunnel 1
SNMP Management Station's IP Address	● [ ] ○ All
Community String	[ ]
● Basic	Access Mode: Read Only
	□ View Name: Default
● Advanced	Group Name:

The *Add SNMP Community Page* contains the following fields:

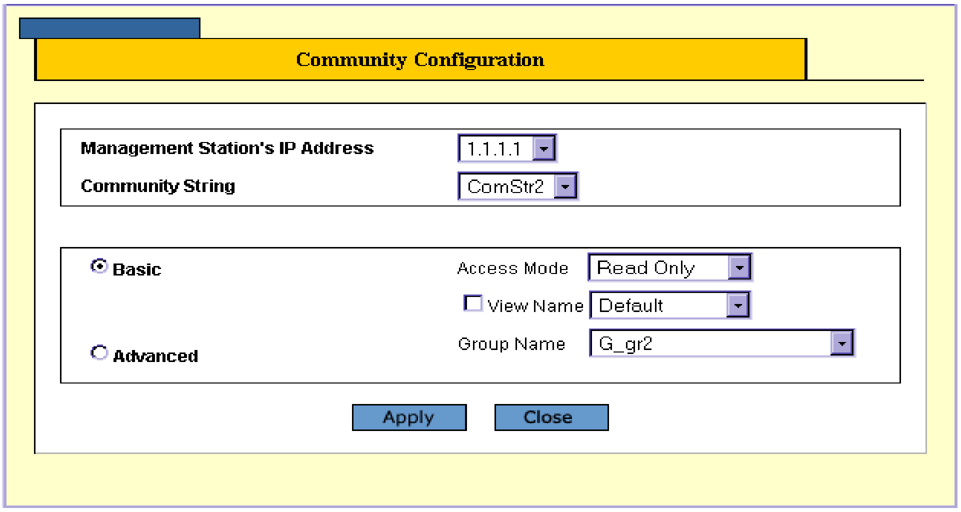
- **Supported IP Format** — Indicates the supported Internet Protocol on the device. The possible field values are:
  - *IPv4* — Indicates that IPv4 is supported.
  - *IPv6* — Indicates that IPv6 is supported.
- **IPv6 Address Type** — Defines the type of configurable static IPv6 IP address for an interface. The possible values are:
  - *Link Local* — Defines a Link Local address; non routable and can be used for communication on the same network only. A Link Local address has a prefix of 'FE80'.
  - *Global* — Defines a globally unique IPv6 address; visible and reachable from different subnets.
- **Link Local Interface** — Indicates the type of Link Local interface. The possible values are:
  - *VLAN 1*
  - *Tunnel 1*
- **SNMP Management Station's IP Address** — Displays the management station IP address for which the advanced SNMP community is defined. A value of *0.0.0.0* indicates all management station IP addresses.
- **Community String** — Defines the community name used to authenticate the management station to the device.
- **Basic** or **Advanced** mode.
- **Access Mode** — Defines the access rights of the community. The possible field values are:
  - *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
  - *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
  - *SNMP Admin* — User has access to all device configuration options, as well as permissions to modify the community.
- **View Name** — Contains a list of user-defined SNMP views in addition to the Default and DefaultSuper views
- **Group Name** — Indicates the group that was assigned to the community.

3. Define the fields.
4. Click **Apply**. The SNMP community is added, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

To modify SNMP community settings:

1. Select an SNMP community entry in the Basic table or in the Advanced Table.
2. Click **Modify**. The *Community Configuration Page* opens:

Figure 112: Community Configuration Page



Community Configuration

Management Station's IP Address: 1.1.1.1
Community String: ComStr2

● Basic
○ Advanced

Access Mode: Read Only
□ View Name: Default
Group Name: G_gr2

3. Define the **Basic** or **Advanced** configuration of the community.
4. Click **Apply**. The SNMP community settings are modified, and the device is updated.

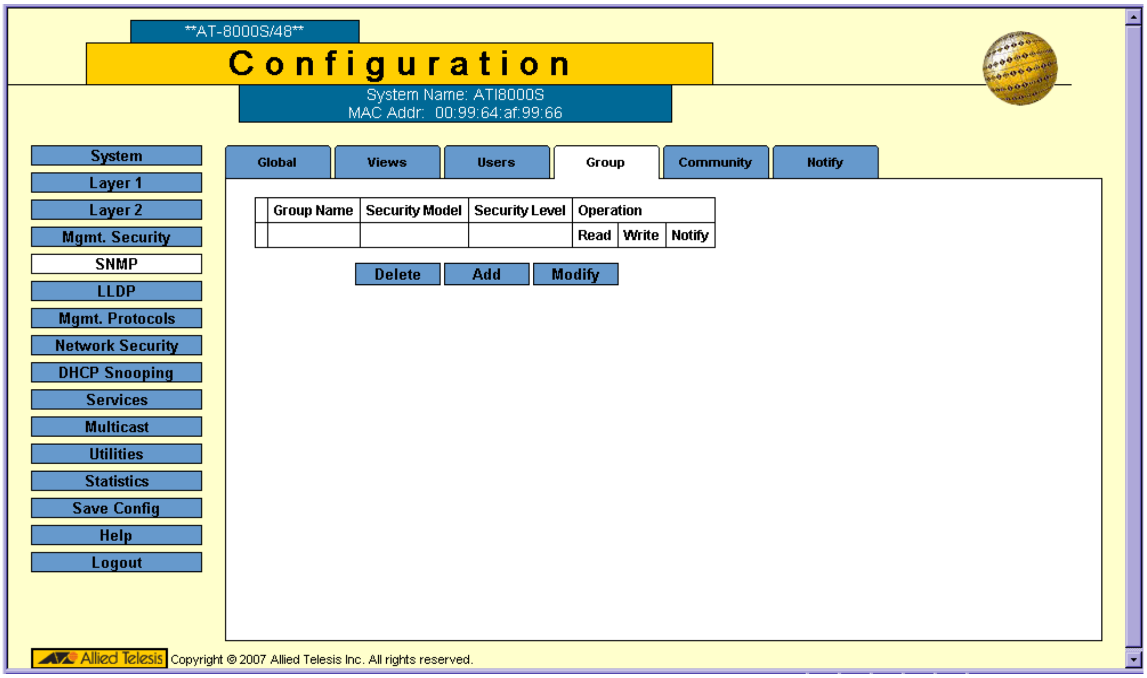
Defining SNMP Groups

The *SNMP Group Page* provides information for creating SNMP groups, and assigning SNMP access control privileges to SNMP groups. Groups allow network managers to assign access rights to specific device features, or feature aspects.

To define an SNMP group:

1. Click **SNMP > Groups**. The *SNMP Group Page* opens:

Figure 113: SNMP Group Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

	Group Name	Security Model	Security Level	Operation		
				Read	Write	Notify

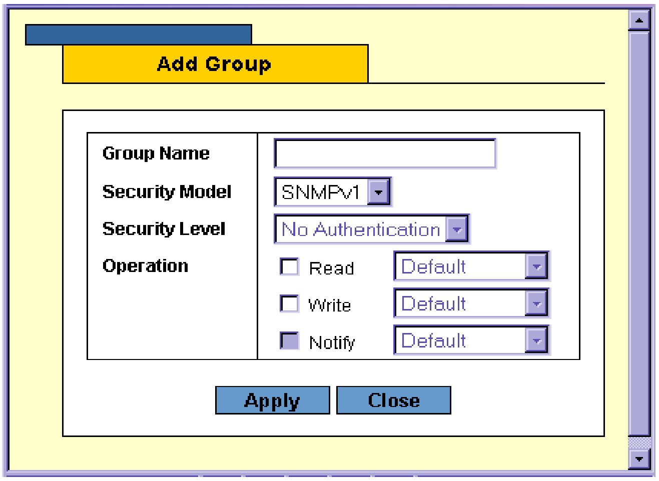
The *SNMP Group Page* contains the following fields:

- **Group Name** — Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  - *SNMPv1* — SNMPv1 is defined for the group.
  - *SNMPv2* — SNMPv2 is defined for the group.
  - *SNMPv3* — SNMPv3 is defined for the group.

- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are:
  - *No Authentication* — Indicates that neither the Authentication nor the Privacy security levels are assigned to the group.
  - *Authentication* — Authenticates SNMP messages, and ensures that the SNMP message's origin is authenticated.
  - *Privacy* — Encrypts SNMP messages.
- **Operation** — Defines the group access rights. The possible field values are:
  - *Read* — Management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.
  - *Write* — Management access is read-write and changes can be made to the assigned SNMP view.
  - *Notify* — Sends traps for the assigned SNMP view.

2. Click **Add**. The *Add Group Page* opens:

Figure 114: Add Group Page



Add Group

Group Name

Security Model: SNMPv1

Security Level: No Authentication

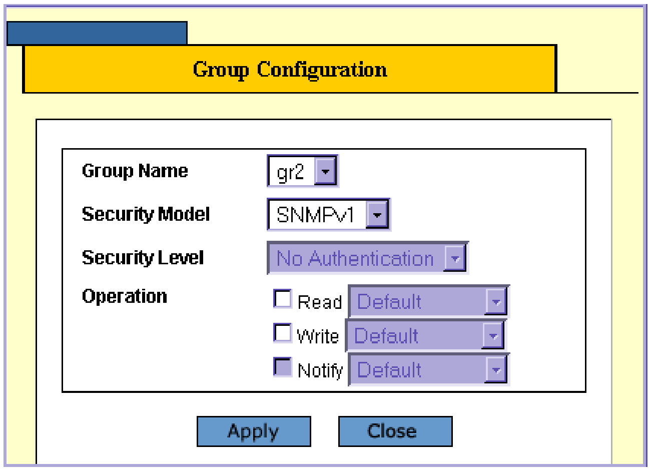
Operation:
☐ Read — Default
☐ Write — Default
☐ Notify — Default

3. Define the **Group Name**, **Security Level, Security Model**, and **Operation** fields.
4. Click **Apply**. The new SNMP group is saved.

To modify an SNMP group:

1. Click **SNMP > Groups**. The *SNMP Group Page* opens.
2. Click **Modify**. The *Group Configuration Page* opens:

Figure 115: Group Configuration Page



Group Configuration

Group Name: gr2

Security Model: SNMPv1

Security Level: No Authentication

Operation:
□ Read Default
□ Write Default
□ Notify Default

3. Define the **Group Name**, **Security Level**, **Security Model**, and **Operation** fields.
4. Click **Apply**. The SNMP group profile is saved.

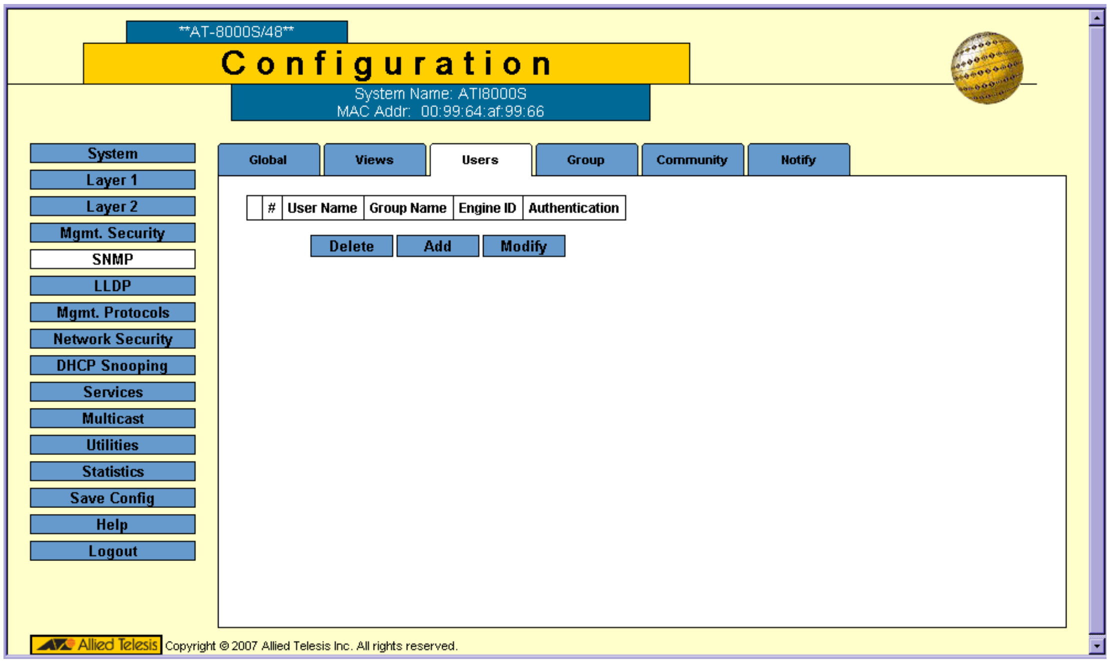
Defining SNMP Users

The *SNMP Users Page* enables assigning system users to SNMP groups, as well as defining the user authentication method.

To define SNMP group membership:

1. Click **SNMP > Users**. The *SNMP Users Page* opens:

Figure 116: SNMP Users Page



	#	User Name	Group Name	Engine ID	Authentication

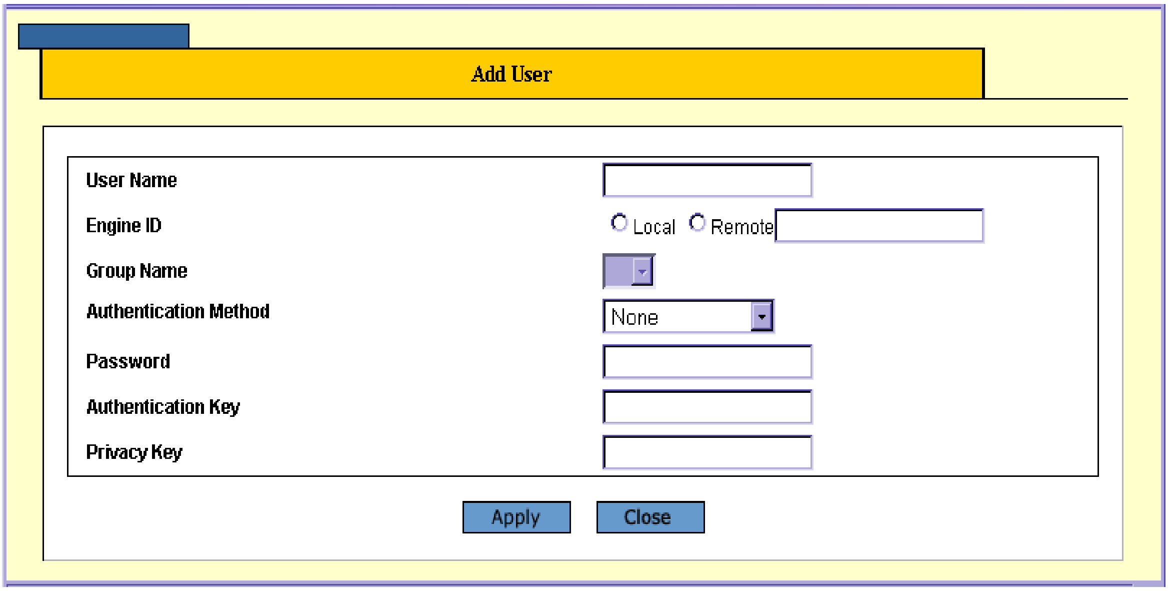
The *SNMP Users Page* contains the following fields:

- **User Name —** Contains a list of user-defined user names. The field range is up to 30 alphanumeric characters.
- **Group Name —** Contains a list of user-defined SNMP groups. SNMP groups are defined in the *SNMP Group Profile Page*.
- **Engine ID —** Displays either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 user database.
  - *Local* — Indicates that the user is connected to a local SNMP entity.
  - *Remote* — Indicates that the user is connected to a remote SNMP entity. If the Engine ID is defined, remote devices receive inform messages.

- **Authentication —** Displays the method used to authenticate users. The possible field values are:
  - *MD5 Key* — Users are authenticated using the HMAC-MD5 algorithm.
  - *SHA Key* — Users are authenticated using the HMAC-SHA-96 authentication level.
  - *MD5 Password* — The HMAC-MD5-96 password is used for authentication. The user should enter a password.
  - *SHA Password* — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.
  - *None* — No user authentication is used.

2. Click **Add**. The *Add SNMP User Page* opens.

Figure 117: Add SNMP User Page



Add User

User Name	
Engine ID	○ Local ○ Remote
Group Name	
Authentication Method	None
Password	
Authentication Key	
Privacy Key	

In addition to the *SNMP Users Page*, the *Add SNMP User Page* contains the following fields:

- **Authentication Method** — Defines the SNMP *Authentication* method. The possible field values are:
  - *MD5 Key* — Users are authenticated using the HMAC-MD5 algorithm.
  - *SHA Key* — Users are authenticated using the HMAC-SHA-96 authentication level.
  - *MD5 Password* — The HMAC-MD5-96 password is used for authentication. The user should enter a password.
  - *SHA Password* — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.
  - *None* — No user authentication is used.
- **Password** — Define the local user password. Local user passwords can contain up to 42 characters for MD5 or 32 characters for SHA.

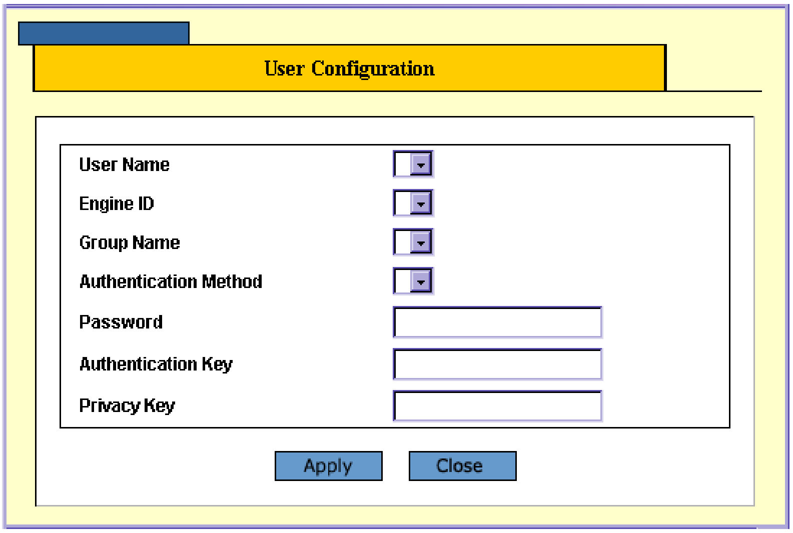
- **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined. If both privacy and authentication are required, 32 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon.
- **Privacy Key** — Defines the Privacy Key (LSB). If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 36 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.

3. Define the fields.
4. Click **Apply**. The SNMP user is added, and the device is updated.

To modify SNMP control privileges:

1. Click **SNMP > Users**. The *SNMP Users Page* opens.
2. Click **Modify**. The *SNMP User Configuration Page* opens:

Figure 118: SNMP User Configuration Page



User Configuration

User Name

Engine ID

Group Name

Authentication Method

Password

Authentication Key

Privacy Key

3. Define the fields.
4. Click **Apply**. The SNMP User is modified, and the device is updated.

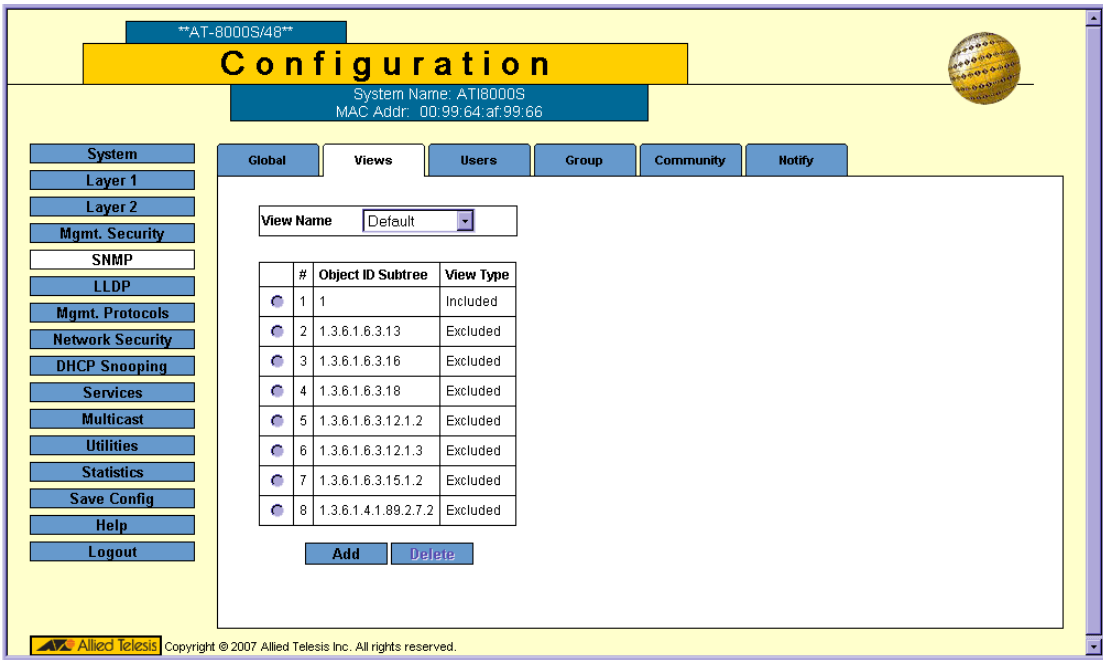
Defining SNMP Views

The SNMP views provide or block access to device features or portions of features. Feature access is granted via the MIB name or MIB Object ID.

To define SNMP views:

1. Click **SNMP > Views**. The *SNMP Views Page* opens:

Figure 119: SNMP Views Page



View Name: Default

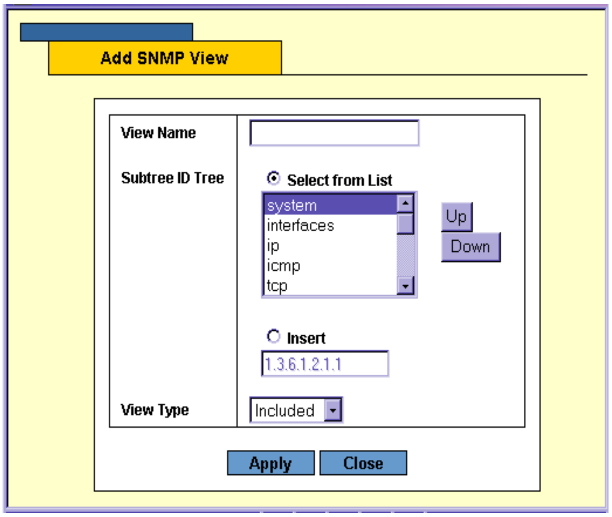
	#	Object ID Subtree	View Type
○	1	1	Included
○	2	1.3.6.1.6.3.13	Excluded
○	3	1.3.6.1.6.3.16	Excluded
○	4	1.3.6.1.6.3.18	Excluded
○	5	1.3.6.1.6.3.12.1.2	Excluded
○	6	1.3.6.1.6.3.12.1.3	Excluded
○	7	1.3.6.1.6.3.15.1.2	Excluded
○	8	1.3.6.1.4.1.89.2.7.2	Excluded

The *SNMP Views Page* contains the following fields:

- **View Name** — Displays the user-defined views. The view name can contain a maximum of 30 alphanumeric characters.
- **Object ID Subtree** — Displays the device feature OID included in or excluded from the selected SNMP view.
- **View Type** — Indicates whether the defined OID branch is to be included in or excluded from the selected SNMP view.

2. Click **Add**. The *Add SNMP VIew Page* opens:

Figure 120:Add SNMP VIew Page



Add SNMP View

View Name

Subtree ID Tree

● Select from List

system
interfaces
ip
icmp
tcp

○ Insert

1.3.6.1.2.1.1

View Type: Included

3. Define the *View Name* field.
4. Select the *Object ID Subtree* using one of the following options:
   - *Select from List* — Select the Subtree from the list provided. Pressing the *Up* and *Down* buttons allows you to change the priority by moving the selected subtree up or down in the list.
   - *Insert* — Enables a Subtree not included in the *Select from List* field to be entered.
5. Click **Apply**. The view is defined, and the device is updated.

Defining Notification Recipients

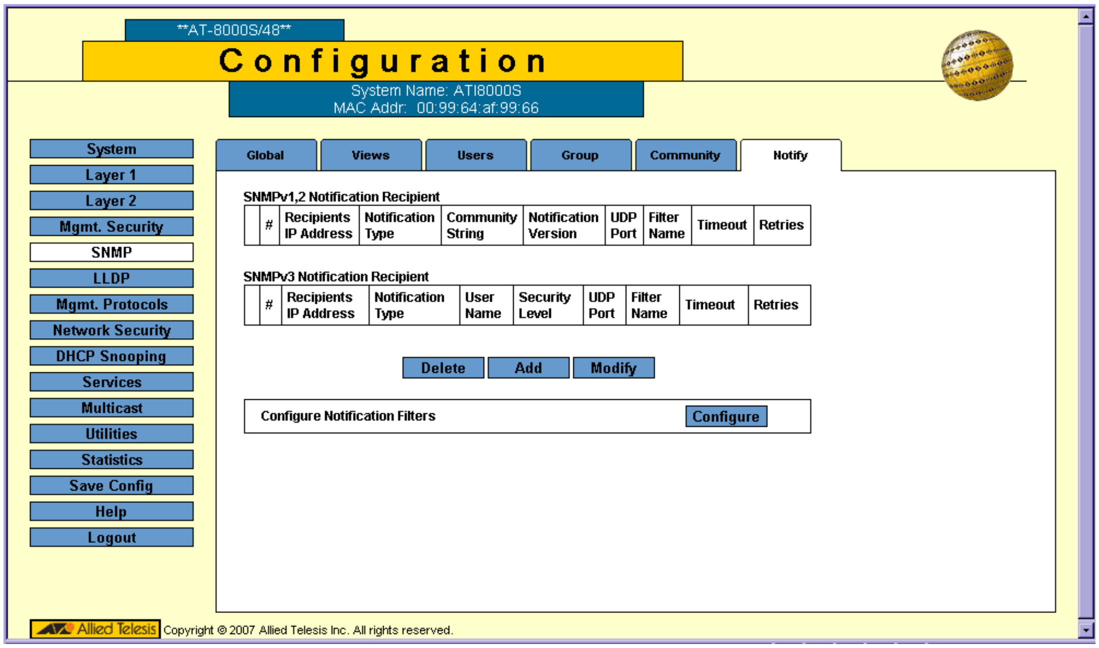
The *SNMP Notify Page* contains fields for defining SNMP notification recipients. The page contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

To configure SNMP notification recipients:

1. Click **SNMP > Notify**. The *SNMP Notify Page* opens:

Figure 121: SNMP Notify Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

SNMPv1,2 Notification Recipient

#	Recipients IP Address	Notification Type	Community String	Notification Version	UDP Port	Filter Name	Timeout	Retries

SNMPv3 Notification Recipient

#	Recipients IP Address	Notification Type	User Name	Security Level	UDP Port	Filter Name	Timeout	Retries

Configure Notification Filters

The *SNMP Notify Page* contains tables for SNMPv2 and SNMPv3 notification recipients and lists the following parameters:

SNMPv1,2c Notification Recipient

The *SNMP v1, v2c Recipient* table contains the following fields:

- **Recipients IP Address —** Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the type of notification sent. The possible field values are:
  - *Trap* — Indicates that traps are sent.
  - *Inform* — Indicates that informs are sent.
- **Community String** — Displays the community string of the trap manager.
- **Notification Version** — Displays the trap type. The possible field values are:
  - *SNMPV1* — Indicates that SNMP Version 1 traps are sent.
  - *SNMPV2c* — Indicates that SNMP Version 2 traps are sent.
- **UDP Port** — Displays the UDP port used to send notifications. The field range is 1-65535. The default is 162.
- **Filter Name** — Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (in seconds) the device waits before resending informs. The field range is 1-300. The default is 15 seconds.
- **Retries** — Indicates the number of times the device resends an inform request. The field range is 1-255. The default is 3.

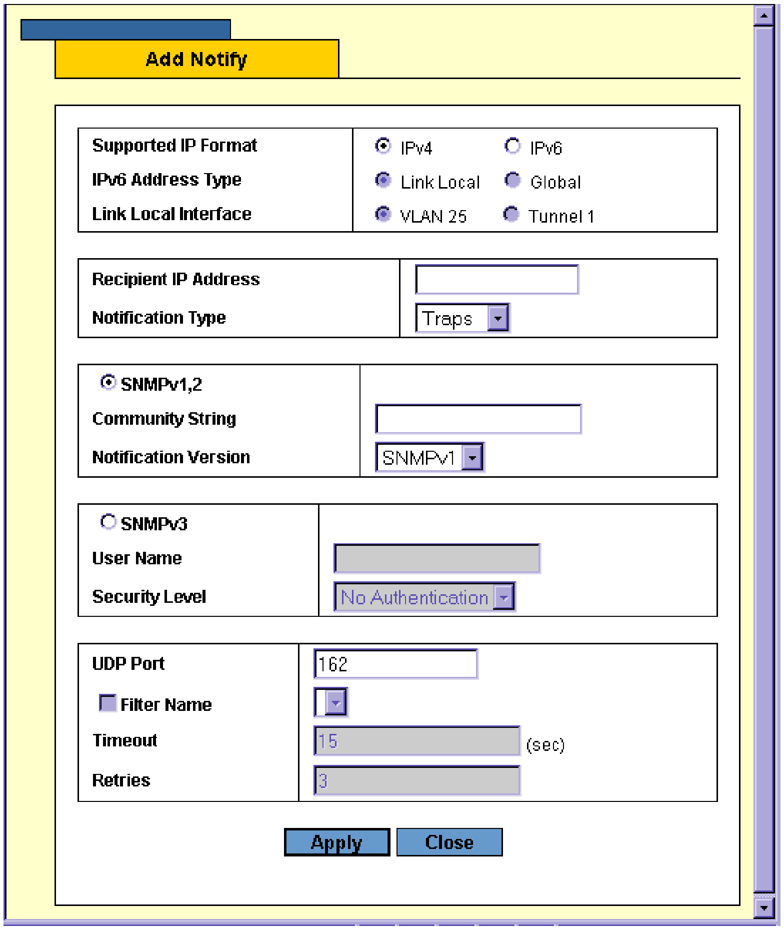
SNMPv3 Notification Recipient

The *SNMPv3 Notification Recipient* table contains the following fields:

- **Recipients IP Address** — Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the type of notification sent. The possible field values are:
  - *Trap* — Indicates that traps are sent.
  - *Inform* — Indicates that informs are sent.
- **User Name** — Displays the user to which SNMP notifications are sent.
- **Security Level** — Displays the means by which the packet is authenticated. The possible field values are:
  - *No Authentication* — Indicates that the packet is neither authenticated nor encrypted.
  - *Authentication* — Indicates that the packet is authenticated.
- **UDP Port** — Displays the UDP port used to send notifications. The field range is 1-65535. The default is 162.
- **Filter Name** — Includes or excludes SNMP filters.
- **Timeout** — Indicates the amount of time (in seconds) the device waits before resending informs. The field range is 1-300. The default is 15 seconds.
- **Retries** — Indicates the number of times the device resends an inform request. The field range is 1-255.The default is 3.

2. Click **Add**. The *Add Notify Page* opens:

Figure 122: Add Notify Page



Supported IP Format	● IPv4 ○ IPv6
IPv6 Address Type	● Link Local ● Global
Link Local Interface	● VLAN 25 ● Tunnel 1
Recipient IP Address	
Notification Type	Traps
● SNMPv1,2	
Community String	
Notification Version	SNMPv1
○ SNMPv3	
User Name	
Security Level	No Authentication
UDP Port	162
□ Filter Name	
Timeout	15 (sec)
Retries	3

In addition to the *SNMP Notify Page*, the *Add Notify Page* contains the following fields:

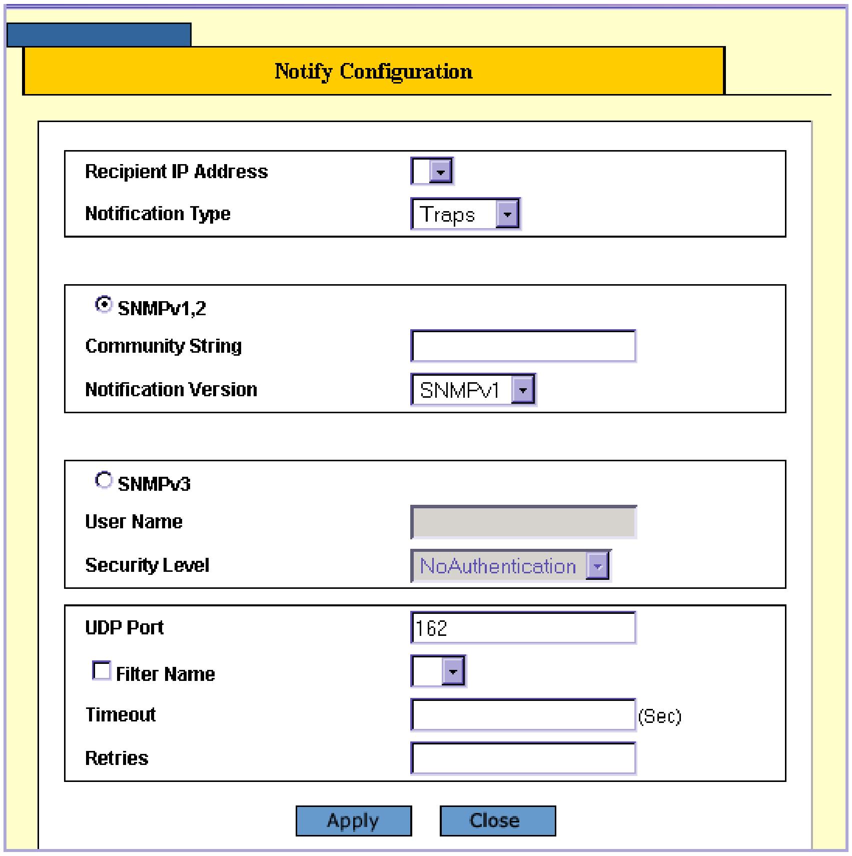
- **Supported IP Format** — Indicates the supported Internet Protocol on the device. The possible field values are:
  - *IPv4* — Indicates that IPv4 is supported.
  - *IPv6* — Indicates that IPv6 is supported.
- **IPv6 Address Type —** Defines the type of configurable static IPv6 IP address for an interface. The possible values are:
  - *Link Local* — Defines a Link Local address; non routable and can be used for communication on the same network only. A Link Local address has a prefix of 'FE80'.
  - *Global* — Defines a globally unique IPv6 address; visible and reachable from different subnets.
- **Link Local Interface —** Indicates the type of Link Local interface. The possible values are:
  - *VLAN 1*
  - *Tunnel 1*

3. Define the fields.
4. Click **Apply**. The notification recipient settings are saved and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

To modify notification settings:

1. Click **SNMP > Notify**. The *SNMP Notify Page* opens.
2. Select an entry from one of the tables and click **Modify**. The *SNMP Notify Configuration Page* opens.

Figure 123: SNMP Notify Configuration Page



Notify Configuration

Recipient IP Address	
Notification Type	Traps
● SNMPv1,2	
Community String	
Notification Version	SNMPv1
○ SNMPv3	
User Name	
Security Level	NoAuthentication
UDP Port	162
□ Filter Name	
Timeout	(Sec)
Retries	

3. Define the fields.
4. Click **Apply**. The SNMP Notification configuration is modified, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

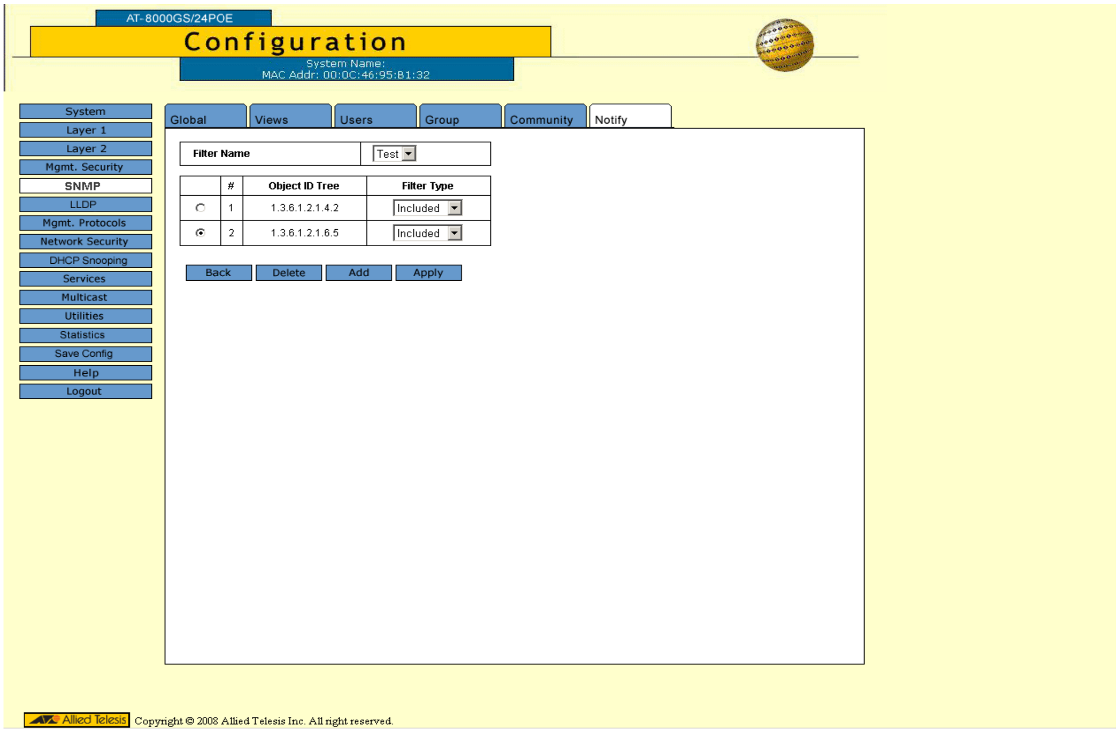
Defining Notification Filters

The *SNMP Notification Filter Page* permits filtering traps based on OIDs. Each OID is linked to a device feature or a portion of a feature. The *SNMP Notification Filter Page* also allows network managers to filter notifications.

To configure SNMP notification filters:

1. Click **SNMP > Notify**. The *SNMP Notify Page* opens.
2. Click **Configure** next to *Configure Notification Filters*. The *SNMP Notification Filter Configuration Page* opens:

Figure 124: SNMP Notification Filter Configuration Page



Filter Name	Test

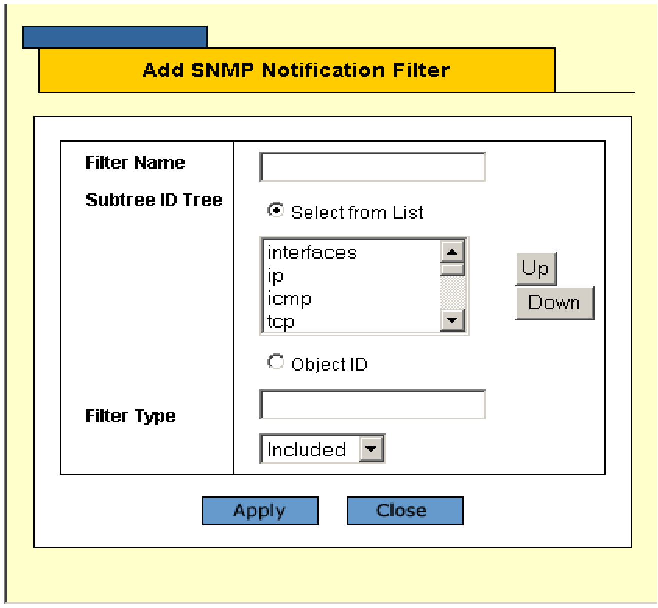
	#	Object ID Tree	Filter Type
○	1	1.3.6.1.2.1.4.2	Included
●	2	1.3.6.1.2.1.6.5	Included

3. Define the *Filter Name* and *Filter Type* fields.
4. Click **Apply**. The SNMP notification filter is defined, and the device is updated.
5. Click **Save Config** on the menu to save the changes permanently.

To add an SNMP notification filter:

1. Click the **Add** button. The *Add SNMP Notification Filter Page* opens:

Figure 125: Add SNMP Notification Filter Page



Add SNMP Notification Filter

Filter Name

Subtree ID Tree ● Select from List

interfaces
ip
icmp
tcp

○ Object ID

Filter Type: Included

The *Add SNMP Notification Filter Page* contains the following fields:

- **Filter Name** — Contains a list of user-defined notification filters.
- **Object ID Tree** — Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. Object IDs are selected from either the *Select from List* or the *Object* ID field. There are two configuration options:
  - *Select from List* — Select the OID from the list provided. Pressing the *Up* and *Down* buttons allows you to change the priority by moving the selected subtree up or down in the list.
  - *Object ID* — Enter an OID not offered in the *Select from List* option.
- **Filter Type** — Indicates whether informs or traps are sent regarding the OID to the trap recipients.
  - *Excluded* — Restricts sending OID traps or informs.
  - *Included* — Sends OID traps or informs.

2. Define the relevant fields.
3. Click **Apply.** The SNMP Notification Filter is added to the list, and the device is updated.
4. Click **Save Config** on the menu to save the changes permanently.

Chapter 13.Configuring LLDP

Link Layer Discovery Protocol (LLDP) is a Layer 2 protocol that allows a network device supporting the 802.1ab standard to advertise its identity and capabilities on a local network. LLDP allows network managers to troubleshoot and enhance network management by discovering and maintaining network topologies over multi-vendor environments. LLDP discovers network neighbors by standardizing methods for network devices to advertise themselves to other systems, and to store discovered information. Device discovery information includes:

- Device Identification
- Device Capabilities
- Device Configuration

The advertising device transmits multiple advertisement message sets in a single LAN packet. The multiple advertisement sets are sent in the packet Type Length Value (TLV) field. LLDP devices must support chassis and port ID advertisement, as well as system name, system ID, system description, and system capability advertisements.

This section includes the following topics:

- Defining Global LLDP Properties
- Defining LLDP Port Settings
- Defining LLDP Media Endpoint Discovery Network Policy
- Defining LLDP MED Port Settings
- Viewing the LLDP Neighbors Information

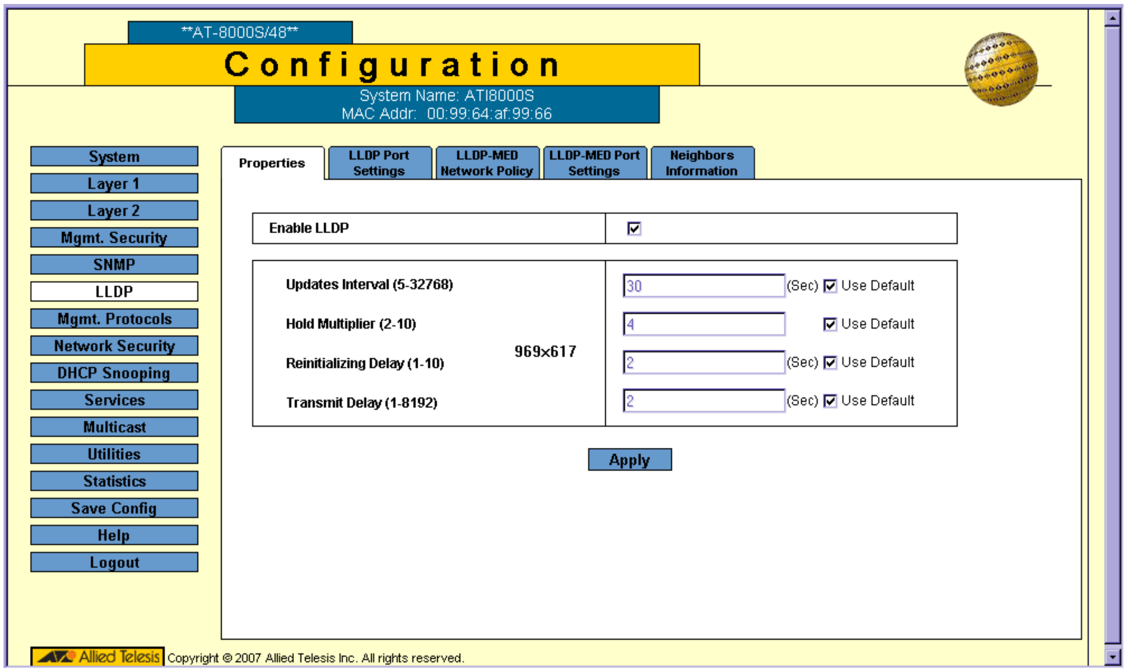
Defining Global LLDP Properties

The *LLDP Properties Page* allows network managers to assign global LLDP parameters.

To enable and configure LLDP on the device:

1. Click **LLDP > Properties**. The *LLDP Properties Page* opens:

Figure 126: LLDP Properties Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Enable LLDP	☑

Updates Interval (5-32768)	30 (Sec) ☑ Use Default
Hold Multiplier (2-10)	4 ☑ Use Default
Reinitializing Delay (1-10)	2 (Sec) ☑ Use Default
Transmit Delay (1-8192)	2 (Sec) ☑ Use Default

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *LLDP Properties Page* contains fields for configuring LLDP:

- **Enable LLDP** — Indicates if LLDP is enabled on the device. The possible field values are:
  - *Checked* —Enables LLDP on the device. This is the default value.
  - *Unchecked* — Disables LLDP on the device.
- **Updates Interval** (5 - 32768) — Indicates the interval (sec.) between consecutive LLDP advertisement updates The possible field range is 5 - 32768 seconds. The default value is 30 seconds.
  - *Use Default* — Selecting the check box returns settings to default.
- **Hold Multiplier** (2 - 10) — Indicates the amount of time that LLDP packets are held by a receiving device before the packets are discarded. The value represents a multiple of the Updates Interval. The possible field range is 2 - 10. The field default is 4. For example, if the Update Interval is 30 seconds and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds.
  - *Use Default* — Selecting the check box returns settings to default.
- **Reinitializing Delay** (1 - 10) — Indicates the amount of time an LLDP port waits before reinitializing LLDP transmissions. The possible field range is 1 - 10 seconds. The default value is 2 seconds.
  - *Use Default* — Selecting the check box returns settings to default.

- **Transmit Delay** (1 - 8192) — Indicates the amount of time that passes between successive LLDP frame transmissions due to changes in the LLDP local systems MIB. The possible field range is 1 - 8192 seconds. The default value is 2 seconds. A Tx delay < 0.25 is recommended for the TLV Adv Interval.
  - – *Use Default* — Selecting the check box returns settings to default.

2. Select Enable in the *LLDP Status* checkbox.
3. Define the rate at which LLDP advertisement updates are sent in the *TLV Advertised Interval Updates Interval* field.
4. Define how LLDP packets are held by a receiving device before the system discards the packets in the *Hold Multiplier* field.
5. Define how long an LLDP port waits before reinitializing LLDP transmissions in the *Reinitializing Delay* field.
6. Define how long the system waits between LLDP packet transmissions if a change has occurred in the MIB in the *Transmit Delay* field.
7. Click **Apply**. LLDP is enabled, the global LLDP parameters are defined, and the device is updated with its LLDP global configuration.

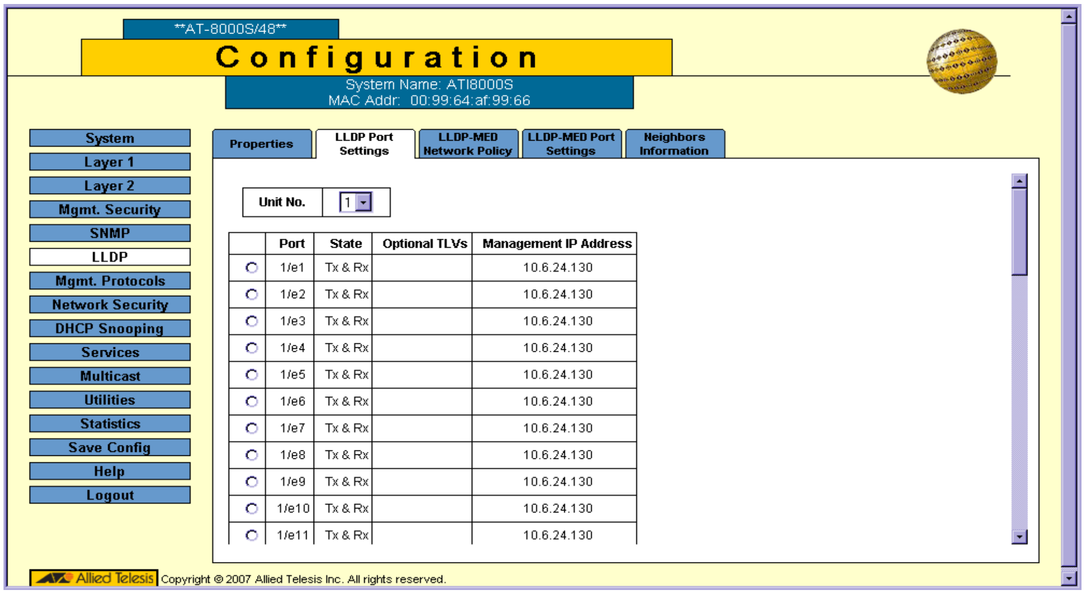
Defining LLDP Port Settings

The *LLDP Port Settings Page* allows network administrators to define LLDP port settings, including the port type, the LLDP port state, and the type of port information advertised.

To define LLDP Port Properties:

1. Click **LLDP > LLDP Port Settings**. The *LLDP Port Settings Page* opens:

Figure 127: LLDP Port Settings Page



Unit No. 1

	Port	State	Optional TLVs	Management IP Address
○	1/e1	Tx & Rx		10.6.24.130
○	1/e2	Tx & Rx		10.6.24.130
○	1/e3	Tx & Rx		10.6.24.130
○	1/e4	Tx & Rx		10.6.24.130
○	1/e5	Tx & Rx		10.6.24.130
○	1/e6	Tx & Rx		10.6.24.130
○	1/e7	Tx & Rx		10.6.24.130
○	1/e8	Tx & Rx		10.6.24.130
○	1/e9	Tx & Rx		10.6.24.130
○	1/e10	Tx & Rx		10.6.24.130
○	1/e11	Tx & Rx		10.6.24.130

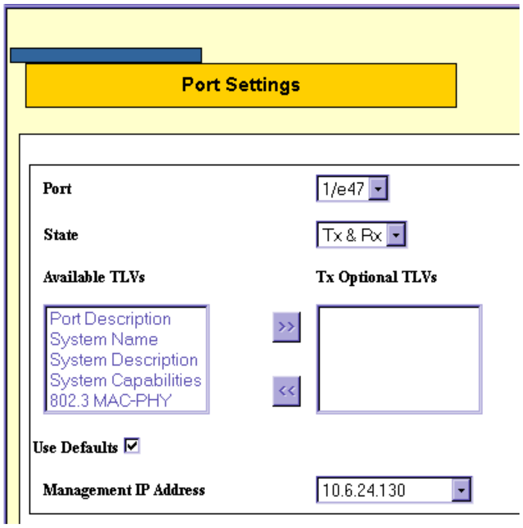
The *LLDP Port Settings Page* contains the following fields:

- **Unit No.** — Indicates the stacking member ports for which the LLDP parameters are displayed.
- **Port** — Specifies the list of ports on which LLDP can be configured.

- **State** — Indicates the LLDP state on the port. The possible field values are:
  - *Tx Only* — Enables transmitting LLDP packets only.
  - *Rx Only* — Enables receiving LLDP packets only.
  - *Tx & Rx* — Enables transmitting and receiving LLDP packets. This is the default value.
  - *Disable* — Indicates that LLDP is disabled on the port.
- **Optional TLVs** — Contains a list of optional TLVs advertised by the port. For the complete list, see the Available TLVs field.
- **Management IP Address** — Indicates the management IP address that is advertised from the interface. The possible field values are:
  - *Stop Advertising* — Indicates the IP address is not advertised. This is the default setting.
  - *IP Address* — Indicates that the IP address is advertised.

2. Click **Modify**. The *Modify Port Settings Page* opens:

Figure 128: Modify Port Settings Page



Port Settings

Port 1/e47

State Tx & Rx

Available TLVs: Port Description, System Name, System Description, System Capabilities, 802.3 MAC-PHY

Tx Optional TLVs

Use Defaults ☑

Management IP Address 10.6.24.130

3. Select the port for which the LLDP parameters are defined in the **Port** drop-down box.
4. Define whether LLDP are only transmitted, only received or both transmitted and received on the port in the **State** field.

   Or

   Select **Disable** to not transmit or receive LLDP packets.
5. Select the TLV to be transmitted by moving the TLVs from the **Available TLVs** list to the **Tx Optional TLVs** list.

   Or

   Select the **Use Default** checkbox to use the factory default settings.
6. Select the Management IP state in the **Management IP Address** drop-down box.
7. Click **Apply**. The Port LLDP settings are defined, and the device is updated.

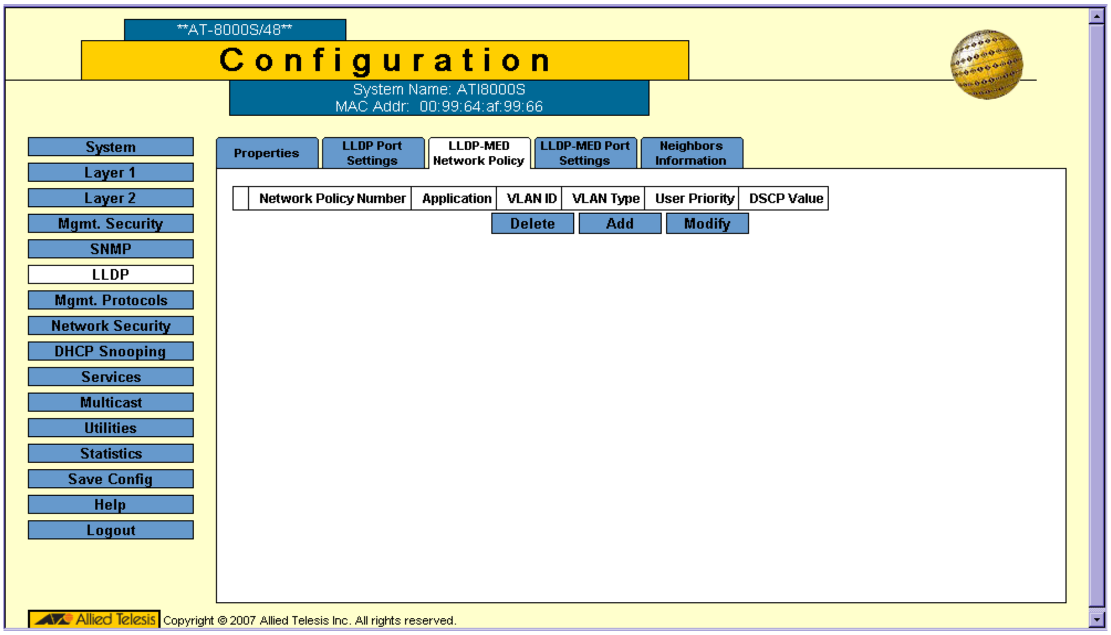
Defining LLDP Media Endpoint Discovery Network Policy

LLDP Media Endpoint Discovery (LLDP MED) is an enhancement to the 802.1ab standard. LLDP MED increases network flexibility by allowing different IP systems to co-exist on a single network. LLDP MED:

- Provides detailed network topology information, including what devices are located on the network, and where the devices are located. For example, what IP phone is connected to what port, what software is running on what switch, and what port is connected to what PC.
- Automatically deploys policies over networks for:
  - QoS Policies
  - Voice VLANs
- Provides Emergency Call Service (E-911) via IP Phone location information.
- Provides troubleshooting information. LLDP MED sends network managers alerts for:
  - Port speed and duplex mode conflicts
  - QoS policy misconfigurations

1. Click **LLDP > LLDP-MED Network Policy**. The *LLDP MED Network Policy Page* opens:

Figure 129: LLDP MED Network Policy Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

	Network Policy Number	Application	VLAN ID	VLAN Type	User Priority	DSCP Value

Copyright © 2007 Allied Telesis Inc. All rights reserved.

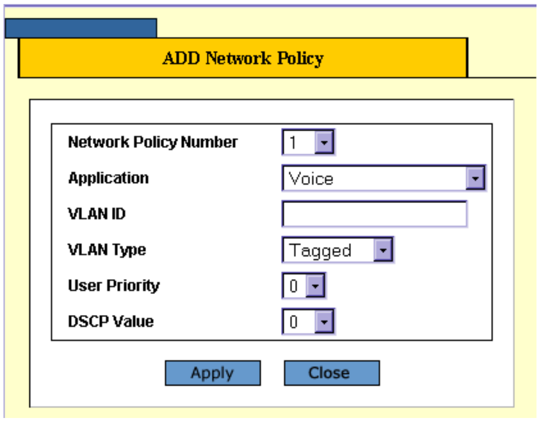
The *LLDP MED Network Policy Page* is used to define LLDP MED network policies. It contains the following fields:

- **Network Policy Number** — Displays the network policy number. The range of values is 1-32.
- **Application** — Displays the application for which the network policy is defined. The possible field values are:
  - *Voice* — Indicates that the network policy is defined for a Voice application.
  - *Voice Signaling* — Indicates that the network policy is defined for a Voice Signaling application.
  - *Guest VLAN* — Indicates that the network policy is defined for a Guest VLAN.

   - *Guest VLAN Signaling* — Indicates that the network policy is defined for a Guest VLAN Signalling application.
   - *Softphone Voice* — Indicates that the network policy is defined for a Softphone Voice application.
   - *Video Conferencing* — Indicates that the network policy is defined for a Video Conferencing application.
   - *Streaming Video* — Indicates that the network policy is defined for a Streaming Video application.
   - *Video Signaling* — Indicates that the network policy is defined for a Video Signalling application.
- **VLAN ID** — Displays the VLAN ID for which the network policy is defined.
- **VLAN Type** — Indicates the VLAN type for which the network policy is defined. The possible field values are:
   - *Tagged* — Indicates the network policy is defined for tagged VLANs.
   - *Untagged* — Indicates the network policy is defined for untagged VLANs.
- **User Priority** — Defines the user priority assigned to the network application.
- **DSCP Value** — Defines the DiffServe Code Point (DSCP) value assigned to the network policy. The possible field value is 0-63. For more information on DSCP, see Configuring Quality of Service.

2. Click **Add**. The *Add Network Policy Page* opens:

Figure 130: Add Network Policy Page



ADD Network Policy

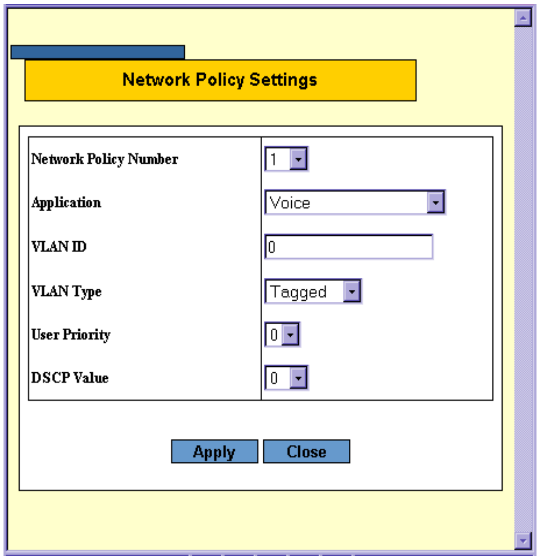
Network Policy Number	1
Application	Voice
VLAN ID	
VLAN Type	Tagged
User Priority	0
DSCP Value	0

3. Select the network policy number in the **Network Policy Number** field.
4. Define the Application type for which the network policy is defined in the **Application** field.
5. Define the VLAN assigned to the network policy in the **VLAN ID** field.
6. Define if the network policy is defined for tagged or untagged VLANs in the **VLAN Type** field.
7. Assign the network policy a user priority value in the **User Priority** field.
8. Define the DiffServe Code Point value attached to the policy in the **DSCP** field.
9. Click **Apply**. The LLDP network policy is defined, and the device is updated.

To modify a network policy setting:

1. Click **LLDP > Profile Rules**: The *LLDP MED Network Policy Page* opens.
2. Click **Modify**. The *Network Policy Settings Configuration Page* opens:

Figure 131: Network Policy Settings Configuration Page



Network Policy Number	1
Application	Voice
VLAN ID	0
VLAN Type	Tagged
User Priority	0
DSCP Value	0

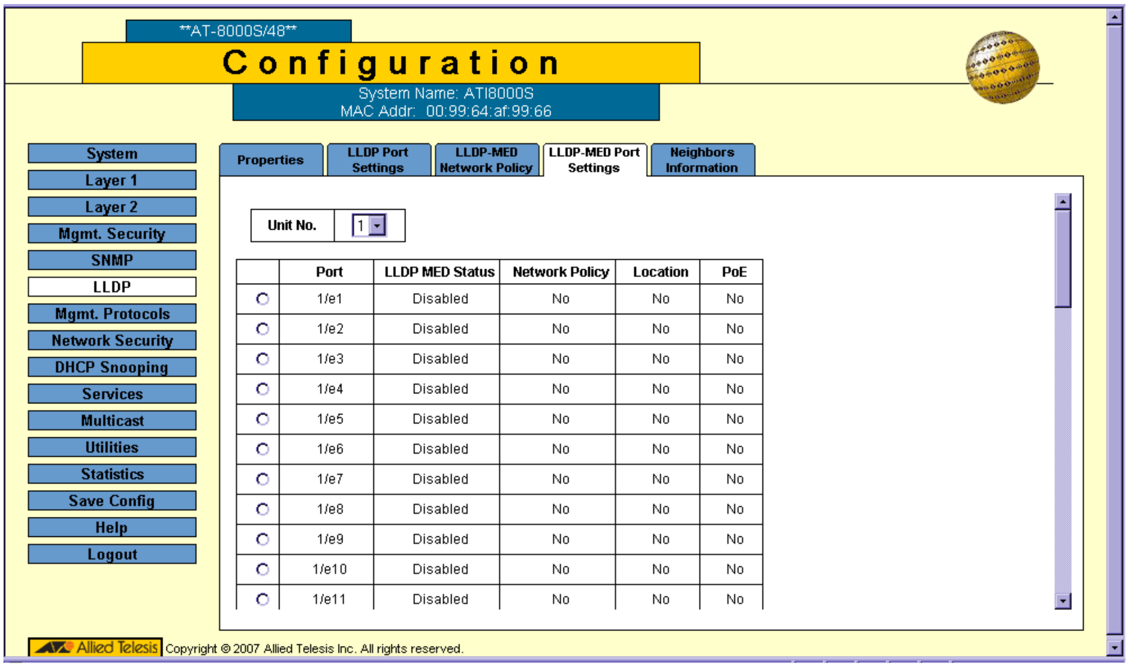
3. Define the fields.
4. Click **Apply**. The network policy setting is saved, and the device is updated.

Defining LLDP MED Port Settings

The *LLDP MED Port Settings Page* contains parameters for assigning LLDP network policies to specific ports. To configure LLDP MED port settings:

1. Click **LLDP > LLDP-MED Port Settings**. The *LLDP MED Port Settings Page* opens:

Figure 132: LLDP MED Port Settings Page



Unit No. 1

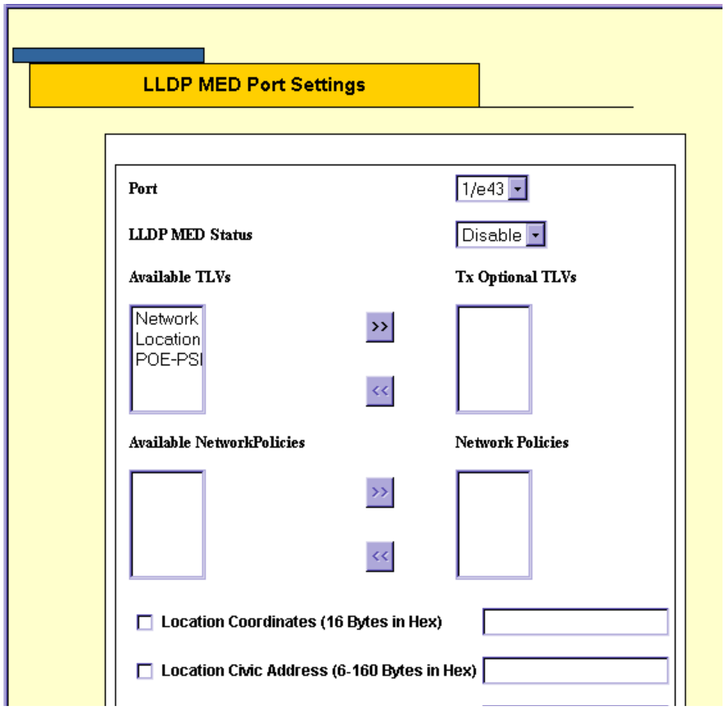
	Port	LLDP MED Status	Network Policy	Location	PoE
○	1/e1	Disabled	No	No	No
○	1/e2	Disabled	No	No	No
○	1/e3	Disabled	No	No	No
○	1/e4	Disabled	No	No	No
○	1/e5	Disabled	No	No	No
○	1/e6	Disabled	No	No	No
○	1/e7	Disabled	No	No	No
○	1/e8	Disabled	No	No	No
○	1/e9	Disabled	No	No	No
○	1/e10	Disabled	No	No	No
○	1/e11	Disabled	No	No	No

The *LLDP MED Port Settings Page* contains the following fields:

- **Unit No.** — Indicates the stacking member's ports for which the LLDP-MED port settings are displayed.
- **Port** — Specifies the list of ports to which LLDP-MED network policy can be attached.
- **LLDP MED Status** —Indicates the LLDP-MED port status, the possible field values are:
  - *Enable* — Indicates that LLDP-MED is enabled on the port.
  - *Disable* — Indicates that LLDP-MED is disabled on the port.
- **Network Policy** — Indicates LLDP MED network policy attached to the port.
- **Location** — Indicates if location identification is transmitted in LLDP packets.
- **PoE** — Indicates if PD-PSE information is transmitted in LLDP packets.

2. Click Modify. The *Modify LLDP MED Port Settings Page* opens:

Figure 133: Modify LLDP MED Port Settings Page



LLDP MED Port Settings

Port: 1/e43

LLDP MED Status: Disable

Available TLVs: Network, Location, POE-PSI

Tx Optional TLVs

Available NetworkPolicies

Network Policies

□ Location Coordinates (16 Bytes in Hex)

□ Location Civic Address (6-160 Bytes in Hex)

In addition to the fields in the *LLDP MED Port Settings Page*, the *Modify LLDP MED Port Settings Page* contains the following additional fields:

- **Available TLVs/Tx Optional TLVs** — Contains a list of available TLVs that can be advertised by the port. The possible field values are:
  - *Network Policy* — Advertises network policies attached to the port.
  - *Location* — Advertises the port's location.
  - *PoE-PSE* — Advertises the port PoE information.
- **Available Network Policies/Network Policy** — Contains a list of network policies that can be assigned to a port.
- **Location Coordinate** (16 Bytes in Hex) — Displays the device's location map coordinates.
- **Location Civic Address** (6-160 Bytes in Hex) — Displays the device's civic or street address location, for example 414 23rd Ave E. The possible field value are 6 - 160 bytes.
- **Location ECS ELIN** (10-25 Bytes in Hex) — Displays the device's ECS ELIN location. The field range is 10 - 25 bytes.

3. Select port in the **Port** field. The LLDP port settings are displayed in the fields.
4. Select **Enable** in the **LLDP MED Status** field.
5. Select the TLVs which are applied the port in the **Available TLVs/Tx Optional TLVs** list boxes. Move the TLVs between list boxes using the arrows.
6. Define the port location in the **Location Coordinate** (16 Bytes in Hex), **Location Civic Address** (6-160 Bytes in Hex), **Location ECS ELIN** (10-25 Bytes in Hex) fields.
7. Click **Apply**. The LLDP MED port settings are saved, and the device is updated.

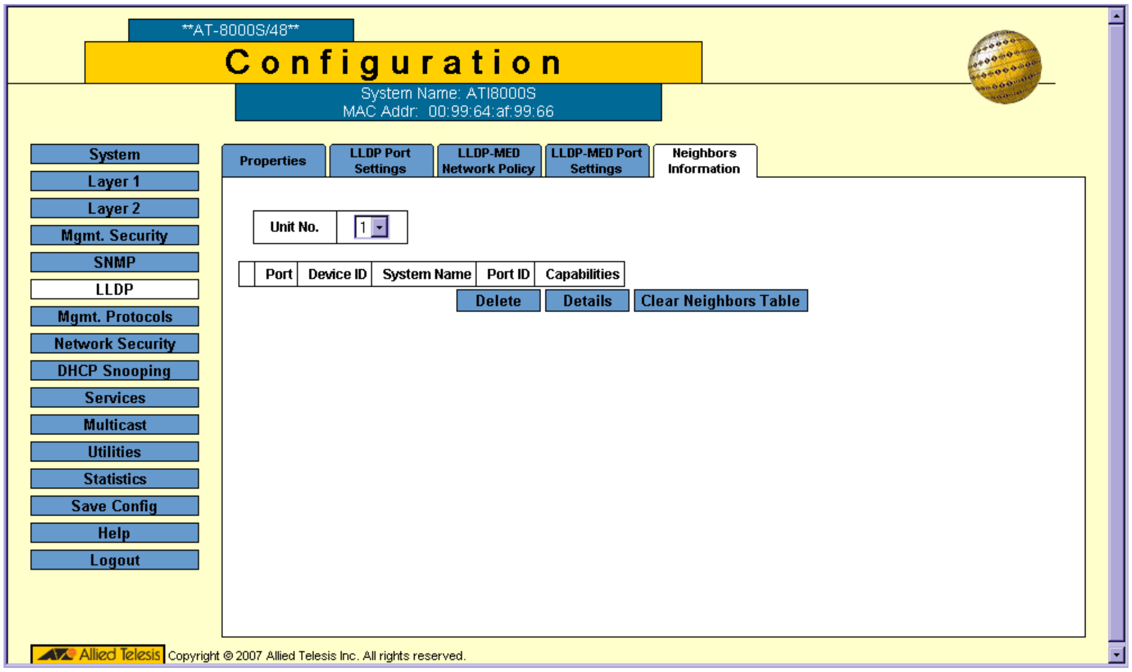
Viewing the LLDP Neighbors Information

The *LLDP Neighbors Information Page* contains information received from neighboring device LLDP advertisements.

To view LLDP Neighbor information:

1. Click **LLDP > Neighbors Information**. The *LLDP Neighbors Information Page* opens:

Figure 134: LLDP Neighbors Information Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Unit No. 1

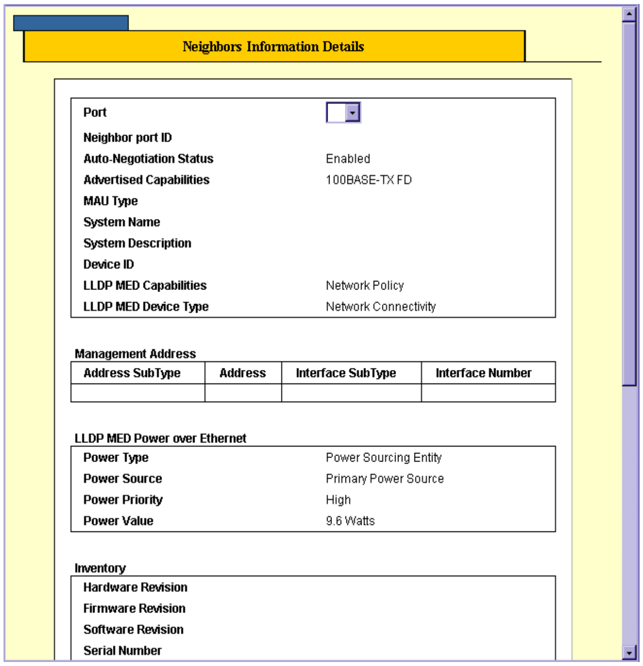
	Port	Device ID	System Name	Port ID	Capabilities

The *LLDP Neighbors Information Page* contains the following fields:

- **Unit No.** — Displays the stacking member's ports for which the LLDP neighbor information is displayed.
- **Port** — Displays the neighboring port number.
- **Device ID** — Displays the neighboring advertised port's device ID.
- **System Name** — Displays the user-defined system name.
- **Port ID** — Displays the neighboring port's ID.
- **Capabilities** — Displays the neighboring port's capabilities.

2. Click **Details** to view the *Neighbors Information Details Page* for ports.

Figure 135: Neighbors Information Details Page



Neighbors Information Details

Port	
Neighbor port ID	
Auto-Negotiation Status	Enabled
Advertised Capabilities	100BASE-TX FD
MAU Type	
System Name	
System Description	
Device ID	
LLDP MED Capabilities	Network Policy
LLDP MED Device Type	Network Connectivity

Management Address

Address SubType	Address	Interface SubType	Interface Number

LLDP MED Power over Ethernet

Power Type	Power Sourcing Entity
Power Source	Primary Power Source
Power Priority	High
Power Value	9.6 Watts

Inventory

Hardware Revision	
Firmware Revision	
Software Revision	
Serial Number	

The *Neighbors Information Details Page* contains the following fields:

- **Port** — The port for which detailed information is displayed.
- **Auto-Negotiation Status** — The auto-negotiation status of the port. The possible field values are:
  - *Enabled* — Auto-negotiation is enabled on the port.
  - *Disabled* — Auto-negotiation is disabled on the port.
- **Advertised Capabilities** — Displays the port capabilities advertised for the port.
- **MAU Type** — Indicates the media attachment unit type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network.
- **System Name** — Displays the advertised system name for the port.
- **System Description** — Displays the advertised system description for the port.
- **Device ID** — Displays the advertised port's device ID.
- **LLDP MED Capabilities** — Indicates the LLDP-MED capabilities that are advertised on the port.
- **LLDP MED Device Type** — Indicates whether a sender is a network connectivity device or an endpoint device.

Management Address

- **Address SubType** —Displays the management address's subtype.
- **Address** — Displays the management stations IP address.
- **Interface SubType** — Displays the management interface's subtype.
- **Interface Number** — Displays the management interface's ID number.

LLDP MED Power over Ethernet

The port PoE information.

- **Power Type** — Indicates the power type advertised on the port.
- **Power Source** — Indicates the power source advertised on the port.
- **Power Priority** — Indicates the port’s power priority advertised on the port.
- **Power Value** — Indicates the port’s power value, in Watts advertised on the port.

Inventory

- **Hardware Revision** — Displays the hardware version number.
- **Firmware Revision** — Displays the firmware version number.
- **Software Revision** —Displays the software version number.
- **Serial Number** — Displays the device serial number.
- **Model Name** — Displays the device model name.
- **Asset ID** — Displays the device asset ID.

LLDP MED Network Policy

- **Application Types** — Indicates the port’s LLDP Network Policy for each of the following:
  - *Voice*
  - *Voice Signaling*
  - *Guest VLAN*
  - *Guest VLAN Signaling*
  - *Softphone Voice*
  - *Video Conferencing*
  - *Streaming Video*
  - *Video Signaling*
- **Flags** — Displays the VLAN tagging status for the application type. The possible field values are:
  - *Tagged* — The packets are tagged.
  - *Untagged* — The packets are not tagged.
- **VLAN ID** — Displays the VLAN ID attached to the LLDP-MED network policy.
- **User Priority** — Displays the User Priority attached to the LLDP-MED network policy.
- **DSCP** — Displays the DSCP value attached to the LLDP-MED network policy. The possible field value is 0-63.

LLDP MED Location

- **Location Type** — The port’s advertised LLDP-MED location of the following:
  - *Coordinates* — Displays the device’s location map coordinates.
  - *Civic Address* — Displays the device’s civic or street address location, for example 414 23rd Ave E. The possible field value are 6 - 160 bytes.
  - *ECS ELIN* — Displays the device’s ECS ELIN location. The field range is 10 - 25 bytes.
- **Location Address** — The location as described.

3. Select the port for which you want to see the LLDP MED neighbors information details.

Chapter 14.Configuring Power Over Ethernet

This section describes configuring *Power over Ethernet* (PoE) for an AT-S9 device. PoE only applies to the supporting AT-8000S devices.

Power-over-Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power-over-Ethernet removes the necessity of placing network devices next to power sources. Power-over-Ethernet can be used in the following applications:

- IP phones
- Wireless Access Points
- IP gateways
- PDAs
- Audio and video remote monitoring

Powered Devices are devices which receive power from the device power supplies, for example IP phones. Powered Devices are connected to the device via Ethernet ports.

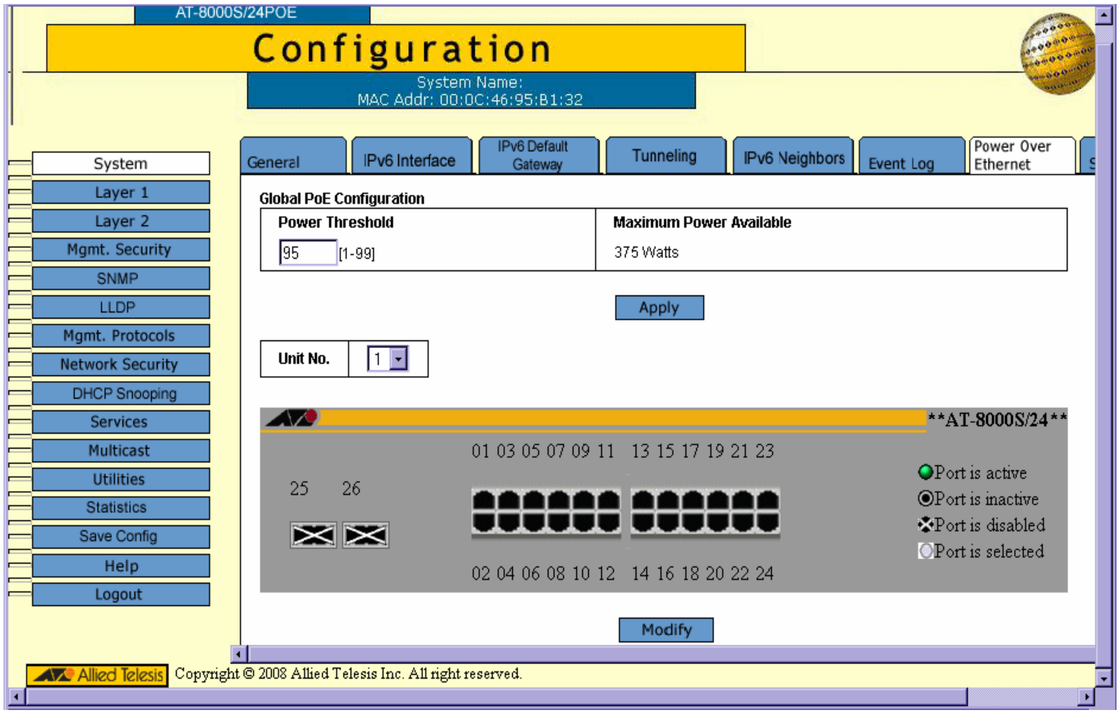
The PoE threshold is a percentage of the total maximum PoE power on the device (375 W). If the total power requirements of the powered devices exceed this threshold, the device sends an SNMP trap to the management workstation and enters an event in the event log. The threshold is adjustable. For management workstations to receive traps from the device, configure SNMP on the device by specifying the IP addresses of the workstations.

The *Power Over Ethernet Page* contains system PoE information for enabling PoE on the device, monitoring the current power usage, and enabling PoE traps.

To enable PoE for the device:

1. Click **System > Power Over Ethernet**. The *Power Over Ethernet Page* opens:

Figure 136: Power Over Ethernet Page



System Name:
MAC Addr: 00:0C:46:95:B1:32

Global PoE Configuration

Power Threshold	Maximum Power Available
95 [1-99]	375 Watts

Unit No. 1

● Port is active
◉ Port is inactive
✖ Port is disabled
○ Port is selected

Copyright © 2008 Allied Telesis Inc. All right reserved.

The *Power Over Ethernet Page* contains the following fields:

Global PoE Configuration

- **Power Threshold** — Indicates the percentage of power consumed before an alarm is generated. The value range is 1-99 percent; the default value is 95 percent.

  If maximum power available is 375 W, and the power threshold is 95%, the threshold is exceeded when the PoE devices require more than 356.25 W.

- **Maximum Power Available** — Indicates the maximum power allocated to the device.
- **Unit Number** — Indicates the stacking member for which the PoE information is displayed.

The Zoom View shows device ports and indicators of current PoE port status. The possible port settings are:

● *Port is active* — Indicates that the port is linked.

◉ *Port is inactive* — Indicates that the port is not linked.

✖ *Port is disabled* — Indicates that the port is disabled.

○ *Port is selected* — Indicates that the port is selected for modification.

2. Click the ports to enable. Clicking a port toggles it through the possible settings.
3. Define the fields.

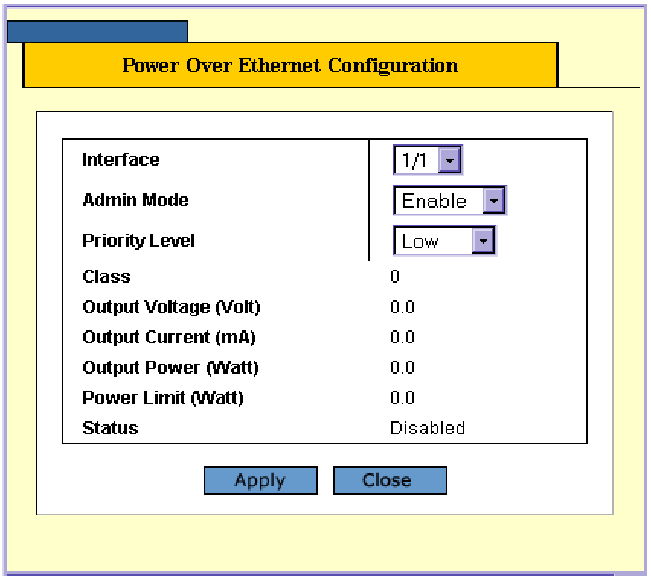
4. Click **Modify**. PoE is enabled on the device and global settings are saved. The new threshold is immediately activated on the device.
5. Click **Save Config** on the menu to permanently save the change.

Defining Power Over Ethernet Configuration

To modify PoE port settings:

1. In the *Power Over Ethernet Page* Zoom View, click the port(s) to modify. The port indication changes to *Port is selected*.
2. Click **Modify**. The *Power Over Ethernet Configuration Page* opens:

Figure 137: Power Over Ethernet Configuration Page



Power Over Ethernet Configuration

Interface	1/1
Admin Mode	Enable
Priority Level	Low
Class	0
Output Voltage (Volt)	0.0
Output Current (mA)	0.0
Output Power (Watt)	0.0
Power Limit (Watt)	0.0
Status	Disabled

The *Power Over Ethernet Configuration Page* displays the currently configured PoE ports and contains the following information:

- **Interface** — Displays the selected port's number.
- **Admin Mode** — Indicates whether PoE is enabled or disabled on the port. The possible values are:
  - *Enable* — Enables PoE on the port. This is the default setting.
  - *Disable* — Disables PoE on the port.
- **Priority Level** — Indicates the PoE ports' priority. The possible values are: Critical, High and Low. The default is Low.
- **Class** — Indicates the power class, the IEEE 802.3af class of the device.
- **Output Voltage (Volt)** — The voltage delivered to the powered device.
- **Output Current (mA)** — The current drawn by the powered device.
- **Output Power (Watt)** — Indicates the power being supplied to the device, in Watts.
- **Power Limit (Watt)** — Indicates the maximum amount of power allowed by the port for the device. The default is 15400 milliwatts (15.4 W), and the range is 3000 -15400 milliwatts.
- **Status** — Indicates the state of a PoE-enabled port. The possible field values are:
  - *On* — Indicates the device is delivering power to the interface.
  - *Off* — Indicates the device is not delivering power to the interface.
  - *Searching* — Indicates that the device is currently searching for a powered device. Searching is the default PoE operational status.

- *Fault* — Indicates one of the following:
  - –The powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device.
  - –The device has detected a fault on the powered device. For example, the powered device memory could not be read.
- *Test* — Indicates the powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply.

3. Modify the *Admin Mode* and *Priority Level* fields.
4. Click **Apply**. The PoE settings are saved and the device is updated.
5. Click **Save Config** on the menu, to save the settings permanently.

Section 15. Configuring Services

This section describes Quality of Service related configurations. QoS supports activating one of the following Trust settings:

- VLAN Priority Tag
- DiffServ Code Point
- None

Only packets that have a Forward action are assigned to the output queue, based on the specified classification. By properly configuring the output queues, the following basic mode services can be set:

- **Minimum Delay** — The queue is assigned to a strict priority policy, and traffic is assigned to the highest priority queue.
- **Best Effort** — Traffic is assigned to the lowest priority queue
- **Bandwidth Assignments** — Bandwidths are assigned by configuring the WRR scheduling scheme.

After packets are assigned to a specific egress queue, Class of Service (CoS) services can be assigned to the queue. Egress queues are configured with a scheduling scheme by one of the following methods:

- **Strict Priority** — Ensures that time-sensitive applications are always forwarded. Strict Priority (SP) allows the prioritization of mission-critical, time-sensitive traffic over less time-sensitive applications. For example, under SP, voice over IP (VoIP) traffic can be prioritized so that it is forwarded before FTP or e-mail (SMTP) traffic.
- **Weighted Round Robin** — Ensures that a single application does not dominate the device forwarding capacity. Weighted Round Robin (WRR) forwards entire queues in a round robin order. All queues can participate in WRR, except SP queues. SP queues are serviced before WRR queues. If the traffic flow is minimal, and SP queues do not occupy the whole bandwidth allocated to a port, the WRR queues can share the bandwidth with the SP queues. This ensures that the remaining bandwidth is distributed according to the weight ratio.

When configuring QoS for stacking, note that stacking only uses three queues.

This section contains the following topics:

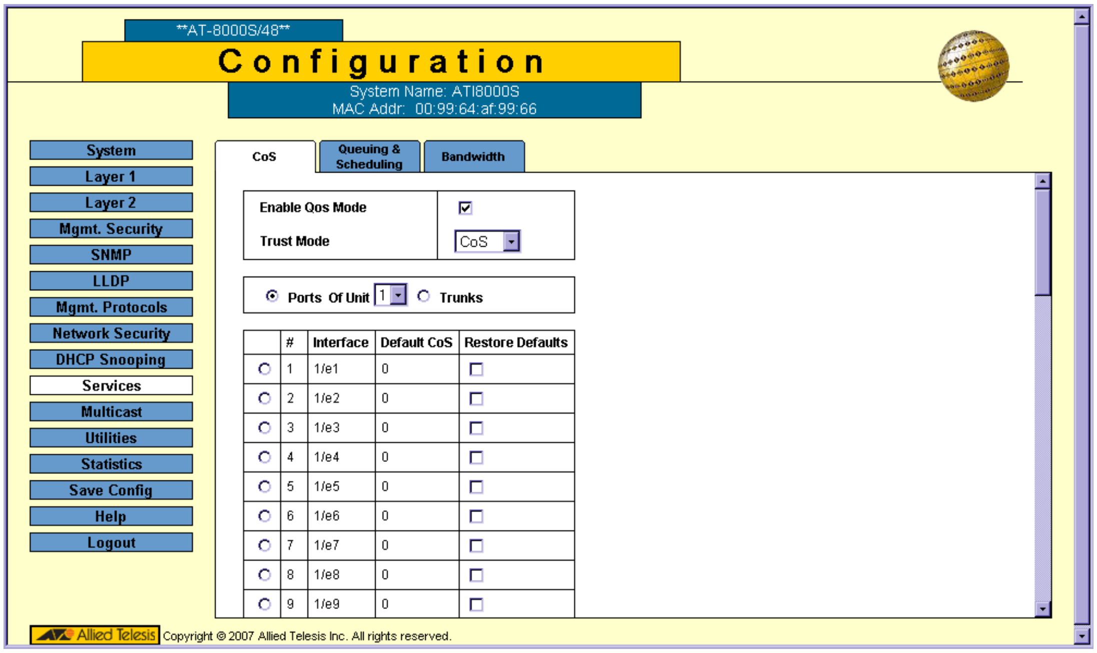
Enabling Class of Service (CoS)

The *CoS Page* enables configuring the CoS ports or trunks on the device.

To configure CoS ports or trunks on the device:

1. Click **Services > CoS**. The *CoS Page* opens:

Figure 138: CoS Page



Enable Qos Mode	☑
Trust Mode	CoS

● Ports Of Unit 1 ○ Trunks

	#	Interface	Default CoS	Restore Defaults
○	1	1/e1	0	□
○	2	1/e2	0	□
○	3	1/e3	0	□
○	4	1/e4	0	□
○	5	1/e5	0	□
○	6	1/e6	0	□
○	7	1/e7	0	□
○	8	1/e8	0	□
○	9	1/e9	0	□

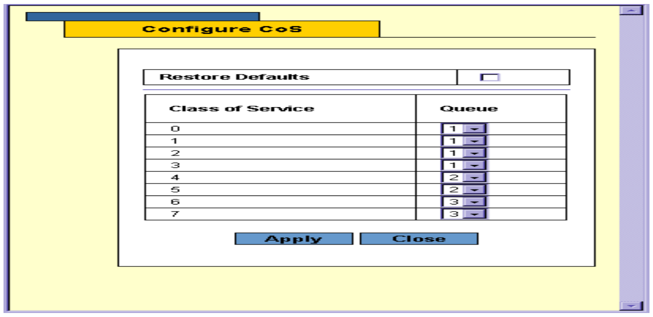
As a default the *CoS Page* opens displaying the port options. The fields are identical when displaying the trunk CoS. The *CoS Page* contains the following fields:

- **Enable QoS Mode** — Indicates if QoS is enabled on the device. The possible values are:
  - *Checked* — Enables QoS on the device.
  - *Unchecked* — Disables QoS on the device.
- **Trust Mode** — Defines which packet fields to use for classifying packets entering the device. When no rules are defined, the traffic containing the predefined packet CoS field is mapped according to the relevant trust modes table. Traffic not containing a predefined packet field is mapped to best effort. The possible Trust Mode field values are:
  - *CoS* — Classifies traffic based on the CoS tag value.
  - *DSCP* — Classifies traffic based on the DSCP tag value.
- Select the interfaces displayed in the table.
  - *Ports of Unit* — Specifies the port and stacking member for which the CoS configuration is displayed.
  - *Trunk* — Specifies the trunk for which the CoS configuration is displayed.

- **Interface** — Displays the interface number.
- **Default CoS**— Determines the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are 0-7. The default CoS is 0. This field appears in the CoS Ports table.
- **Restore Defaults** — Restores the factory CoS defaults. The possible field values are:
  - *Checked* — Restores the factory CoS defaults on the interface.
  - *Unchecked* — Maintains the current CoS settings. This is the default value.

2. Select the interfaces.
3. Check the **Restore Defaults** option, where needed.
4. Click **Modify**. The *CoS Configuration Page* opens:

Figure 139: CoS Configuration Page



Configure CoS

Restore Defaults	□

Class of Service	Queue
0	1
1	1
2	1
3	1
4	2
5	2
6	3
7	3

The *CoS Configuration Page* contains the following fields:

- **Interface** — Sets this CoS configuration for a port or trunk.
  - *Port* — Defines CoS for a specific port.
  - *Trunk* — Defines CoS for a specific trunk.
- **Set Default User Priority** — Indicates the priority level for CoS on the selected port/trunk. Default Priority determines the default CoS value for incoming packets. The value range is 0-7 and the default is 0.

5. Select the *Interface* and the *Priority* level.
6. Click **Apply**. The CoS settings for the selected port/trunk are updated.
7. Click **Save Config** on the menu to save the changes permanently.

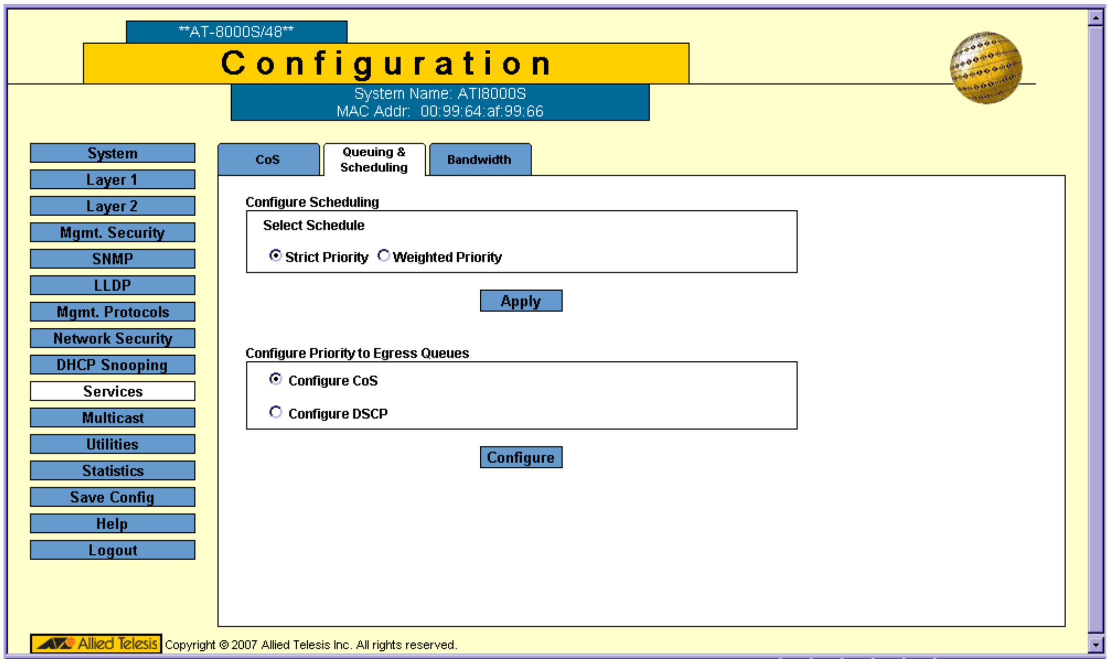
Configuring CoS Queueing and Scheduling

The *CoS Queuing & Scheduling Page* provides fields for configuring CoS Priority to Egress Queues and for defining Egress Weights. The queue settings are set system-wide. When configuring QoS for stacking, note that stacking only uses three queues.

To define schedule and queue settings for Quality of Service:

1. Click **Services > Queuing & Scheduling**. The *CoS Queuing & Scheduling Page* opens:

Figure 140: CoS Queuing & Scheduling Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Configure Scheduling

Select Schedule

● Strict Priority ○ Weighted Priority

Configure Priority to Egress Queues

● Configure CoS

○ Configure DSCP

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *CoS Queuing & Scheduling Page* contains scheduling and Priority Queue settings for the defined CoS and DSCP and contains the following fields:

- **Select Schedule** — Defines the priority method in queuing.
  - *Strict Priority* — Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.
  - *Weighted Priority* — Indicates that traffic scheduling for the selected queue is based strictly on the Weighted Priority.
- **Configure Priority to Egress Queues** — Maps CoS (VPT tag) or DSCP values to a queue (1-4).
  - *Configure CoS* — Maps CoS priority to a queue.
  - *Configure DSCP* — Maps DSCP priority to a queue.

2. Select a schedule type.
3. Click **Apply**. The configuration is saved and the device is updated.
4. Click **Save Config** on the menu to save the changes permanently.

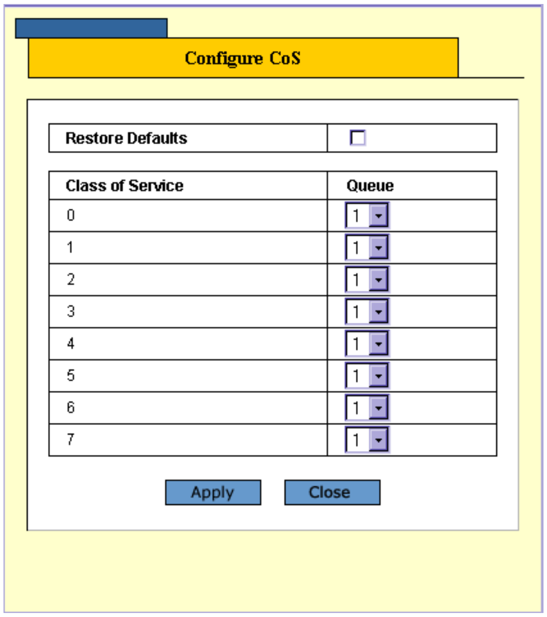
Mapping CoS Values to Queues

The *Configure CoS Page* contains fields for classifying CoS settings to traffic queues. When configuring QoS for stacking, note that stacking only uses three queues.

To set CoS to queue:

1. Click **Services > Queuing & Scheduling**. The *CoS Queuing & Scheduling Page* opens:
2. In the *Configure Priority to Egress Queues* section, select **Configure CoS**.
3. Click **Configure**. The *Configure CoS Page* opens:

Figure 141: Configure CoS Page



Configure CoS

Restore Defaults	□

Class of Service	Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1

The *Configure CoS Page* contains the following fields:

- **Restore Defaults** — Restores the device factory defaults for mapping CoS tags to a forwarding queue.
- **Class of Service** — Specifies the CoS priority tag values, where zero is the lowest and 7 is the highest.
- **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported (1-4) for a standalone unit and three (1-3) are supported for a stackable device.

4. Modify the *Queue* values or select *Restore Defaults*.
5. Click **Apply**. The *CoS to Queue* mapping settings are saved and the device is updated.
6. Click **Save Config** on the menu to save the changes permanently.

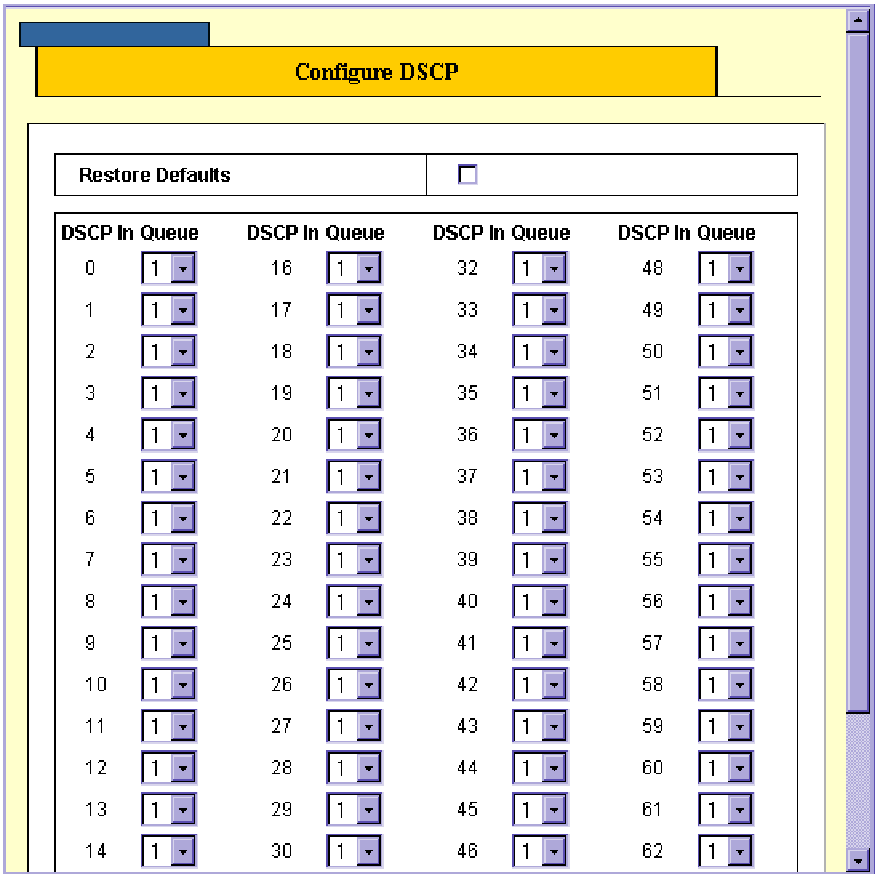
Mapping DSCP Values to Queues

The *Configure DSCP Page* contains fields for classifying DSCP settings to traffic queues. For example, a packet with a DSCP tag value of 3 can be assigned to queue 2.

To set DSCP to queues:

1. Click **Services > Queuing & Scheduling**. The *CoS Queuing & Scheduling Page* opens:
2. In the *Configure Priority to Egress Queues* section, select **Configure DSCP**.
3. Click **Configure**. The *Configure DSCP Page* opens:

Figure 142: Configure DSCP Page



Configure DSCP

Restore Defaults	□

DSCP In	Queue	DSCP In	Queue	DSCP In	Queue	DSCP In	Queue
0	1	16	1	32	1	48	1
1	1	17	1	33	1	49	1
2	1	18	1	34	1	50	1
3	1	19	1	35	1	51	1
4	1	20	1	36	1	52	1
5	1	21	1	37	1	53	1
6	1	22	1	38	1	54	1
7	1	23	1	39	1	55	1
8	1	24	1	40	1	56	1
9	1	25	1	41	1	57	1
10	1	26	1	42	1	58	1
11	1	27	1	43	1	59	1
12	1	28	1	44	1	60	1
13	1	29	1	45	1	61	1
14	1	30	1	46	1	62	1

The *Configure DSCP Page* contains the following fields:

- **Restore Defaults** — Restores the device factory defaults for mapping DSCP values to a forwarding queue.
- **DSCP In** — Displays the incoming packet’s DSCP value.
- **Queue** — Defines the traffic forwarding queue to which the DSCP priority is mapped. Four traffic priority queues are supported.

4. Modify the *Queue* values.
5. Click **Apply**. The *DSCP to Queue* mapping is updated.
6. Click **Save Config** on the menu to save the changes permanently.

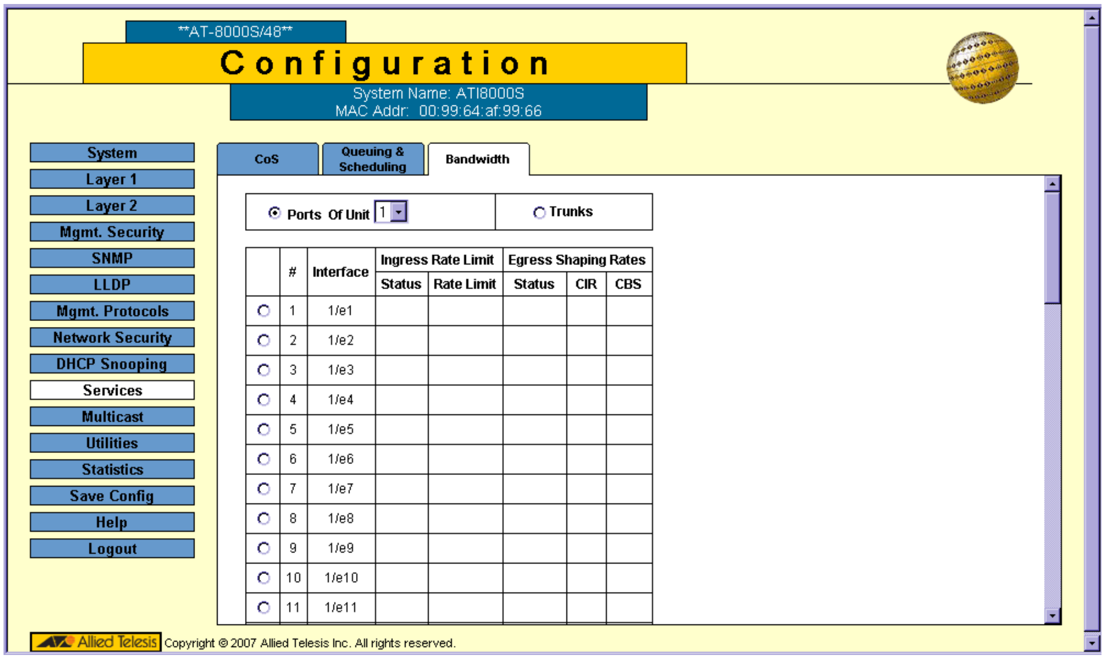
Configuring QoS Bandwidth

The *Bandwidth Page* allows network managers to define the bandwidth settings for a specified egress interface. The *Bandwidth Page* is not used with the Service mode, as bandwidth settings are based on services.

To configure bandwidth:

1. Click **Services > Bandwidth**. The *Bandwidth Page* opens:

Figure 143: Bandwidth Page



● Ports Of Unit 1 ○ Trunks

	#	Interface	Ingress Rate Limit		Egress Shaping Rates		
			Status	Rate Limit	Status	CIR	CBS
○	1	1/e1					
○	2	1/e2					
○	3	1/e3					
○	4	1/e4					
○	5	1/e5					
○	6	1/e6					
○	7	1/e7					
○	8	1/e8					
○	9	1/e9					
○	10	1/e10					
○	11	1/e11					

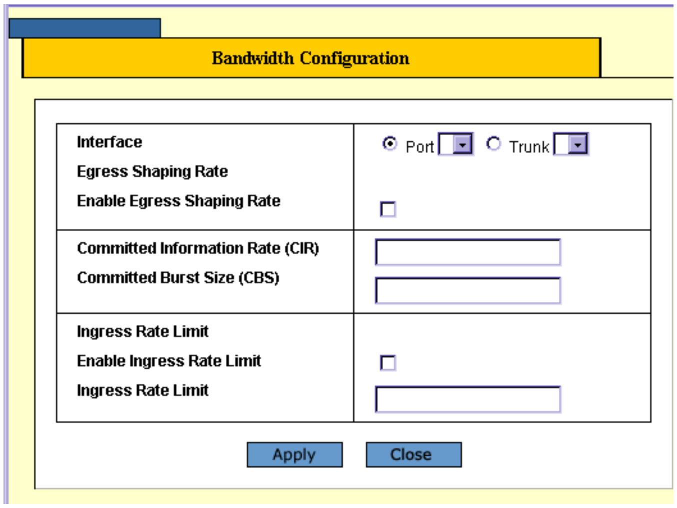
Copyright © 2007 Allied Telesis Inc. All rights reserved.

As a default the *Bandwidth Page* opens displaying the port options. The fields are identical when displaying the trunk CoS. The *Bandwidth Page* contains the following fields:

- Select the interfaces displayed in the table.
  - *Ports of Unit* — Specifies the port and stacking member for which the bandwidth settings are displayed.
  - *Trunk* — Specifies the trunk for which the bandwidth settings are displayed.
- **Interface** — Indicates the interface for which this bandwidth information is displayed.
- **Ingress Rate Limit** — Indicates the traffic limit for ingress interfaces. The possible field values are:
  - *Status* — Enables or disables rate limiting for ingress interfaces. *Disable* is the default value.
  - *Rate Limit* — Defines the rate limit for ingress ports. Defines the amount of bandwidth assigned to the interface. The available values are 62 Kbps - 1 Gbps.
- **Egress Shaping Rates** — Indicates the traffic shaping type, if enabled, for egress ports. The possible field values are:
  - *Status* — Indicates the egress shaping rate status. The default status is Disabled.
  - *CIR* — Defines Committed Information Rate *(*CIR) as the queue shaping type. The possible field values are 0-62.5 Mbps.
  - *CBS* — Defines Committed Burst Size (CbS) as the queue shaping type. CbS is supported only on GE interfaces. The possible field value is 4 KB - 16 MB.

2. Select the port/unit or trunk.
3. Select the interfaces to configure.
4. Click **Modify**. The *Bandwidth Configuration Page* opens:

Figure 144: Bandwidth Configuration Page



Bandwidth Configuration

Interface	● Port ▾ ○ Trunk ▾
Egress Shaping Rate	
Enable Egress Shaping Rate	□
Committed Information Rate (CIR)	
Committed Burst Size (CBS)	
Ingress Rate Limit	
Enable Ingress Rate Limit	□
Ingress Rate Limit	

5. Define the fields.
6. Click **Apply**. The bandwidth information is saved and the device is updated.
7. Click **Save Config** on the menu to save the changes permanently.

Chapter 16.System Utilities

The configuration file structure involves the following configuration files:

- **Startup Configuration File** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted. The Startup file is created by copying the configuration commands from the Running Configuration file or the Backup Configuration file.
- **Running Configuration File** — Contains all configuration file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost. During the startup process, all commands in the Startup file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands existing in the Running Configuration file. Commands are not overwritten. To update the Startup file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file. The next time the device is restarted, the commands are copied back into the Running Configuration file from the Startup Configuration file.
- **Backup Configuration Files** — Contains a backup copy of the device configuration. Up to five backup configuration files can be saved on the device, with user configured names. These files are generated when the user copies the Running Configuration file or the Startup Configuration file to a user-named file. The contents of the backup configuration files can be copied to either the Running Configuration or the Startup Configuration files.
- **Image Files** — Software upgrades are used when a new version file is downloaded. The file is checked for the right format, and that it is complete. After a successful download, the new version is marked, and is used after the device is reset.

There are two types of files, firmware files and configuration files. The firmware files manage the device, while the configuration files configure the device for transmissions. Configuration files can be uploaded and downloaded to the device.

System files are uploaded or downloaded using the *Trivial File Transfer Protocol* (TFTP). TFTP utilizes the *User Data Protocol* (UDP) without security features.

Note

Only one type of download or upload can be performed at any one time. During upload or download, no user configuration can be performed.

File maintenance includes configuration file management and device access, and is described in the following topics:

- Restoring the Default Configuration
- Defining TFTP File Uploads and Downloads
- Viewing Integrated Cable Tests
- Viewing Optical Transceivers
- Resetting the Device

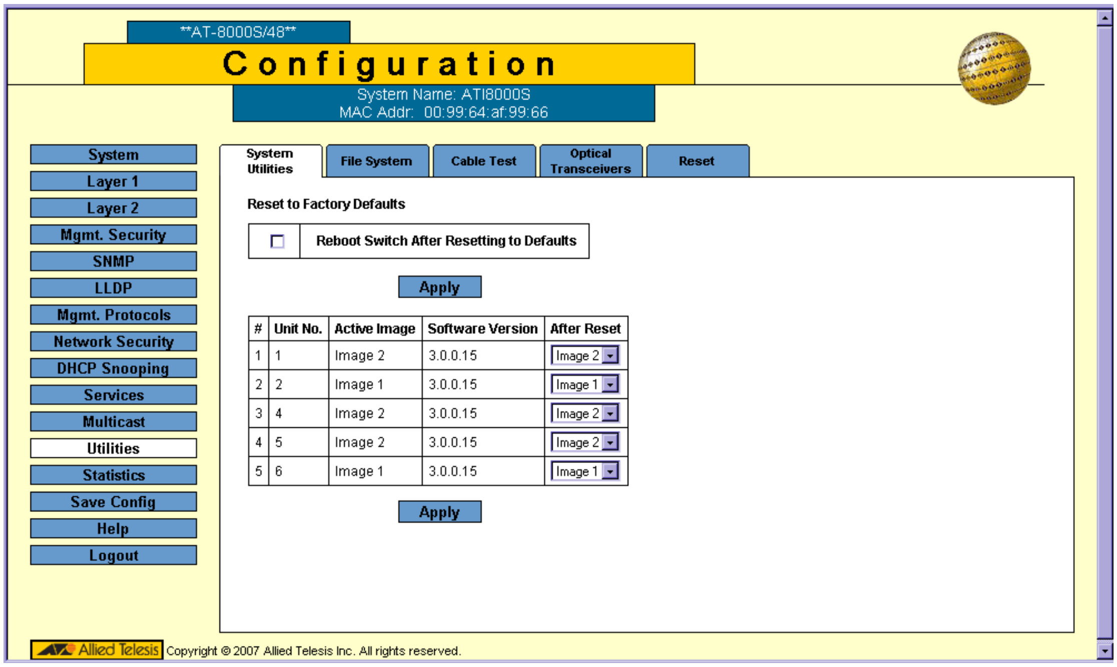
Restoring the Default Configuration

The *Reset to Factory Defaults* function restores the Configuration file to factory defaults during device reset. When this option is not selected, the device maintains the current Configuration file.

To restore the default system configuration:

1. Click **Utilities > System Utilities**. The *System Utilities Page* opens:

Figure 145: System Utilities Page



Reset to Factory Defaults

☐ Reboot Switch After Resetting to Defaults

Apply

#	Unit No.	Active Image	Software Version	After Reset
1	1	Image 2	3.0.0.15	Image 2
2	2	Image 1	3.0.0.15	Image 1
3	4	Image 2	3.0.0.15	Image 2
4	5	Image 2	3.0.0.15	Image 2
5	6	Image 1	3.0.0.15	Image 1

Apply

The *System Utilities Page* contains the following fields:

- **Reboot Switch After Resetting to Defaults** — Performs reboot after the reset. The possible field values are:
  - *Checked* — System restarts after the Configuration File is restored to the factory defaults.
  - *Unchecked* — After the Configuration File is restored to the factory defaults, the system remains in session.
- **Unit No.** — Indicates the unit number.
- **Active Image** — Indicates the current image file.
- **Software Version** — Displays the current software release.
- **After Reset** — The Image file that is active after the device is reset. The possible field values are:
  - *Image 1* — Activates Image file 1 after the device is reset.
  - *Image 2* — Activates Image file 2 after the device is reset.

To reset the configuration file to defaults without rebooting the device:

- Click **Apply** in the *Reset to Factory Defaults* section.

To reset the configuration file to defaults with reboot:

1. Check the **Reboot Switch After Resetting to Defaults** option.

2. Select the **After Reset** image file.
3. Click **Apply** (below the table). The factory defaults are restored, and the device is updated. The device reboots.

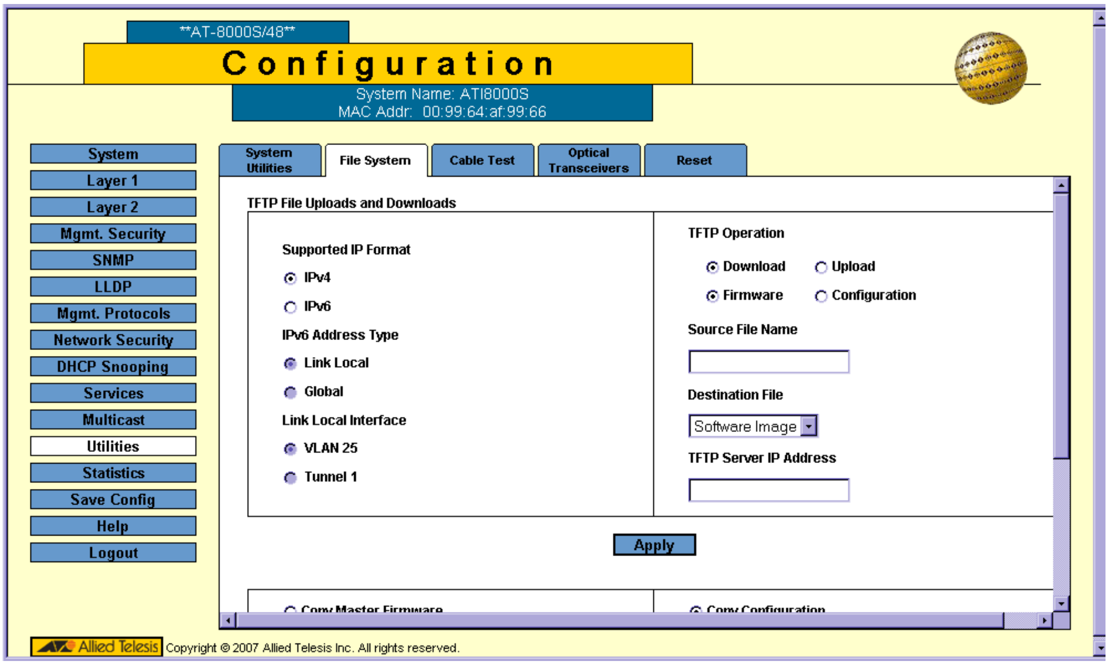
Defining TFTP File Uploads and Downloads

The *File System Page* contains parameters for system uploads and downloads and for copying firmware and configuration files.

To define file upload and download settings:

1. Click **Utilities > File System** The *File System Page* opens:

Figure 146: File System Page



TFTP File Uploads and Downloads

Supported IP Format
● IPv4
○ IPv6

IPv6 Address Type
● Link Local
○ Global

Link Local Interface
● VLAN 25
○ Tunnel 1

TFTP Operation
● Download ○ Upload
● Firmware ○ Configuration

Source File Name

Destination File
Software Image

TFTP Server IP Address

The *TFTP File Uploads and Downloads* section of the *File System Page* contains the following fields:

- **Supported IP Format** — Defines the supported Internet Protocol for TFTP operations. The possible field values are:
  - *IPv4* — Indicates that IPv4 is supported.
  - *IPv6* — Indicates that IPv6 is supported.
- **IPv6 Address Type** — If IPv6 is selected as the Supported IP Format, indicates the supported Unicast address type. The possible field values are:
  - *Link Local* — Indicates that link local addressing is supported by the interface.
  - *Global* — Indicates that global Unicast addressing is supported by the interface.

- **Link Local Interface** — If Link Local is selected as the supported IPv6 Address Type, indicates the supported interface. The possible field values are:
  - *VLAN 1* — Indicates that VLAN 1 is supported.
  - *Tunnel 1* — Indicates that ISATAP tunneling (Tunnel 1) mechanism is supported.
- **TFTP Operation** — Defines the type of TFTP operation and the type of file. The possible values are:
  - *Download* — Downloads a firmware or configuration file, depending on the selection below.
  - *Upload* — Uploads a firmware or configuration file, depending on the selection below.
  - *Firmware* — Device downloads or uploads a firmware file, depending on the selection above.
  - *Configuration* — Device downloads or uploads a configuration file, depending on the selection above.
- **Source File Name** — Specifies the file to be uploaded or downloaded.
- **Destination File** — Specifies file types, as described below.

  If the TFTP Operation is *Firmware*, the possible values are:
  - *Software Image* — Boots the Image file.
  - *Boot File* — Copies the boot file from the TFTP server to the device.

If the TFTP Operation is *Configuration*, the possible values are:

  - *Running Configuration* — Contains the configuration currently valid on the device.
  - *Starting Configuration* — Contains the configuration that is valid following system startup or reboot.

> Note
>
> The configuration file is copied only to the Master Unit, since this unit controls the entire stack. The configuration file is automatically synchronized with the configuration file on the Secondary Master Unit, so that in the event of failure of the Master Unit, the Secondary Master Unit takes over immediately with the same configuration information.

- **TFTP Server IP Address** — Specifies the TFTP Server IP Address from which files are downloaded.

To download or upload *TFTP File*s:

1. Select the *TFTP Operation* type: upload or download; firmware or configuration file.
2. Define the Source file and Destination file type.
3. Click **Apply**.

In the *Copy Files* section, network administrators can copy firmware or configuration files from one device to another.

- **Copy Master Firmware** — Copies the Firmware or the Boot file from the Stacking Master.
  - *Software Image* — Downloads the Image file.
- **Destination Unit** — Downloads firmware or the Boot file to the designated unit. The values are:
  - *All* — Copies the Firmware or the Boot file to all stacking members.

To copy firmware:

1. Click **Copy Master Firmware**. The copy firmware parameters are activated.
2. Select the *Source* and the *Destination Unit*.
3. Click **Apply**.

The *Configuration Copy* section of the *File System Page* contains the following fields:

- **Copy Configuration**— Allows the copy configuration operation.
- **Source File Name** — Specifies the configuration file type to be copied.
  - *Startup Configuration* — Copies the Startup Configuration file, and overwrites the old Startup Configuration file.
  - *Running Configuration* — Copies the Running Configuration file.
- **Destination File Name** — Specifies the destination file type to create. The possible field values are:
  - *Startup Configuration* — Downloads the Startup Configuration file, and overwrites it.
  - *Running Configuration* — Downloads commands into the Running Configuration file.

To copy configuration:

1. Click **Copy Configuration**. The copy configuration parameters are activated.
2. Select the *Source* file name and the *Destination* file name.
3. Click **Apply**.

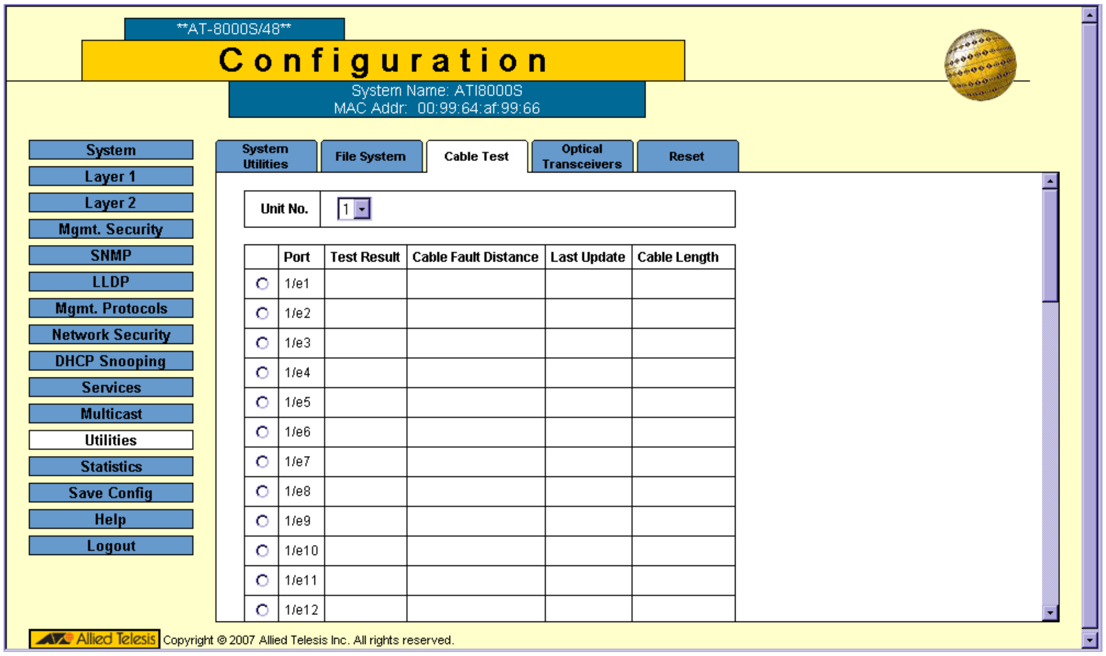
Viewing Integrated Cable Tests

The *Cable Test Page* contains fields for performing tests on copper cables. Cable testing provides diagnostic information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error that occurred. The tests use *Time Domain Reflectometry* (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the Approximated Cable Length test.

To perform a copper cable test:

1. Click **Utilities > Cable Test**. The *Cable Test Page* opens:

Figure 147: Cable Test Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Unit No. 1

	Port	Test Result	Cable Fault Distance	Last Update	Cable Length
○	1/e1				
○	1/e2				
○	1/e3				
○	1/e4				
○	1/e5				
○	1/e6				
○	1/e7				
○	1/e8				
○	1/e9				
○	1/e10				
○	1/e11				
○	1/e12				

Copyright © 2007 Allied Telesis Inc. All rights reserved.

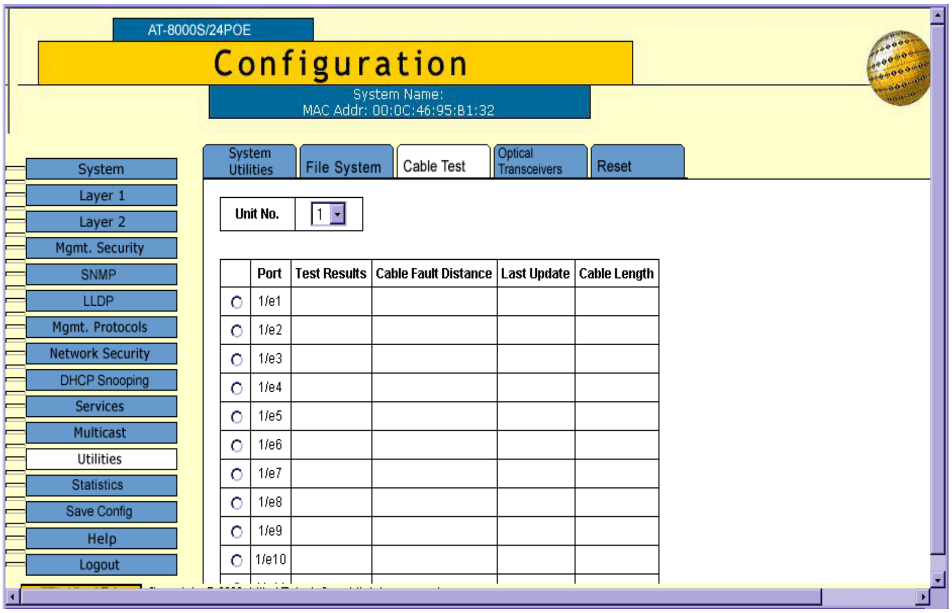
The *Cable Test Page* displays the following information:

- **Unit Number** — Indicates the stacking member for which the Ethernet ports information is displayed.
- **Port** — Specifies the port to which the cable is connected.
- **Test Result** — Displays the cable test results. Possible values are:
  - *No Cable* — Indicates that a cable is not connected to the port.
  - *Open Cable* — Indicates that a cable is connected on only one side.
  - *Short Cable* — Indicates that a short has occurred in the cable.
  - *OK* — Indicates that the cable passed the test.
- **Cable Fault Distance** — Indicates the distance from the port where the cable error occurred.
- **Last Update** — Indicates the last time the port was tested.
- **Cable Length** — Indicates the approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.

2. Select the *Unit Number*, and the *Port.*

3. Click **Test**. The cable test is performed.
4. Click **Advanced**. The *Cable Test Configuration Page* opens, and the copper cable test results are displayed.

Figure 148: Cable Test Configuration Page



Unit No. 1

	Port	Test Results	Cable Fault Distance	Last Update	Cable Length
○	1/e1				
○	1/e2				
○	1/e3				
○	1/e4				
○	1/e5				
○	1/e6				
○	1/e7				
○	1/e8				
○	1/e9				
○	1/e10				

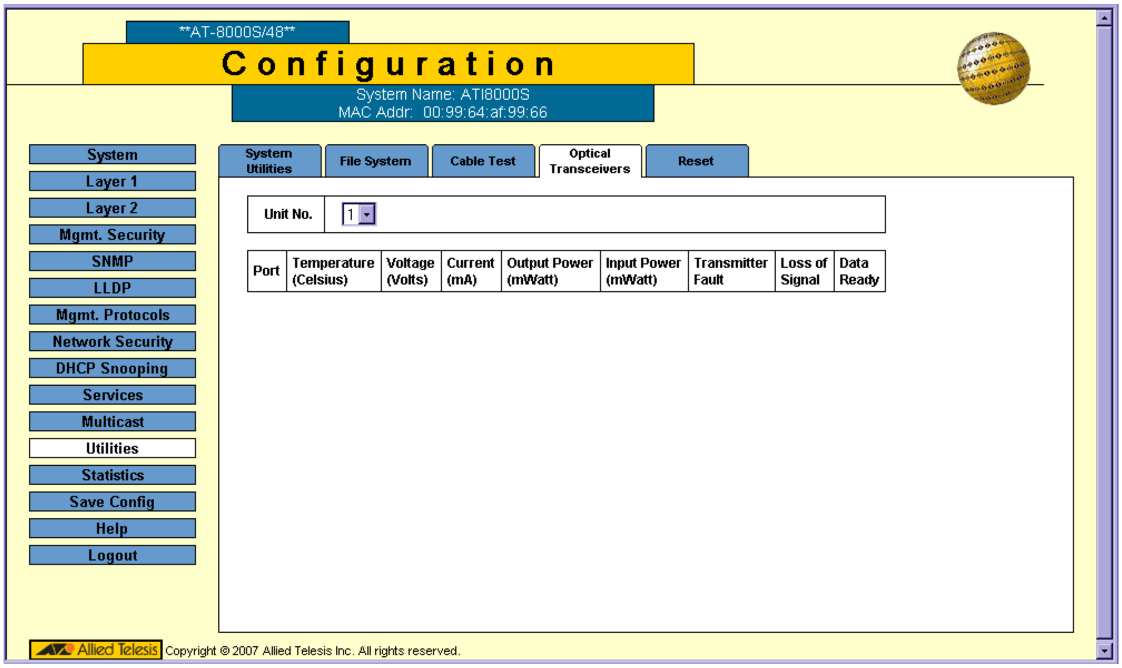
Viewing Optical Transceivers

The *Optical Transceivers Page* allows network managers to perform tests on Fiber Optic cables. Optical transceiver diagnostics can be performed only when the link is present.

To view transceiver diagnostics:

1. Click **Utilities > Optical Transceivers**. The *Optical Transceivers Page* opens:

Figure 149: Optical Transceivers Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Unit No. 1

Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Output Power (mWatt)	Input Power (mWatt)	Transmitter Fault	Loss of Signal	Data Ready

The *Optical Transceivers Page* contains the following fields:

- **Unit No.** — Indicates the stacking member for which the interface configuration information is displayed.
- **Port** — Displays the IP address of the port on which the cable is tested.
- **Temperature (Celsius)** — Displays the temperature (^{o}C) at which the cable is operating.
- **Voltage (Volts)** — Displays the voltage at which the cable is operating.
- **Current (mA)** — Displays the current at which the cable is operating.
- **Output Power (Watts)** — Indicates the rate at which the output power is transmitted.
- **Input Power (Watts)** — Indicates the rate at which the input power is transmitted.
- **Transmitter Fault** — Indicates if a fault occurred during transmission.
- **Loss of Signal** — Indicates if a signal loss occurred in the cable.
- **Data Ready** — Indicates the transceiver has achieved power up and data is ready.

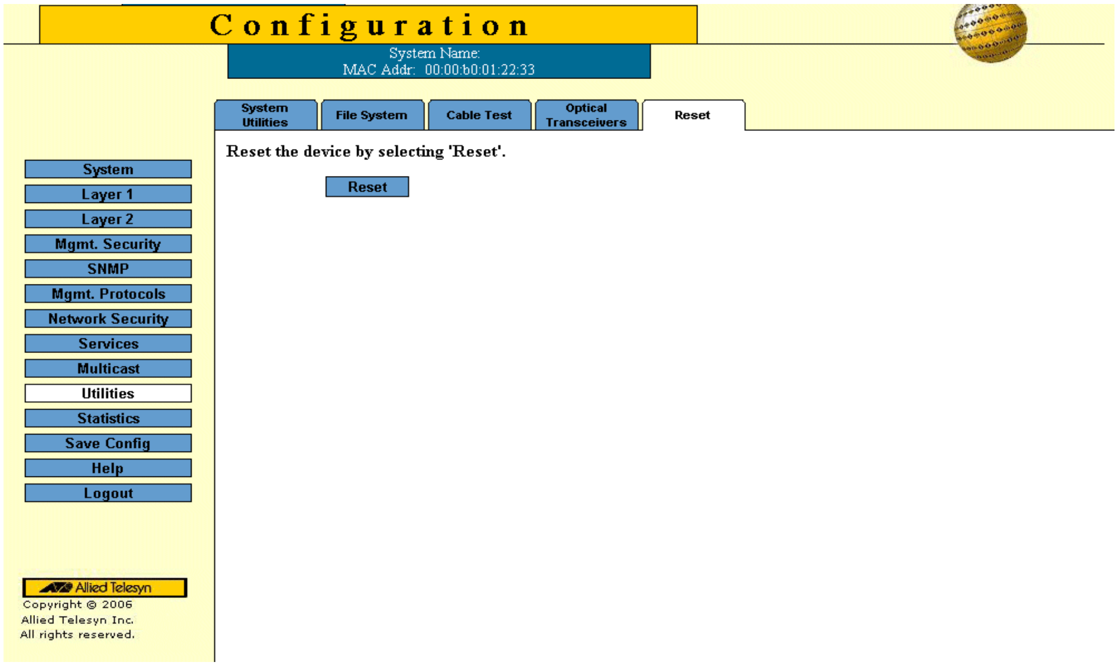
Resetting the Device

The *Reset Page* enables the user to reset the system. Save all changes to the Startup Configuration file before resetting the device. This prevents the current (Running) device configuration from being lost.

To reset the device:

1. Click **Utilities > Reset**. The *Reset Page* opens.

Figure 150: Reset Page



Reset the device by selecting 'Reset'.

Reset

2. Select the **Reset Unit No.** Select a specific unit number in the dropdown list or select *Stack* to reset all stack members simultaneously.
3. Click **Reset**. The confirmation message appears informing that reset ends the management session.
4. Click **OK**. The device is reset.

Chapter 17.Viewing Statistics

This section provides device statistics for RMON, interfaces, and Etherlike. This section contains the following topics:

- Viewing Device Statistics
- Managing RMON Statistics

Viewing Device Statistics

This section contains the following topics:

- Viewing Interface Statistics
- Viewing Etherlike Statistics

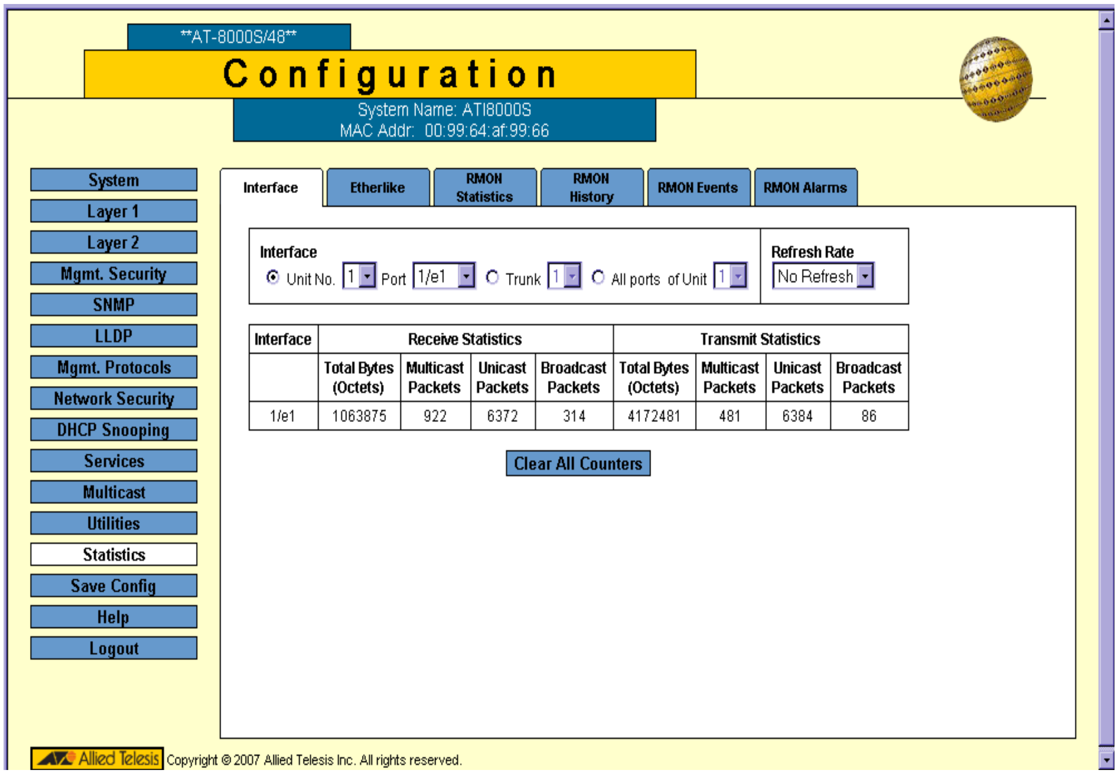
Viewing Interface Statistics

The interface page contains statistics for both received and transmitted packets.

To view interface statistics:

1. Click **Statistics > Interface**. The *Interface Statistics Page* opens:

Figure 151:Interface Statistics Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Interface
● Unit No. 1 Port 1/e1 ○ Trunk 1 ○ All ports of Unit 1

Refresh Rate
No Refresh

Interface	Receive Statistics				Transmit Statistics			
	Total Bytes (Octets)	Multicast Packets	Unicast Packets	Broadcast Packets	Total Bytes (Octets)	Multicast Packets	Unicast Packets	Broadcast Packets
1/e1	1063875	922	6372	314	4172481	481	6384	86

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Interface Statistics Page* contains the following fields:

- Select the interfaces displayed in the table.
  - *Unit No.* — Specifies the unit for which the Etherlike statistics are displayed.
  - *Port* — Specifies the port for which the interface statistics are displayed.
  - *Trunk* — Specifies the trunk for which the interface statistics are displayed.
  - *All Ports of Unit* — Specifies all ports on the selected unit for which the interface statistics are displayed.
- **Refresh Rate** — Defines the frequency of the interface statistics updates. The possible field values are:
  - *15 Sec* — Indicates that the Interface statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the Interface statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the Interface statistics are refreshed every 60 seconds.
  - *No Refresh* — Indicates that the Interface statistics are not refreshed.

Receive Statistics

- **Total Bytes (Octets)** — Displays the number of octets received on the selected interface.
- **Multicast Packets** — Displays the number of Multicast packets received on the selected interface.
- **Unicast Packets** — Displays the number of Unicast packets received on the selected interface.
- **Broadcast Packets** — Displays the number of Broadcast packets received on the selected interface.

Transmit Statistics

- **Total Bytes (Octets)** — Displays the number of octets transmitted from the selected interface.
- **Multicast Packets** — Displays the number of Multicast packets transmitted from the selected interface.
- **Unicast Packets** — Displays the number of Unicast packets transmitted from the selected interface.
- **Broadcast Packets** — Displays the number of Broadcast packets transmitted from the selected interface.

2. Select the *Interface* and the *Refresh Rate*. The selected interface’s Interface statistics are displayed.

To reset interface statistics counters:

1. Open the *Interface Statistics Page*.
2. Click **Clear All Counters**. The interface statistics counters are cleared.

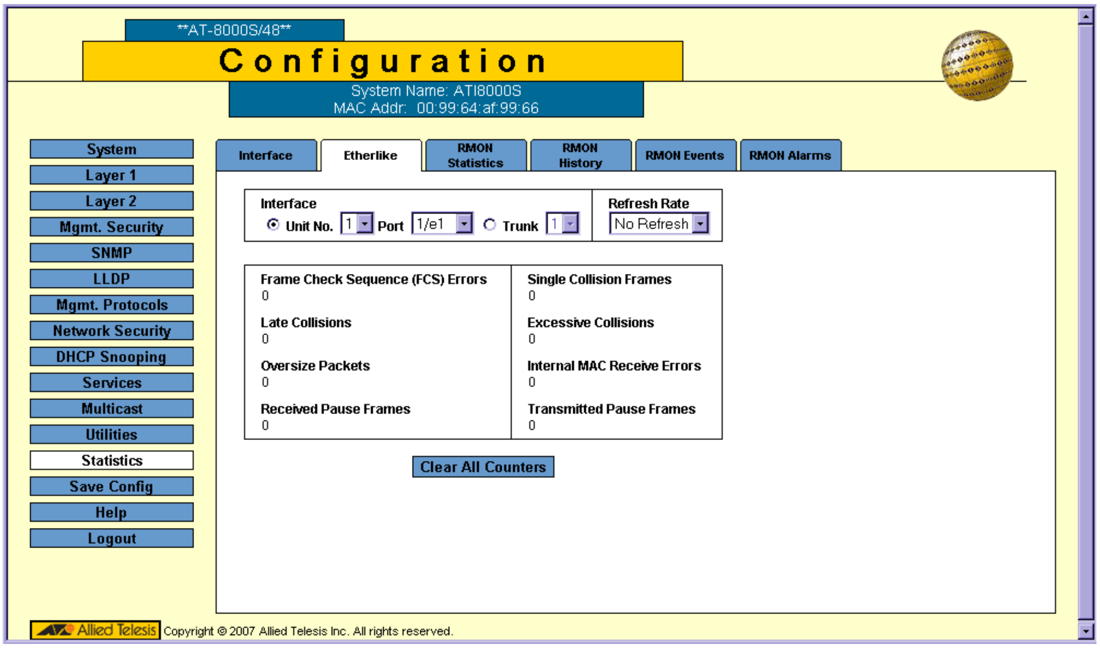
Viewing Etherlike Statistics

The *Etherlike Statistics Page* displays interface statistics.

To view Etherlike statistics:

1. Click **Statistics > Etherlike.** The *Etherlike Statistics Page* opens:

Figure 152: Etherlike Statistics Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Interface
● Unit No. 1 Port 1/e1 ○ Trunk 1

Refresh Rate
No Refresh

Frame Check Sequence (FCS) Errors 0	Single Collision Frames 0
Late Collisions 0	Excessive Collisions 0
Oversize Packets 0	Internal MAC Receive Errors 0
Received Pause Frames 0	Transmitted Pause Frames 0

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Etherlike Statistics Page* contains the following fields:

- Select the interfaces displayed in the table.
  - *Unit No.* — Specifies the unit for which the Etherlike statistics are displayed.
  - *Port* — Specifies the port within the unit for which the Etherlike statistics are displayed.
  - *Trunk* — Defines the specific trunk for which the Etherlike statistics are displayed.
- **Refresh Rate** — Defines the frequency of the interface statistics updates. The possible field values are:
  - *15 Sec* — Indicates that the Etherlike statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the Etherlike statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the Etherlike statistics are refreshed every 60 seconds.

  - *No Refresh* — Indicates that the Etherlike statistics are not refreshed.
- **Frame Check Sequence (FCS) Errors** — Displays the number of FCS errors received on the selected interface.
- **Single Collision Frames** — Displays the number of single collision frames received on the selected interface.
- **Late Collisions** — Displays the number of late collision frames received on the selected interface.
- **Excessive Collisions** — Displays the number of excessive collisions received on the selected interface.
- **Oversize Packets** — Displays the number of oversized packet errors on the selected interface.
- **Internal MAC Receive Errors** — Displays the number of internal MAC received errors on the selected interface.
- **Received Pause Frames** — Displays the number of received paused frames on the selected interface.
- **Transmitted Paused Frames** — Displays the number of paused frames transmitted from the selected interface.

2. Select the *Interface* and the *Refresh Rate*. The selected interface’s Etherlike statistics are displayed.

To update the refresh time:

- To change the refresh rate for statistics, select another rate from the *Refresh Rate* drop-down list.

To reset Etherlike interface statistics counters:

1. Open the *Etherlike Statistics Page*.
2. Click **Clear All Counters**. The Etherlike interface statistics counters are cleared.

Managing RMON Statistics

This section contains the following topics:

- Viewing RMON Statistics
- Configuring RMON History
- Configuring RMON Events
- Defining RMON Alarms

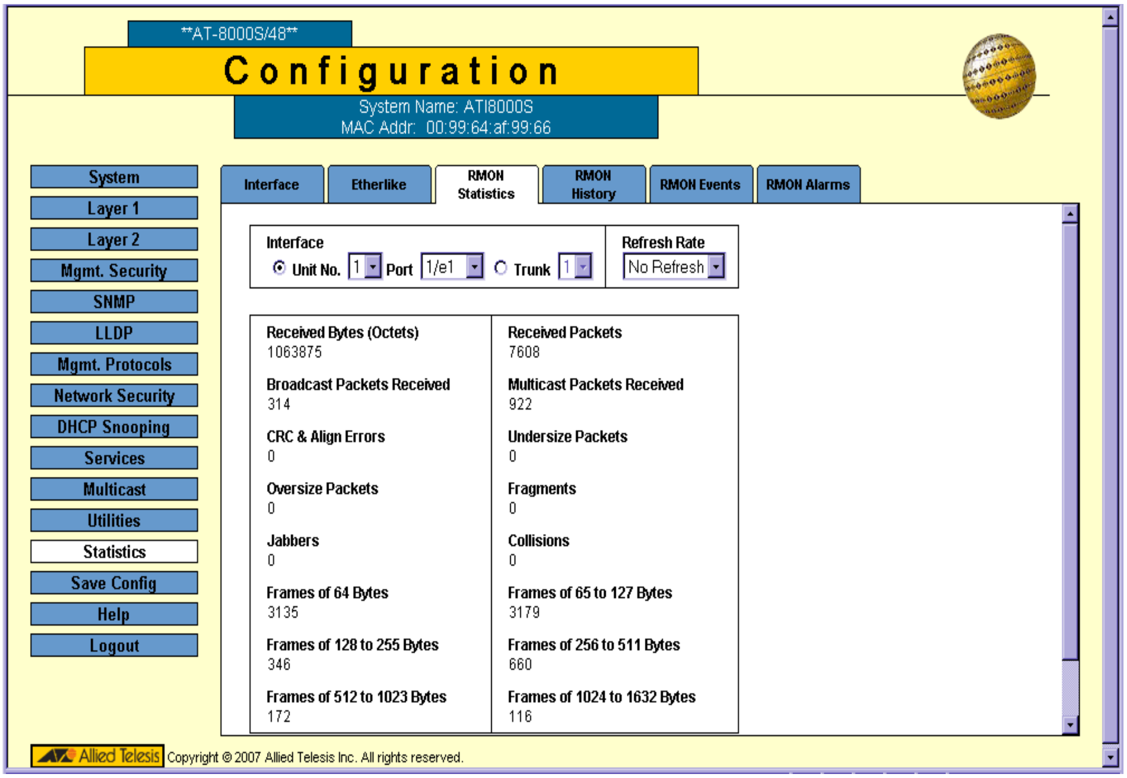
Viewing RMON Statistics

The *RMON Statistics Page* contains fields for viewing information about device utilization and errors that occurred on the device. The *RMON Statistics Page* contains statistics for both received and transmitted packets.

To view RMON statistics:

1. Click **Statistics > RMON Statistics**. The *RMON Statistics Page* opens:

Figure 153: RMON Statistics Page



AT-8000S/48

Configuration

System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Interface
● Unit No. 1 Port 1/e1 ○ Trunk 1

Refresh Rate
No Refresh

Received Bytes (Octets) 1063875	Received Packets 7608
Broadcast Packets Received 314	Multicast Packets Received 922
CRC & Align Errors 0	Undersize Packets 0
Oversize Packets 0	Fragments 0
Jabbers 0	Collisions 0
Frames of 64 Bytes 3135	Frames of 65 to 127 Bytes 3179
Frames of 128 to 255 Bytes 346	Frames of 256 to 511 Bytes 660
Frames of 512 to 1023 Bytes 172	Frames of 1024 to 1632 Bytes 116

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *RMON Statistics Page* contains the following fields:

- Select the interfaces displayed in the table.
  - *Unit No.* — Specifies the unit for which the RMON statistics are displayed.
  - *Port* — Specifies the port for which the RMON statistics are displayed.
  - *Trunk* — Defines the specific trunk for which the RMON statistics are displayed.
- **Refresh Rate** — Defines the frequency of the RMON statistics updates. The possible field values are:
  - *15 Sec* — Indicates that the RMON statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the RMON statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the RMON statistics are refreshed every 60 seconds.

   – *No Refresh*—Indicates that the RMON statistics are not refreshed.

- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Displays the number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
- **Broadcast Packets Received** — Displays the number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets Received** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC & Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
- **Frames of *xx* Bytes** — Displays the number of *xx*-byte frames received on the interface since the device was last refreshed.

2. Select the *Interface* and the *Refresh Rate*. The selected interface's RMON statistics are displayed.

To reset Etherlike interface statistics counters:

1. Open the *RMON Statistics Page*.
2. Click **Clear All Counters**. The RMON interface statistics counters are cleared.

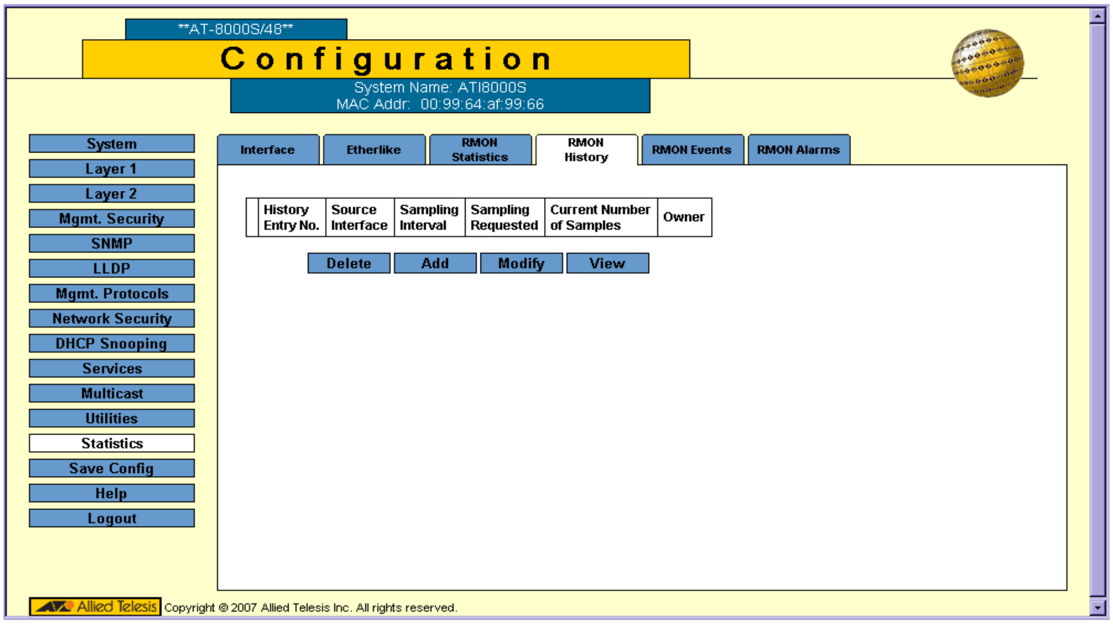
Configuring RMON History

The *RMON History Page* contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods.

To view RMON history information:

1. Click **Statistics > RMON History**. The *RMON History Page* opens:

Figure 154: RMON History Page



System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

	History Entry No.	Source Interface	Sampling Interval	Sampling Requested	Current Number of Samples	Owner

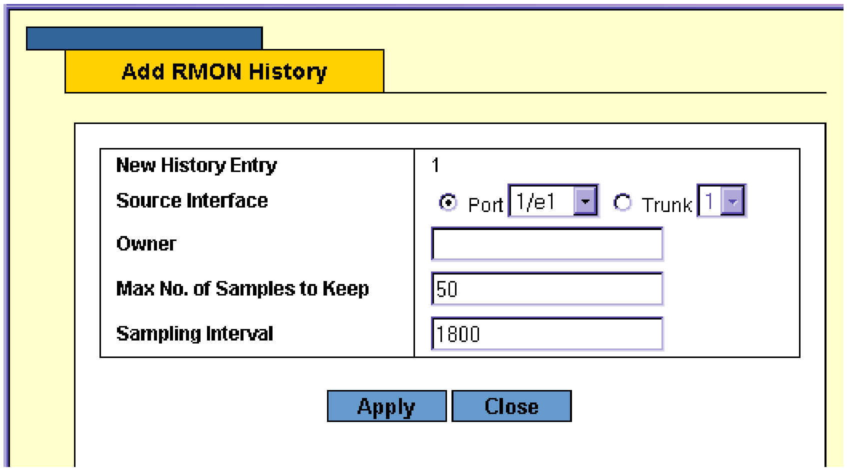
Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *RMON History Page* contains the following fields:

- **History Entry No.** — Displays the history control entry number.
- **Source Interface** — Displays the interface from which the history samples were taken. The possible field values are:
  - *Port* — Specifies the port from which the RMON information was taken.
  - *Trunk* — Specifies the trunk from which the RMON information was taken.
- **Sampling Interval** — Indicates in seconds the time period that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).
- **Sampling Requested**— Displays the number of samples to be saved (see **Max. No. of Samples to Keep** in the *Add RMON History Page*). The field range is 1-65535. The default value is 50.
- **Current Number of Samples** — Displays the current number of samples taken. This number should be equal to or close to the number of samples requested. If the number of samples exceeds the requested number, the device discards the older samples until the current number equals the requested amount.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.

2. Click **Add**. The *Add RMON History Page* opens:

Figure 155: Add RMON History Page



Add RMON History

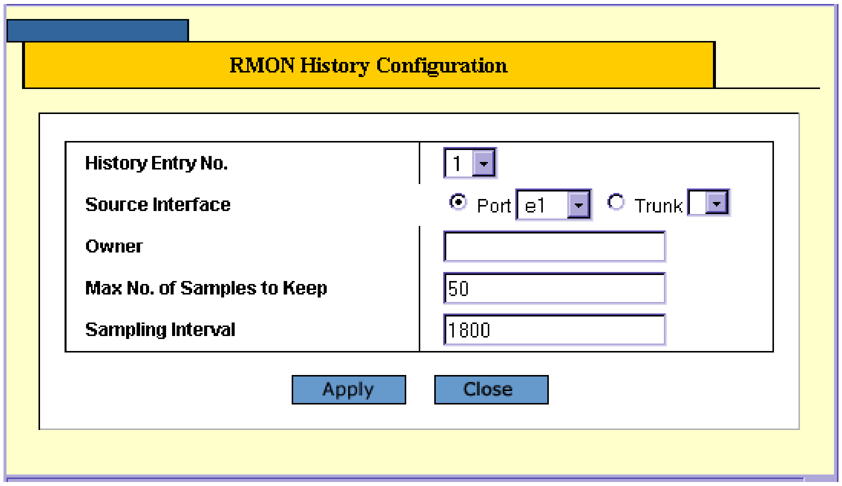
New History Entry	1
Source Interface	● Port 1/e1 ○ Trunk 1
Owner	
Max No. of Samples to Keep	50
Sampling Interval	1800

3. Define the *Source Interface*, *Owner*, *Max. No. of Samples to Keep*, *and Sampling Interval* fields.
4. Click **Apply**. The new entry is added to the history table, and the device is updated.

To edit an RMON history entry:

1. Click **Statistics > RMON History**. The *RMON History Page* opens.
2. Click **Modify**. The *RMON History Configuration Page* opens:

Figure 156: RMON History Configuration Page



RMON History Configuration

History Entry No.	1
Source Interface	● Port e1 ○ Trunk
Owner	
Max No. of Samples to Keep	50
Sampling Interval	1800

3. Define the fields.
4. Click **Apply.** The new entry is added to the history table, and the device is updated.

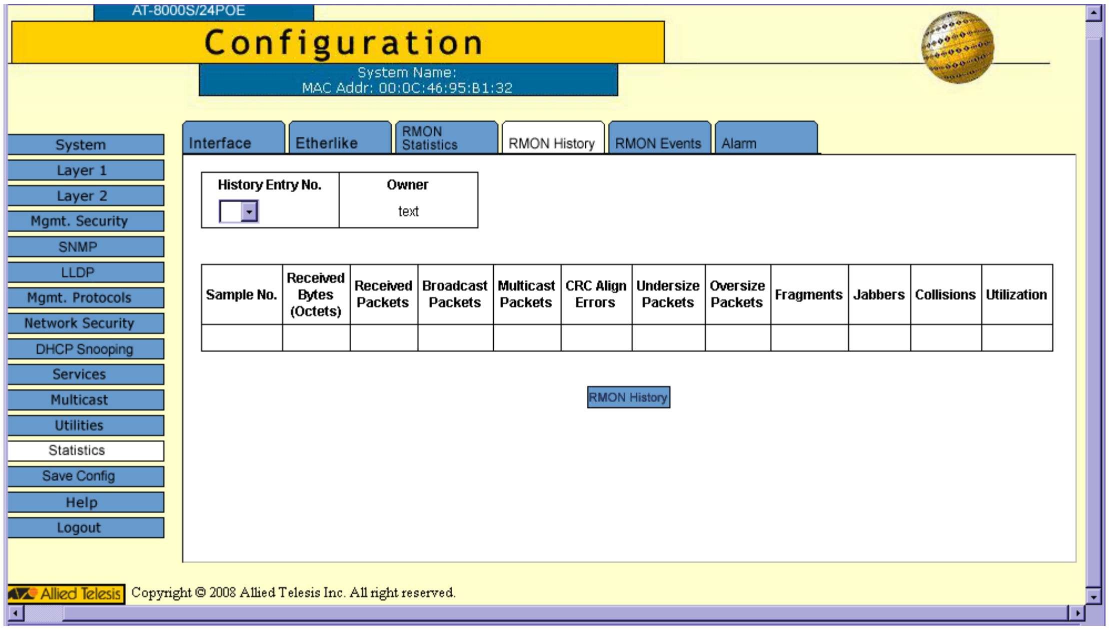
Viewing the RMON History Table

The *RMON History Table Page* contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

To view the RMON History Table:

1. Click **Statistics > RMON History**. The *RMON History Page* opens.
2. Click **View**. The *RMON History Table Page* opens:

Figure 157: RMON History Table Page



History Entry No.	Owner
	text

Sample No.	Received Bytes (Octets)	Received Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization

Copyright © 2008 Allied Telesis Inc. All right reserved.

The *RMON History Table Page* contains the following fields:

- **History Entry No.** — Select the history table entry number.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.

Each table entry represents all counter values compiled during a single sample.

- **Sample No.** — Displays the entry number for the History Control Table page.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets** — Displays the number of packets received on the interface since the device was last refreshed, including bad packets, Multicast and Broadcast packets.
- **Broadcast Packets** — Displays the number of good Broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
- **Utilization** — Displays the percentage of the interface utilized.

3. Select an entry in the *History Entry No.* field.
4. Select the sample number. The statistics are displayed.
5. Click **RMON History** to return to the *RMON History Page*.

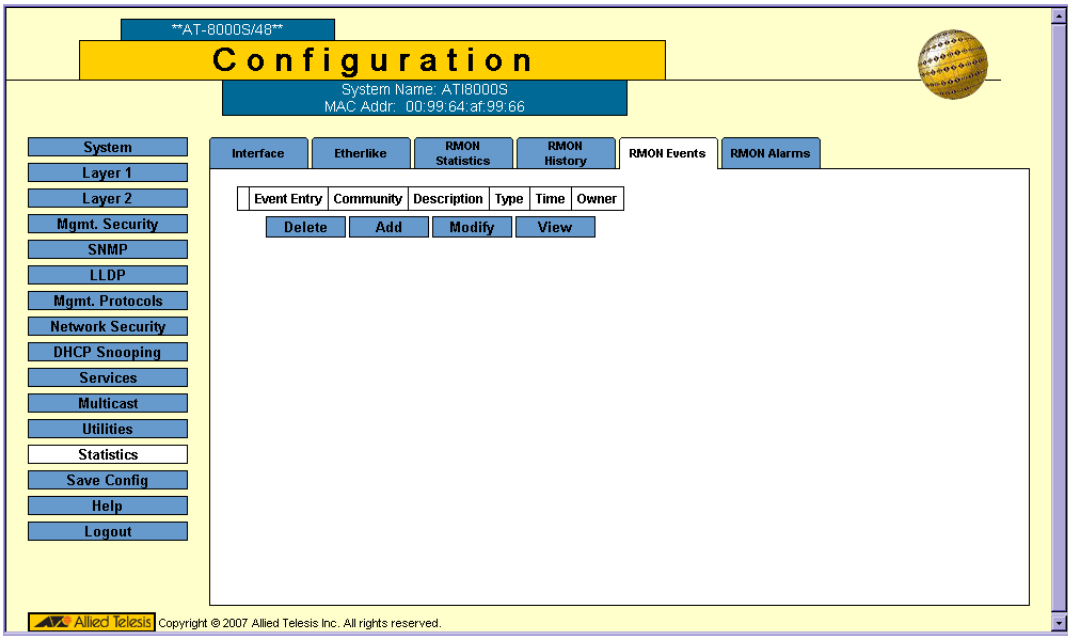
Configuring RMON Events

The *RMON Events Page* contains fields for defining, modifying and viewing RMON events statistics.

To add an RMON event:

1. Click **Statistics > RMON Events**. The *RMON Events Page* opens:

Figure 158: RMON Events Page



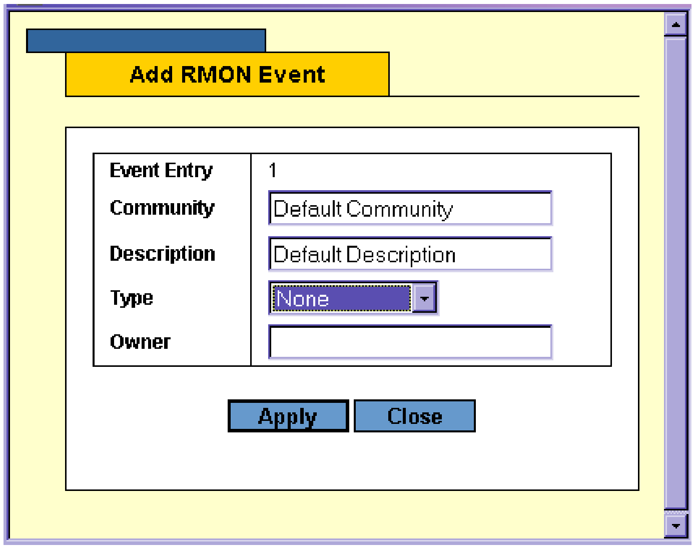
	Event Entry	Community	Description	Type	Time	Owner

The *RMON Events Page* contains the following fields:

- **Event Entry** — Displays the event.
- **Community** — Displays the community to which the event belongs.
- **Description** — Displays the user-defined event description.
- **Type** — Describes the event type. Possible values are:
  - *Log* — Indicates that the event is a log entry.
  - *Trap* — Indicates that the event is a trap.
  - *Log and Trap* — Indicates that the event is both a log entry and a trap.
  - *None* — Indicates that no event occurred.
- **Time** — Displays the time that the event occurred.
- **Owner** — Displays the device or user that defined the event.

2. Click **Add**. The *Add RMON Events Page* opens:

Figure 159: Add RMON Events Page



Add RMON Event

Event Entry	1
Community	Default Community
Description	Default Description
Type	None
Owner	

3. Define the *Community*, *Description*, *Type* and *Owner* fields.
4. Click **Apply**. The event entry is added and the device is updated.

To modify the RMON Event entry settings:

1. Click **Statistics > RMON Events**. The *RMON Events Page* opens.
2. Click **Modify**. The *RMON Events Configuration Page* opens
3. Select an event entry and define the fields for the entry.
4. Click **Apply**. The event control settings are saved and the device is updated.

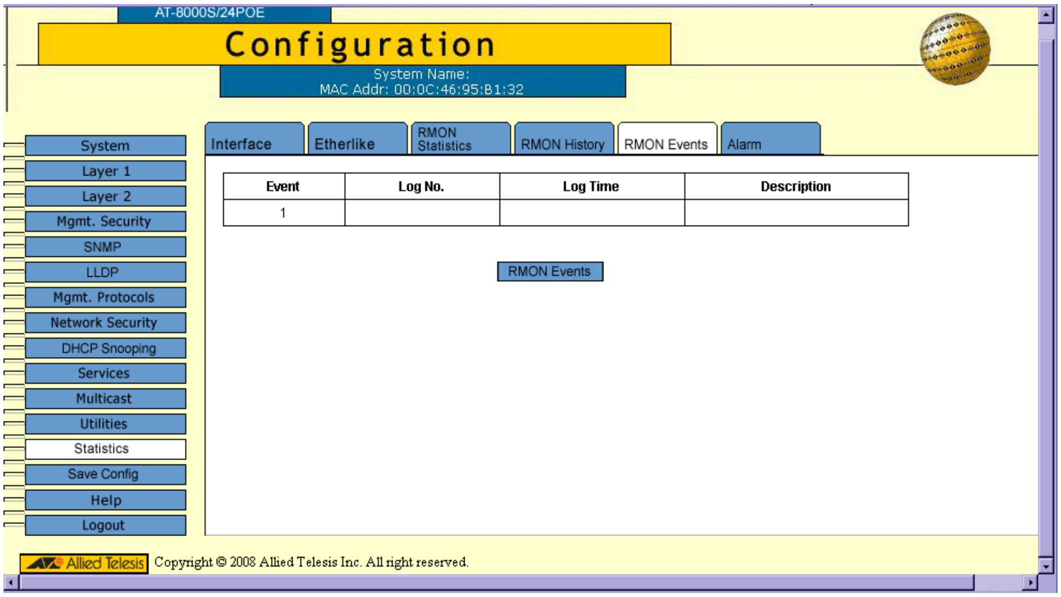
Viewing the RMON Events Logs

The *RMON Events Logs Page* contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

To view the RMON Events Table:

1. Click **Statistics > RMON Events**. The *RMON Events Page* opens.
2. Click **View**. The *RMON Events Logs Page* opens:

Figure 160: RMON Events Logs Page



System Name:
MAC Addr: 00:0C:46:95:B1:32

Event	Log No.	Log Time	Description
1			

Copyright © 2008 Allied Telesis Inc. All right reserved.

The *RMON Events Logs Page* contains the following event log information:

- **Event** — Displays the RMON Events Log entry number.
- **Log No.** — Displays the log number.
- **Log Time** — Displays the time when the log entry was entered.
- **Description** — Displays the log entry description.

3. Click **RMON Event** to return to the *RMON Events Page*.

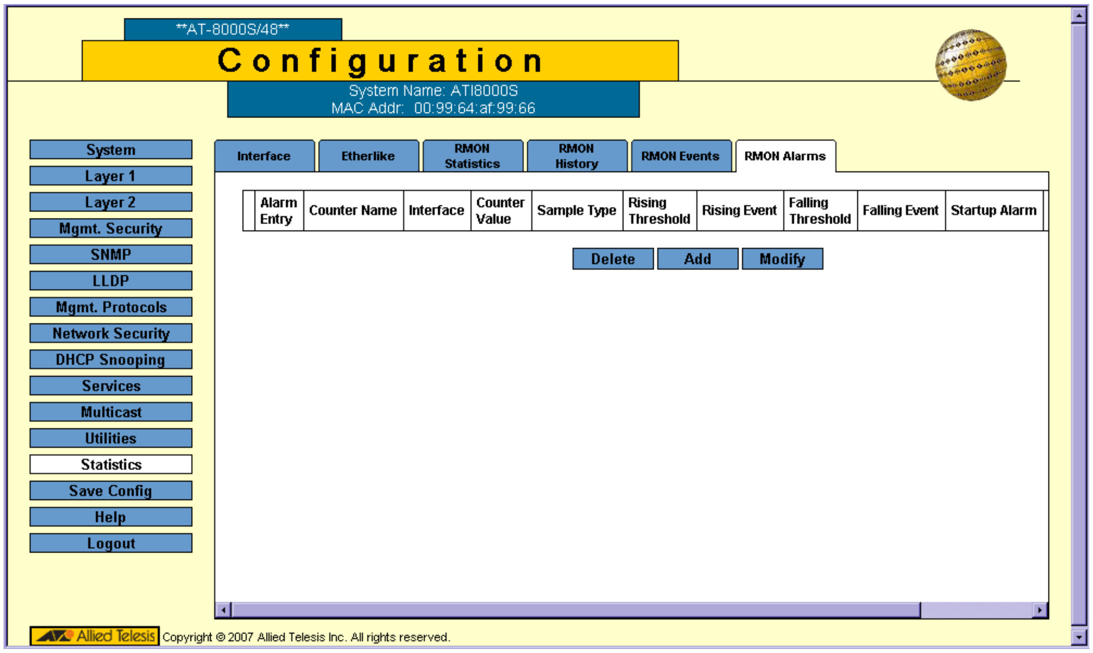
Defining RMON Alarms

The *RMON Alarm Page* contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events.

To set RMON alarms:

1. Click **Statistics > RMON Alarm**. The *RMON Alarm Page* opens:

Figure 161: RMON Alarm Page



	Alarm Entry	Counter Name	Interface	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Startup Alarm

The *RMON Alarm Page* contains the following fields:

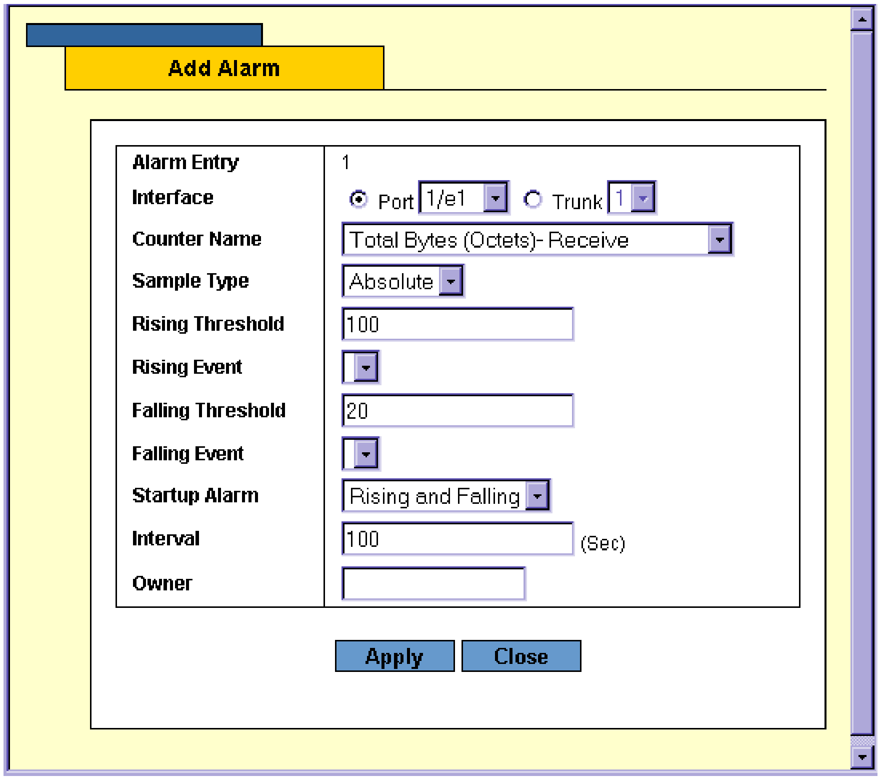
- **Alarm Entry** — Indicates a specific alarm.
- **Counter Name** — Displays the selected MIB variable.
- **Interface** — Displays interface for which RMON statistics are displayed. The possible field values are:
  - *Port* — Displays the RMON statistics for the selected port.
  - *Trunk* — Displays the RMON statistics for the selected trunk.
- **Counter Value** — Displays the selected MIB variable value.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
  - *Delta* — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

- *Absolute* — Compares the values directly with the thresholds at the end of the sampling interval.

- **Rising Threshold** — Displays the rising counter value that triggers the rising threshold alarm.
- **Rising Event** — Displays the event that triggers the specific alarm. The possible field values are user-defined RMON events.
- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm.
- **Falling Event** — Displays the event that triggers the specific alarm. The possible field values are user-defined RMON events.
- **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
- **Interval (sec)** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.

2. Click **Add**. The *Add Alarm Page* opens:

Figure 162: Add Alarm Page



Add Alarm

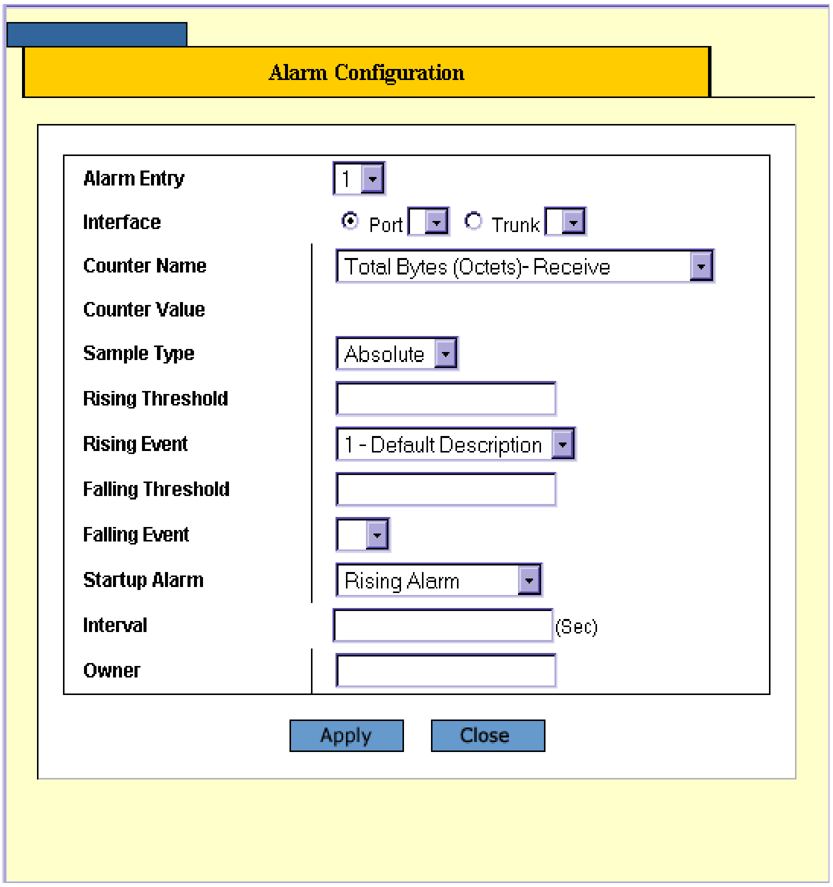
Alarm Entry	1
Interface	● Port 1/e1 ○ Trunk 1
Counter Name	Total Bytes (Octets)- Receive
Sample Type	Absolute
Rising Threshold	100
Rising Event	
Falling Threshold	20
Falling Event	
Startup Alarm	Rising and Falling
Interval	100 (Sec)
Owner	

3. Define the *Interface*, *Counter Name, Sample Type*, *Rising Threshold*, *Rising Event*, *Falling Threshold*, *Falling Event*, *Startup Alarm*, *Interval*, and *Owner* fields.
4. Click **Apply**. The RMON alarm is added, and the device is updated.

To modify RMON alarms:

1. Click **Statistics > RMON Alarm**. The *RMON Alarm Page* opens.
2. Click **Modify**. The *Alarm Configuration Page* opens:

Figure 163: Alarm Configuration Page



Alarm Configuration

Alarm Entry	1
Interface	● Port ○ Trunk
Counter Name	Total Bytes (Octets)- Receive
Counter Value	
Sample Type	Absolute
Rising Threshold	
Rising Event	1 - Default Description
Falling Threshold	
Falling Event	
Startup Alarm	Rising Alarm
Interval	(Sec)
Owner	

3. Define the fields.
4. Click **Apply**. The RMON alarm is saved, and the device is updated.

Chapter 18.Managing Stacking

This section describes the stacking control management and includes the following topics:

- Stacking Overview
- Configuring Stacking Management

Stacking Overview

Stacking provides multiple switch management through a single point as if all stack members are a single unit. All stack members are accessed through a single IP address through which the stack is managed. The stack can be managed using the following interfaces:

- Web-based Interface
- SNMP Management Station
- Command Line Interface (CLI)

Devices support stacking up to six units per stack, or can operate as stand-alone units. During the Stacking setup, one switch is selected as the Stacking Master and another stacking member can be selected as the Secondary Master. All other devices are selected as stack members, and assigned a unique Unit ID.

Switch software is downloaded for each stack member. During a software download, the software version is downloaded to the master unit and can then be copied to all units at once. All units in the stack must be running the same software version.

Switch stacking and configuration is maintained by the Stacking Master. The Stacking Master detects and reconfigures the ports with minimal operational impact in the event of:

- Unit Failure
- Inter-unit Stacking Link Failure
- Unit Insertion
- Removing a Stacking Unit

This section includes the following topics:

- Stacking Ring Topology
- Stacking Chain Topology
- Stacking Members and Unit ID
- Removing and Replacing Stacking Members
- Exchanging Stacking Members

Stacking Ring Topology

Stacked devices operate in a Ring topology. A Ring topology is where all devices in the stack are connected to each other forming a circle. Each stacked device accepts data and sends it to the device to which it is physically connected. The packet continues through the stack until it reaches the destination port. The system automatically discovers the optimal path on which to send traffic.

Most difficulties in Ring topologies occur when a device in the ring becomes non-functional, or a link is severed. In a stack, the system automatically switches to a Stacking Failover topology without any system downtime. An SNMP message is automatically generated, but no stack management action is required. However, the stacking link or stacking member must be repaired to ensure the stacking integrity.

After the stacking issues are resolved, the device can be reconnected to the stack without interruption, and the Ring topology is restored.

Stacking Chain Topology

In a chain topology, there are two units that have only one neighbor. Every unit has an uplink neighbor and a downlink neighbor. The chain topology is less robust than the ring topology. A failure in the chain results in a topology change to the stack. The location of the failure determines the severity of this topology change. The chain topology also acts as a fail-safe for the ring topology. When the ring topology fails, the stack automatically reverts to the chain topology.

Stacking Members and Unit ID

Stacking Unit IDs are essential to the stacking configuration. The stacking operation is determined during the boot process. The Operation Mode is determined by the Unit ID selected during the initialization process. For example, if the user selected stand-alone mode, the device boots as a stand-alone device.

The device units are shipped with the default Unit ID of the stand-alone unit. If the device is operating as a stand-alone unit, all stacking LEDs are off. Once the user selects a different Unit ID, the default Unit ID is not erased, and remains valid, even if the unit is reset.

Unit ID 1 and Unit ID 2 are reserved for Master-enabled units. Unit IDs 3 to 6 can be defined for stack members.

When the Stacking Master unit boots, or when inserting or removing a stack member, the Stacking Master initiates a stacking discovering process.

If two members are discovered with the same Unit ID, the stack continues to function, however only the unit with the older join time joins the stack. A message is sent to the user, notifying that a unit failed to join the stack.

For first time Unit ID assignment, see the *Installation Guide*.

Removing and Replacing Stacking Members

Stacking member 1 and stacking member 2 are Master-enabled units. Unit 1 and Unit 2 are either designated as Stacking Master or Secondary Master. The Stacking Master assignment is performed during the configuration process. One Master-enabled stack member is elected Stacking Master, and the other Master-enabled stack member is elected Secondary Master, according to the following decision process:

If only one Master-enabled unit is present, it is elected Stacking Master.

If two Master-enabled stacking members are present, and one has been manually configured as the Stacking Master, the manually configured member is elected Stacking Master.

If two Master-enabled units are present and neither has been manually configured as the Stacking Master, the one with the longer up-time is elected Stacking Master.

If the two Master-enabled stacking members are the same age, Unit 1 is elected Stacking Master.

Two stacking member are considered the same age if they were inserted within the same ten minute interval.

For example, if Stack member 2 is inserted in the first minute of a ten-minute cycle, and Stack member 1 is inserted in fifth minute of the same cycle, the units are considered the same age. If there are two Master-enabled units that are the same age, then Unit 1 is elected Stacking Master.

The Stacking Master and the Secondary Master maintain a Warm Standby. The Warm Standby ensures that the Secondary Master takes over for the Stacking Master if a failover occurs. This guarantees that the stack continues to operate normally.

During the Warm Standby, the Master and the Secondary Master are synchronized with the static configuration only. When the Stacking Master is configured, the Stacking Master must synchronize the Secondary Master. The Dynamic configuration is not saved, for example, dynamically learned MAC addresses are not saved.

Each port in the stack has a specific Unit ID, port type, and port number, which are part of both the configuration commands and the configuration files. Configuration files are managed only from the device Stacking Master, including:

- Saving to the Flash
- Uploading configuration files to an external TFTP Server
- Downloading configuration files from an external TFTP Server

Whenever a reboot occurs, topology discovery is performed, and the Master learns all units in the stack. Unit IDs are saved in the unit and are learned through topology discovery. If a unit attempts to boot without a selected Master, and the unit is not operating in stand-alone mode, the unit does not boot.

Configuration files are changed only through explicit user configuration. Configuration files are not automatically modified when:

- Units are added
- Units are removed
- Units are reassigned Unit IDs
- Units toggle between Stacking mode and Stand-alone mode

Each time the system reboots, the Startup configuration file in the Master unit is used to configure the stack. If a stack member is removed from the stack and then replaced with a unit with the same Unit ID, the stack member is configured with the original device configuration. Only ports which are physically present are displayed in the Web Management Interface home page, and can be configured through the Web management system. Non-present ports are configured through the CLI or SNMP interfaces.

Exchanging Stacking Members

If a stack member with the same Unit ID replaces an existing Unit ID with the same Unit ID, the previous device configuration is applied to the inserted stack member. If the new inserted device has either more ports or less ports than the previous device, the relevant port configuration is applied to the new stack member.

The Secondary Master replaces the Stacking Master if the following events occur:

- The Stacking Master fails or is removed from the stack.
- Links from the Stacking Master to the stacking members fails.
- A soft switchover is performed via the web interface or the CLI.

Switching between the Stacking Master and the Secondary Master results in a limited service loss. Any dynamic tables are relearned if a failure occurs. The Running Configuration file is synchronized between the Stacking Master and the Secondary Master, and continues running on the Secondary Master.

Configuring Stacking Management

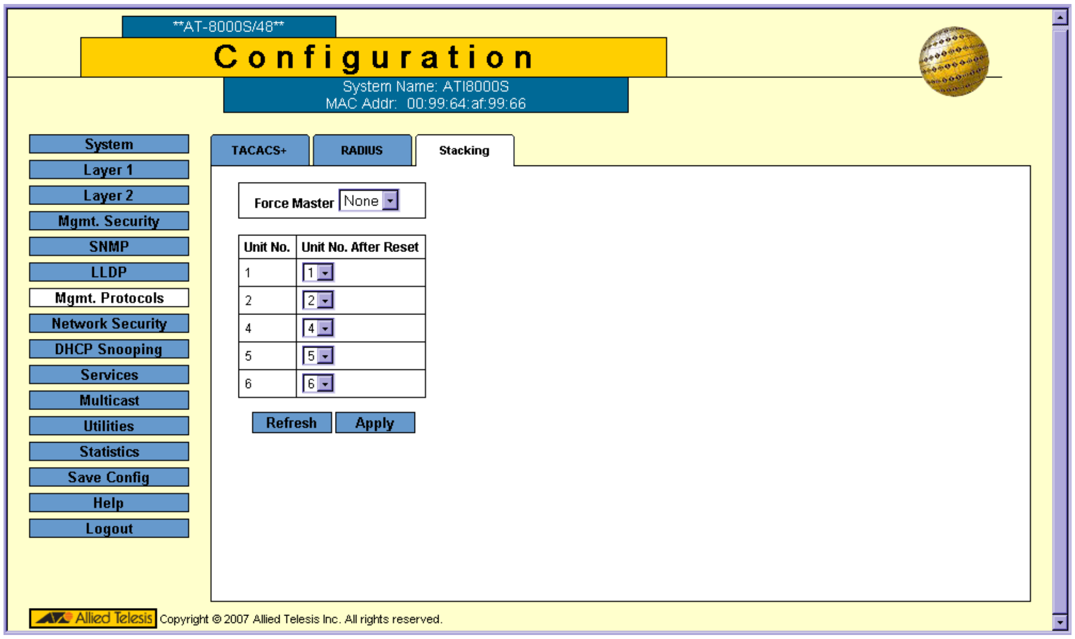
The *Stacking Page* allows network managers to either reset the entire stack or a specific device. Device configuration changes that are not saved before the device is reset are not saved. If the Stacking Master is reset, the entire stack is reset. In addition, Unit IDs can be changed on the *Stacking Page*.

When configuring QoS for stacking, note that stacking only uses three queues.

To configure stack control:

1. Click **Mgmt. Protocols > Stacking**. The *Stacking Page* opens:

Figure 164: Stacking Page



AT-8000S/48

Configuration

System Name: ATI8000S
MAC Addr: 00:99:64:af:99:66

Force Master: None

Unit No.	Unit No. After Reset
1	1
2	2
4	4
5	5
6	6

Copyright © 2007 Allied Telesis Inc. All rights reserved.

The *Stacking Page* contains the following stack configuration fields:

- **Force Master** — The unit is forced to be master of the stack. Note that only Unit 1 or Unit 2 can be the stack master. Select *None* for the system to decide which of the two master-enabled units is the master in the stack.
- **Unit No.** — Indicates the Unit ID assigned to the unit in the current stacking configuration.
- **Unit No. After Reset** — Indicates the Unit ID to be reassigned to the unit in the stacking configuration after reset.

2. Select the master election method, type of ports to be used in stacking,
3. Map/assign the unit numbers.
4. Click **Apply**. A confirmation message displays. The stacking settings are saved and the device configuration is updated.
5. Click **Refresh**. The stacking configuration is applied.
6. Click **Save Config** on the menu to save the changes permanently.

If a different Unit ID is selected, the device must be reset for the configuration changes to be applied.

Appendix A. Downloading Software with the CLI

This section describes how to download system files using the Command Line Reference (CLI), and includes the following topics:

- Connecting a Terminal
- Initial Configuration
- Downloading Software

Connecting a Terminal

Before connecting a device, ensure that the device has been installed according to the instructions described in the *Allied Telesis AT-S94 Installation Guide*.

Once installed the device is connected to a terminal through a console port (located on the front panel of 24 port devices and the back panel for the 48 port devices). The console connection enables a connection to a terminal desktop system running a terminal emulation software for monitoring and configuring the device. For a stack, only the console port of the Stacking Master is connected.

The terminal must be a VT100 compatible terminal or a desktop or portable system with a serial port and running VT100 terminal emulation software. The CLI can be accessed through the connected Terminal.

To connect a terminal to the device Console port, perform the following:

1. Connect a cable from the device console port to the terminal running VT100 terminal emulation software.
2. Ensure that the terminal emulation software is set as follows:
   a) Select the appropriate port to connect to the device.
   b) Set the data rate to 115, 200 baud.
   c) Set the data format to 8 data bits, 1 stop bit, and no parity.
   d) Set flow control to none.
   e) Under Properties, select VT100 for Emulation mode.
   f) Select **Terminal keys** for **Function**, **Arrow**, and **Ctrl** keys. Ensure that the setting is for Terminal keys (not Windows keys).

Note

When using HyperTerminal with Microsoft Windows 2000, ensure that you have Windows 2000 Service Pack 2 or later installed. With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal’s VT100 emulation. Go to www.microsoft.com for information on Windows 2000 service packs.

The device is now ready to download the system software.

Initial Configuration

Before a device can download system software, the device must have an initial configuration of IP address and network mask.

Before assigning a static IP address to the device, obtain the following information from the network administrator:

- A specific IP address allocated by the network administrator for the switch to be configured
- Network mask for the network

After making any configuration changes, the new configuration must be saved before rebooting. To save the configuration, enter the following CLI command: The following prompt is displayed:

```
Console# copy running-config startup-config
```

Configuration

The initial configuration, which starts after the device has booted successfully, includes static IP address and subnet mask configuration, and setting user name and privilege level to allow remote management. If the device is to be managed from an SNMP-based management station, SNMP community strings must also be configured. The following basic configurations are required:

- "Static IP Address and Subnet Mask"
- "User Name"

Static IP Address and Subnet Mask

IP interfaces can be configured on each port of the device. After entering the configuration command, it is recommended to check if a port was configured with the IP address by entering the “show ip interface” command.

The commands to configure the device are port specific.

To manage the switch from a remote network, a static route must be configured, which is an IP address to where packets are sent when no entries are found in the device tables. The configured IP address must belong to the same subnet as one of the device IP interfaces.

To configure a static route, enter the required commands at the system prompt as shown in the following configuration example where 101.101.101.101 is the specific management station, and 5.1.1.100 is the static route:

```
Console# configure
Console(config)# interface vlan 1
Console(config-if)# ip address 100.101.101.101 255.255.255.0
Console(config-if)# exit
Console# ip route 192.168.2.0/24 100.1.1.33
```

Note

100.1.1.33 is the IP address of the next hop that can be used to reach the management network 192.168.2.0.

To check the configuration, enter the command “show ip interface” as illustrated in the following example.

```
Console# show ip interface
Proxy ARP is disabled
IP Address                  I/F         Type        Broadcast
                                                    Directed
------------                ------      ------      ---------
100.101.101.101/24          vlan 1      static      disable
```

User Name

A user name is used to manage the device remotely, for example through SSH, Telnet, or the Web interface. To gain complete administrative (super-user) control over the device, the highest privilege (15) must be specified.

Note

Only an administrator (super-user) with the highest privilege level (15) is allowed to manage the device through the Web browser interface.

For more information about the privilege level, see the CLI Reference Guide.

The configured user name is entered as a login name for remote management sessions. To configure user name and privilege level, enter the command at the system prompt as shown in the configuration example:

```
Console> enable
Console# configure
Console(config)# username admin password lee privilege 15
```

Downloading Software

For this explanation, the following parameters are going to be used:

- **TFTP Server** — 172.16.101.101
- **System software file** — file1
- **Boot file** — file 2

Standalone Device Software Download

To download software an a standalone device perform the following:

1. Power up the device as described in the *Allied Telesis AT-S945 Installation Guide*. The CLI command prompt is displayed.

```
Console#
```

2. Enter the **copy** command to download the boot file.

```
Console# copy tftp://172.16.101.101/file2.rfb boot

Accessing file 'file2' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
09-Jul-2006 03:15:21 %COPY-W-TRAP: The copy operation was completed successfully
!
Copy: 3329361 bytes copied in 00:03:00 [hh:mm:ss]
```

3. Enter the “bootvar” command to determine which file contains the boot file. By default the inactive image area contains the newly downloaded boot file.

```
console# show bootvar
Unit  Image  Filename   Version    Date                    Status
----  -----  ---------  ---------  ---------------------   -----------
1     1      image-1    v1.1.0.29  25-Nov-2007  12:46:12   Not active
1     2      image-2    v1.1.0.29  25-Nov-2007  12:46:12   Active*
2     1      image-1    v1.1.0.29  25-Nov-2007  12:46:12   Not active
2     2      image-2    v1.1.0.29  25-Nov-2007  12:46:12   Active*
3     1      image-1    v1.1.0.29  25-Nov-2007  12:46:12   Active*
3     2      image-2    v1.1.0.29  25-Nov-2007  12:46:12   Not active
4     1      image-1    v1.1.0.29  25-Nov-2007  12:46:12   Active*
4     2      image-2    v1.1.0.29  25-Nov-2007  12:46:12   Not active
5     1      image-1    v1.1.0.29  25-Nov-2007  12:46:12   Active*
5     2      image-2    v1.1.0.29  25-Nov-2007  12:46:12   Not active
6     1      image-1    v1.1.0.29  25-Nov-2007  12:46:12   Active*
6     2      image-2    v1.1.0.29  25-Nov-2007  12:46:12   Not active

"*" designates that the image was selected for the next boot

console#
```

4. Enter the “boot system” command to change the booting image to the currently inactive image. In the example it is image 1 which has the latest downloaded boot file.

```
Console# boot system image-1
```

5. Enter the “copy” command to download the system file.

```
Console# copy tftp://172.16.101.101/file1.ros image

Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
09-Jul-2006 03:22:27 %COPY-W-TRAP: The copy operation was completed successfully
!
Copy: 6720861 bytes copied in 00:05:00 [hh:mm:ss]
```

6. Reboot the device. The device boots up with the updated boot and system files.

Stacking Member Software Download

Ensure the stack has been correctly connected as described in the *Allied Telesis AT-S94 Installation Guide*.

Downloading software to Stacking Members can be performed in the following ways:

- Download the software to an individual device in the stack. In this example the software is downloaded to the device defined as Stacking Member number 3.
- Download the software to all devices in the stack. The "*" character is used instead of the Stacking Member number.
- The software is downloaded to the device allocated as the Stacking Master, defined as Stacking Member number 1. The software is then copied from the Stacking Master to a specified Stacking Member.

Downloading Software to a Stacking Member

To download software an Stacking Member number 3 perform the following:

1. Power up the stack as described in the *Allied Telesis AT-S94 Installation Guide*. The CLI command prompt is displayed.

```
Console#
```

2. Enter the "copy" command to download the boot file.

```
Console# copy tftp://172.16.101.101/file2.rfb unit://3/boot

Accessing file 'file2' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
09-Jul-2006 03:15:21 %COPY-W-TRAP: The copy operation was completed successfully
!
Copy: 3329361 bytes copied in 00:03:00 [hh:mm:ss]
```

3. Enter the "bootvar" command to determine which file contains the boot file. By default the inactive image area contains the newly downloaded boot file.

```
Console# show bootvar
Images currently available on the FLASH
image-1 active   (selected for next boot)
image-2 not active
```

4. Enter the "boot system" command to change the booting image to the currently inactive image. In the example it is image 2 which has the latest downloaded boot file.

```
Console# boot system image-2
```

5. Enter the “copy” command to download the system file.

```
Console# copy tftp://172.16.101.101/file1.ros unit://3/image

Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
09-Jul-2006 03:22:27 %COPY-W-TRAP: The copy operation was completed successfully
!
Copy: 6720861 bytes copied in 00:05:00 [hh:mm:ss]
```

6. Reboot the devices being updated. The allocated devices boot up with the updated boot and system files.

Copying Software from the Stacking Master to a Stacking Member

To copy the software from the Stacking Master to a specified Stacking Member, number 4 in this example, perform the following:

1. Download the software to the Stacking Master as previously described, using the Stacking Member number 1 instead of number 3, as per the previous example.
2. Enter the “copy” command to copy the software from the Stacking Master to the Stacking Member. To copy the software from the Stacking Master to all the Stacking Members, use the “*” character instead of the Stacking Member number, number 4 in this example.

```
Console# copy unit://1/image unit://4/image
```

3. Reboot the devices being updated. The allocated devices boot up with the updated boot and system files.

Appendix B. System Defaults

This section contains the system defaults, and includes the following topics:

- RS-232 Port Settings
- Port Defaults
- Configuration Defaults
- Security Defaults
- Jumbo Frame Defaults
- System Time Defaults
- Spanning Tree Defaults
- Address Table Defaults
- VLAN Defaults
- Trunking Defaults
- Multicast Defaults
- QoS Defaults

RS-232 Port Settings

The following table contains the RS-232 port setting defaults:

Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Baud Rate	115,200 bps

Port Defaults

The following are the port defaults:

Auto Negotiation	Enabled
Auto Negotiation advertised capabilities	Enabled
Auto MDI/MDIX	Enabled
Head of Line Blocking	Enabled
Back Pressure	Disabled
Flow Control	Disabled
Cable Analysis	Disabled
Optical Transceiver Analysis	Disabled
Manual Port Control and Identification	Disabled

Configuration Defaults

The following are the initial device configuration defaults:

Default User Name	manager
Default Password	friend
System Name	None
Comments	None
BootP	Enabled
DHCP	Disabled

Security Defaults

The following are the system security defaults:

Locked Ports	Disabled
802.1X Port Based Authentication	Disabled
Storm Control	Disabled
DHCP Snooping	Disabled

Jumbo Frame Defaults

The following is the Jumbo Frame default:

Jumbo Frame After Reset	Disabled

System Time Defaults

The following is the system time default:

SNTP	Enabled

Spanning Tree Defaults

The following are the spanning tree defaults:

STP	Enabled
STP Port	Enabled
Rapid STP	Enabled
Multiple STP	Disabled
Fast Link	Disabled
Path Cost	Long

Address Table Defaults

The following the Address Table defaults:

Number of MAC Entries	8,000
MAC Address Aging Time	300 seconds
VLAN-Aware MAC-based Switching	Enabled

VLAN Defaults

The following are the VLAN defaults:

Possible VLANs	256
GVRP	Disabled
Management VLAN	VLAN 1
Join Timer	20 centiseconds
Leave Timer	60 centiseconds
Leave All Timer	1000 centiseconds
Private VLAN Edge	Enabled

Trunking Defaults

The following are the trunking defaults:

Possible Trunks	8
Possible Ports per Trunk	8
LACP Ports/Trunk	16

Multicast Defaults

The following are the Multicast defaults:

IGMP Snooping	Disable
Maximum Multicast Groups	256

QoS Defaults

The following are the QoS defaults:

QoS Mode	Disable	
Queue Mapping	Cos	Queue
	0	2
	1	1
	2	1
	3	2
	4	3
	5	3
	6	4
	7	4
	DSCP	Queue
	1	0-15
	2	16-31
	3	32-47
	4	48-63

Index