GS700TS Series Smart Switch Software User Manual

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10228-01
November 2006
v1.0

Trademarks

NETGEAR, the NETGEAR logo, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

November 2006

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Certificate of the Manufacturer/Importer

It is hereby certified that the GS700TS Smart Switch with Gigaport Ports has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß dasGS700TS Smart Switch with Gigaport Ports gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Product and Publication Details

Model Number:	GS700TS
Publication Date:	November 2006
Product Family:	Smart Switch
Product Name:	GS700TS Smart Switch with Gigaport Ports
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10228-01
Publication Version Number:	1.0

Contents

About This Manual

Chapter 1
Switch Management Overview

Chapter 2
Getting Started

Chapter 3
Smartwizard Discovery Program

Chapter 4
Software Upgrade Procedure

Chapter 5
Configuring The Device Using Your Browser

About This Manual

The *NETGEAR® GS700TS Series Smart Switch Software User Manual* describes how to install, configure and troubleshoot the GS700TS Series Smart Switch. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed`	Screen text, file and server names, extensions, commands, IP addresses

- **Formats.** This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Tip: This format is used to highlight a procedure that will save time or resources.

Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.

Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the GS700TS Series Smart Switch according to these specifications:

Product Version	GS700TS Smart Switch with Gigaport Ports
Manual Publication Date	November 2006

Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/downloads_support.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A ☰ button that Displays the table of contents and an button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View**. Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.
- **Printing a Chapter**. Use the *PDF of This Chapter* link at the top left of any page.
  - Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

  - Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.
  - Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual**. Use the *Complete PDF Manual* link at the top left of any page.
  - Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
  - Click the print icon in the upper left of the window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 1
Switch Management Overview

This section provides an overview of switch management, including the methods you can use to manage your NETGEAR GS700TS family of Smart Gigabit Ethernet Switches.

Your NETGEAR GS700TS family of Smart Gigabit Ethernet Switches contains software for viewing, changing, and monitoring the way the Smart Switch works. Using the management software to configure your switch is not required for any of the gigabit ports to work properly. However, the management software does allow you to configure ports, VLAN and Trunking features to improve the efficiency of the switch and, as a result, improve the overall performance of your network. The switch gives you the flexibility to access and manage the switch using any of the following methods:

- Smartwizard Discovery program
- Web browser interface

After you power-up the switch for the first time, you can configure it using a utility program called Smartwizard Discovery or a Web browser. Please refer to the screenshots in following pages for Smartwizard Discovery and Web Management GUI. Each of these management methods has advantages.

Table 1 compares the three management methods.

Table 1: Comparing Switch Management Methods

Management Method	Advantages
Smartwizard Discovery program	No IP address or subnet needed Shows all switches on the network User-friendly interface Firmware upgradeable
Web browser	Can be accessed from any location via the switch’s IP address Password protected Ideal for configuring the switch remotely Compatible with Internet Explorer and Netscape Navigator Web browsers Intuitive browser interface Most visually appealing Extensive switch configuration allowed Configuration backup for duplicating settings to other switches

For a more detailed discussion of the Smartwizard Discovery Program, see *Chapter 3*. For a more detailed discussion of the Web Browser Interface, see *Chapter 5*.

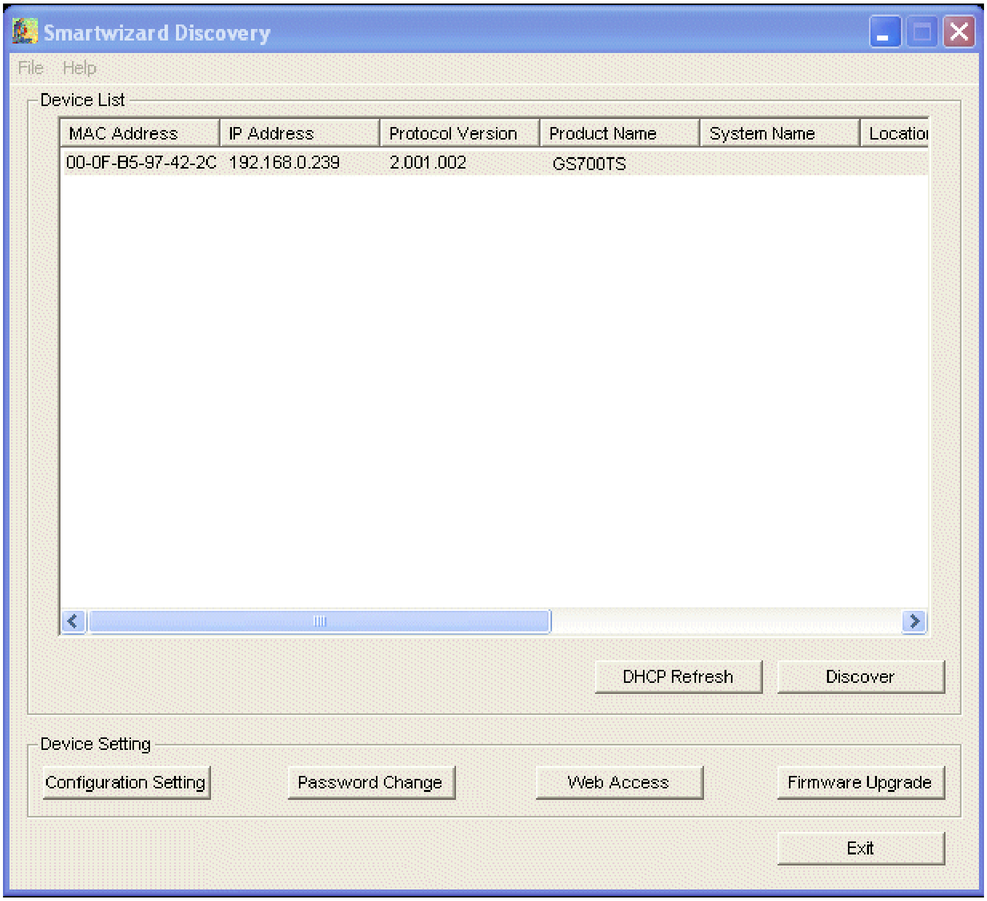
Chapter 2
Getting Started

This section walks you through the steps to start managing your GS700TS switch. This section covers how to get started in a network with a DHCP server (most common) as well as if you do not have a DHCP server.

Network with DHCP Server

1. Connect the GS700TS switch to a DHCP network.
2. Power on the GS700TS switch by plugging in power cord.
3. Install the Smartwizard Discovery program on your computer.

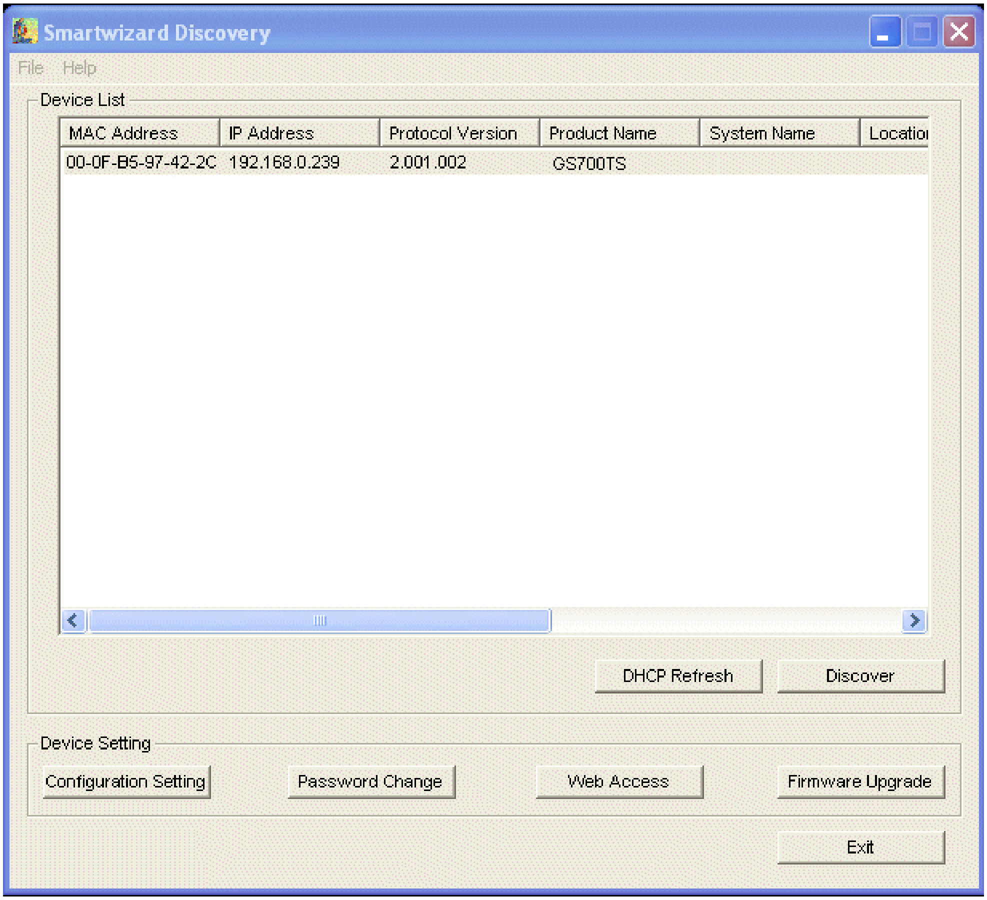
   Start Smartwizard Discovery (*Chapter 3* contains detailed instructions on the Smartwizard Discovery).
4. Click Discover to enable the Smartwizard Discovery to find your GS700TS switch, see *Figure 2-1*.



MAC Address	IP Address	Protocol Version	Product Name	System Name	Locatio
00-0F-B5-97-42-2C	192.168.0.239	2.001.002	GS700TS		

Figure 2-1

5. Select the switch from the Device List. Then click Web Access, see *Figure 2-2*.



MAC Address	IP Address	Protocol Version	Product Name	System Name	Locatio
00-0F-B5-97-42-2C	192.168.0.239	2.001.002	GS700TS		

Figure 2-2

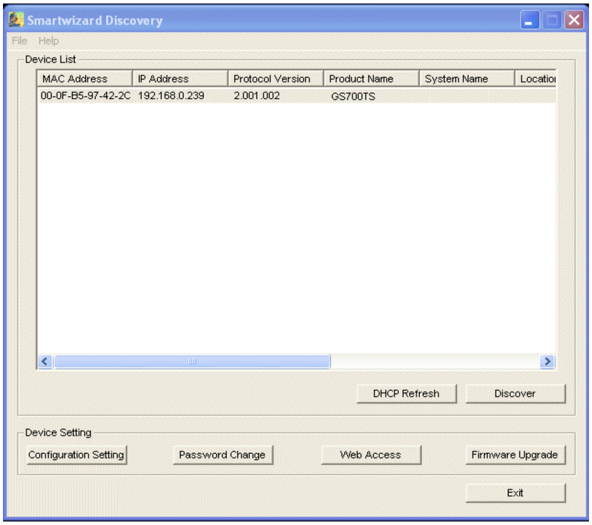
6. Start managing your switch via your web browser. The default password is “*password*”. For a detailed description on web management, please refer to *Chapter 5*.

Network without DHCP Server

A static IP address can be assigned to the GS700TS device even if the network does not have a DHCP server.

1. Connect the GS700TS switch to your existing network.
2. Power on the GS700TS switch by plugging in the power cord. The default IP is 192.168.0.239.
3. Install the Smartwizard Discovery program on your computer.

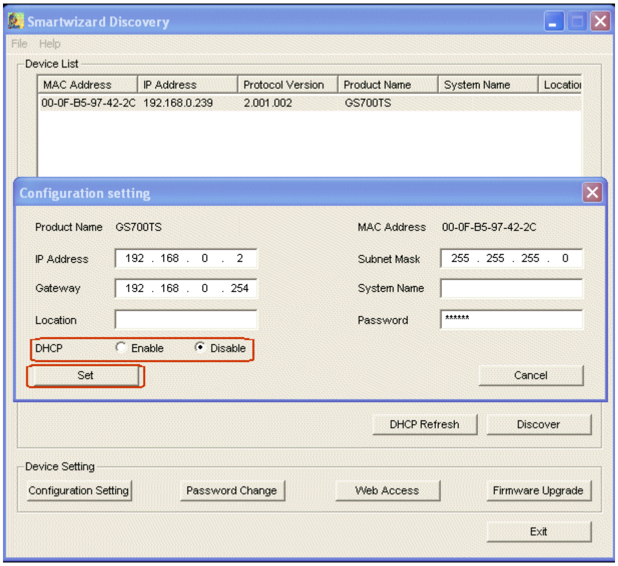
   Start Smartwizard Discovery (*Chapter 3* has detailed instructions on the Smartwizard Discovery).
4. Click Discover to enable the Smartwizard Discovery to find your GS700TS switch.
5. Click Configuration Setting (See *Figure 2-3*).



MAC Address	IP Address	Protocol Version	Product Name	System Name	Locatio
00-0F-B5-97-42-2C	192.168.0.239	2.001.002	GS700TS		

Figure 2-3

6. Choose Disable on DHCP. See *Figure 2-4*.
7. Enter your static IP address, Gateway and Subnet, and then type your password and click *Set*. Please make sure your PC and GS700TS switch are in the same subnet (See *Figure 2-5*).



Smartwizard Discovery

File Help

Device List

MAC Address	IP Address	Protocol Version	Product Name	System Name	Locatio
00-0F-B5-97-42-2C	192.168.0.239	2.001.002	GS700TS		

Configuration setting

Product Name GS700TS

MAC Address 00-0F-B5-97-42-2C

IP Address 192 . 168 . 0 . 2

Subnet Mask 255 . 255 . 255 . 0

Gateway 192 . 168 . 0 . 254

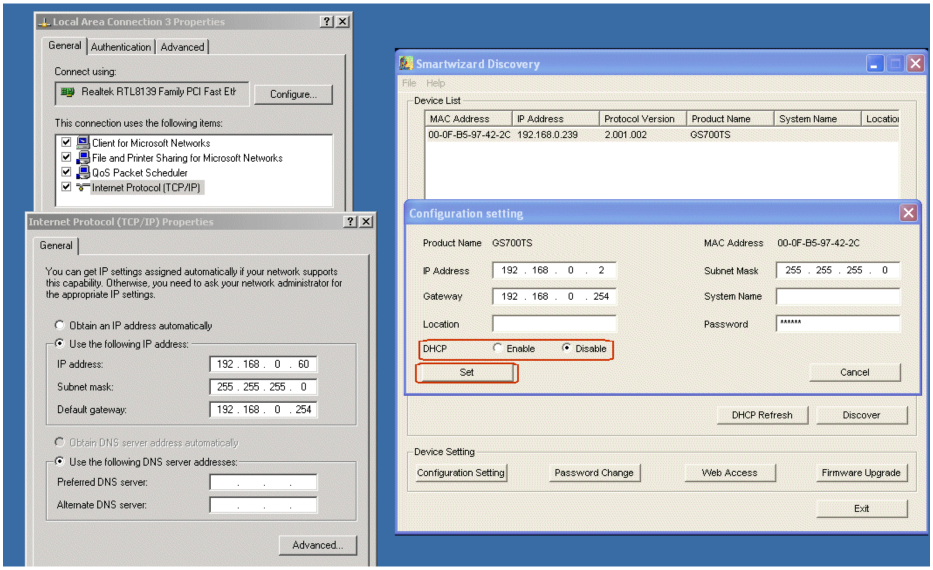
System Name

Location

Password ******

DHCP ○ Enable ● Disable

Figure 2-4



Local Area Connection 3 Properties

General | Authentication | Advanced

Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 60

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Smartwizard Discovery

File Help

Device List

MAC Address	IP Address	Protocol Version	Product Name	System Name	Locatio
00-0F-B5-97-42-2C	192.168.0.239	2.001.002	GS700TS		

Configuration setting

Product Name GS700TS

MAC Address 00-0F-B5-97-42-2C

IP Address 192 . 168 . 0 . 2

Subnet Mask 255 . 255 . 255 . 0

Gateway 192 . 168 . 0 . 254

System Name

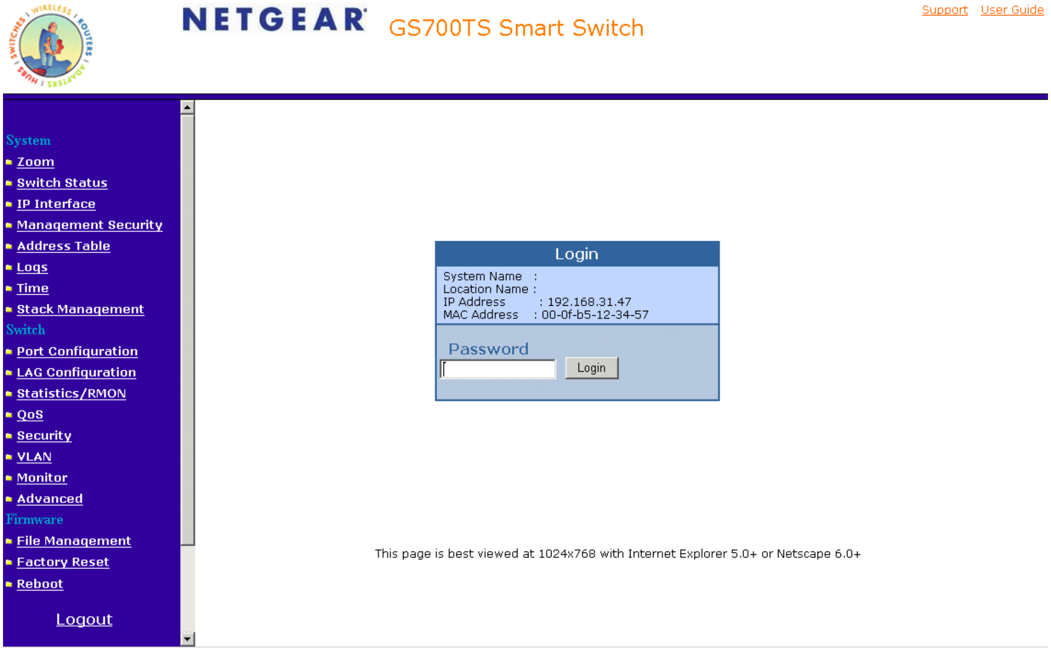
Location

Password ******

DHCP ○ Enable ● Disable

Figure 2-5

8. Select your switch by clicking on it. Then click on Web Access, see *Figure 2-6*.
9. Start managing your switch via your web browser. The default password is ‘password’. For a detailed description on web management access, please refer to *Chapter 5*.



System Name :
Location Name :
IP Address : 192.168.31.47
MAC Address : 00-0f-b5-12-34-57

This page is best viewed at 1024x768 with Internet Explorer 5.0+ or Netscape 6.0+

Figure 2-6

Chapter 3
Smartwizard Discovery Program

The Smartwizard Discovery program is a user-friendly, easy to install tool. Using this program, you can view and configure all the GS700TS Smart Switches in your network.

The installation of the Smartwizard Discovery is as follows:

1. Insert the disc into your CD-ROM drive.
2. Select the \Software folder or click ‘install’ from Browser auto-executed after inserting the Resource CD.
3. Run the Setup program to install the Smartwizard Discovery.
4. The Installation Wizard will guide you through.
5. Run ‘Smartwizard Discovery’ from the window start bar.

Main Screen

The main screen displays the available functions. As shown in *Figure 3-7*, there are six items from which to choose:

- Discover
- Configuration Setting
- Password Change
- Web Access
- Firmware Upgrade
- Exit

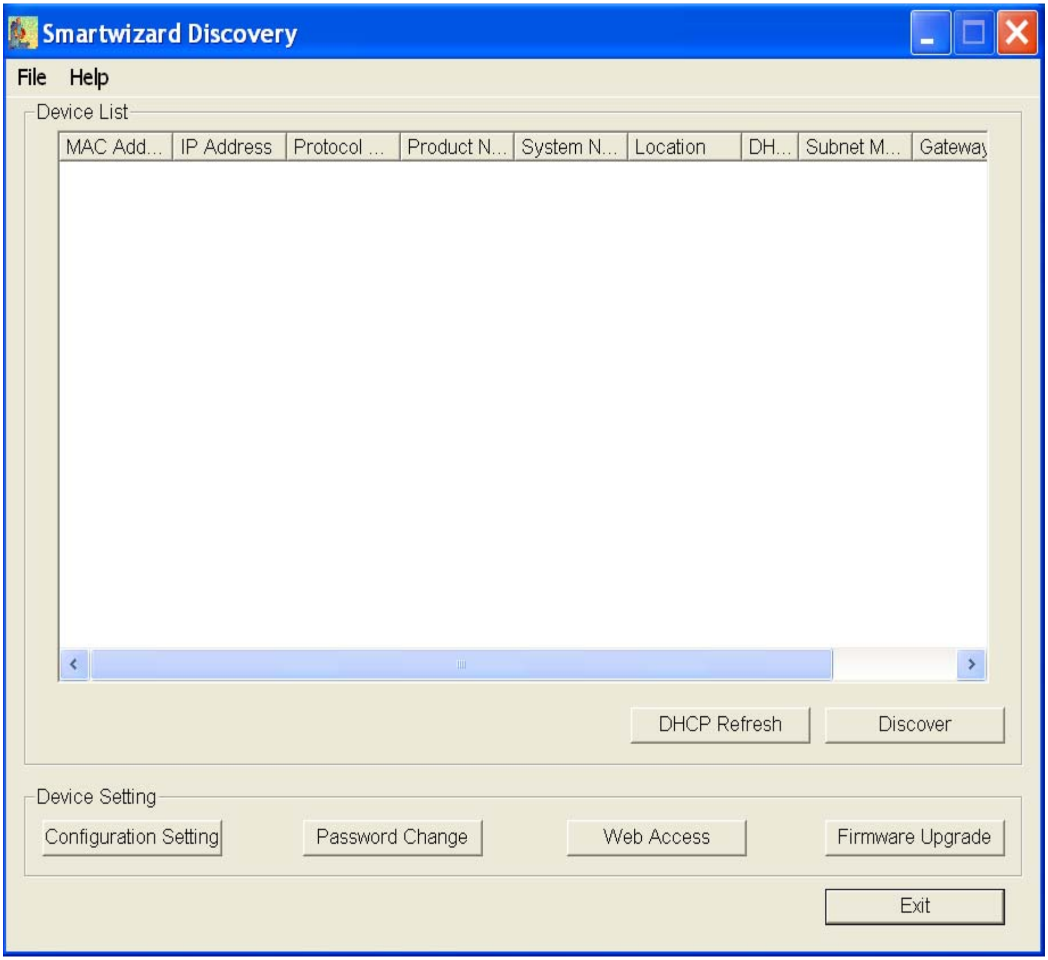


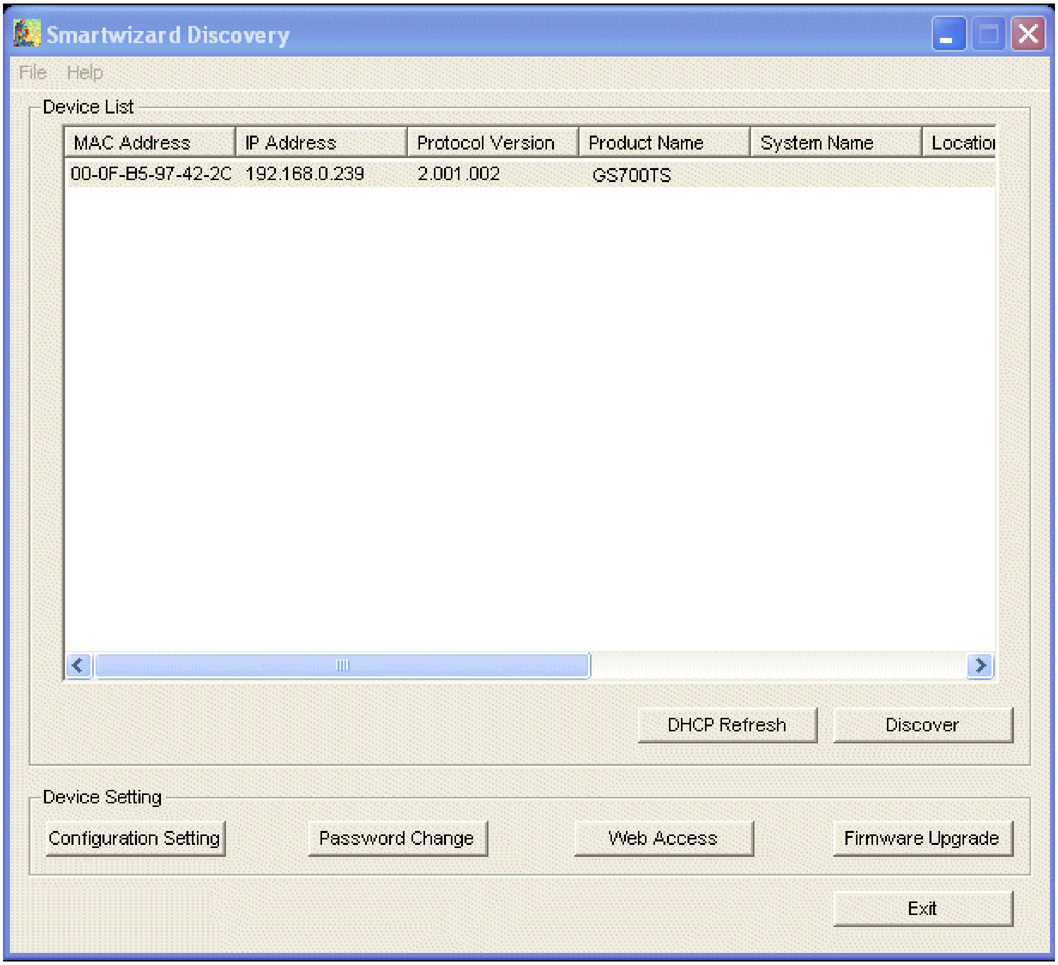
Figure 3-7

Main Screen > Device List > Discover

The Smartwizard Discovery can discover all switches currently connected on the network. Click **Discover** to view the following switch information of any listed switch:

- MAC Address
- IP Address
- Protocol Version

- Product Name
- System Name
- Location
- DHCP
- Subnet Mask
- Gateway
- Firmware Version



MAC Address	IP Address	Protocol Version	Product Name	System Name	Locatio
00-0F-B5-97-42-2C	192.168.0.239	2.001.002	GS700TS		

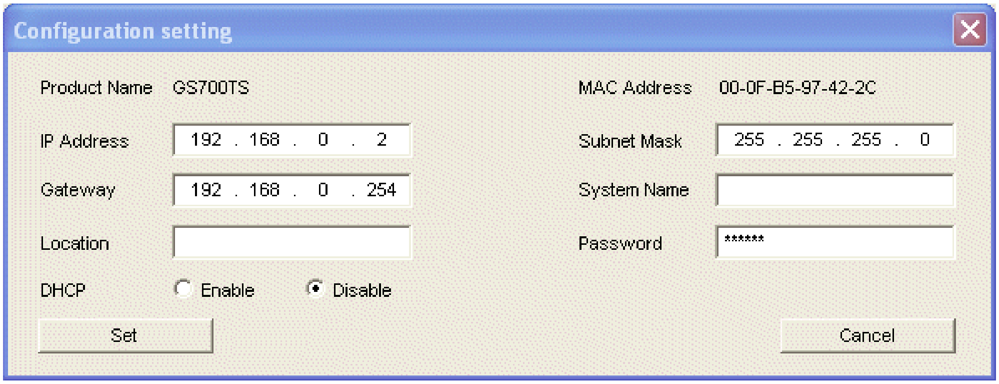
Figure 3-8

By double-clicking a listed switch, you can open the Web management for that switch. Alternatively, you can select a switch by clicking on it once, and then clicking Web Access. For more information on Web management, see *Chapter 5*.

Main Screen > Switch Setting > Configuration Setting

Select a switch by clicking on it. Then click Configuration Setting. The following screen pops up and displays the Product Name and MAC Address. From this screen, you can modify the following:

- **IP Address** – Displays the currently configured IP address.
- **Subnet Mask** – Displays the currently configured Subnet Mask.
- **Gateway** – Displays the currently configured Gateway.
- **System Name** – Provides a user-defined system name field. The System Name field helps you keep track of your switches. It can be any combination of letters and/or numbers.
- **Location** – Provides a user-defined field to help you keep track of where this switch is. It can be any combination of letters and/or numbers.
- **DHCP** – DHCP automatically obtains the IP information for the switch.



Configuration setting

Product Name	GS700TS	MAC Address	00-0F-B5-97-42-2C
IP Address	192 . 168 . 0 . 2	Subnet Mask	255 . 255 . 255 . 0
Gateway	192 . 168 . 0 . 254	System Name	
Location		Password	******
DHCP	○ Enable ● Disable		

Figure 3-9

Main Screen > Device Setting > Configuration Setting > Set

Click ‘Set’ to enable new settings. You must enter your password for these settings to be accepted.

Main Screen > Device Setting > Configuration Setting > Cancel

Click ‘Cancel’ to abort the above settings.

Main Screen > Switch Setting> > Password Change

1. Click ‘Password Change’ from the Switch Setting section. The following screen pops up as shown in *Figure 3-10*.

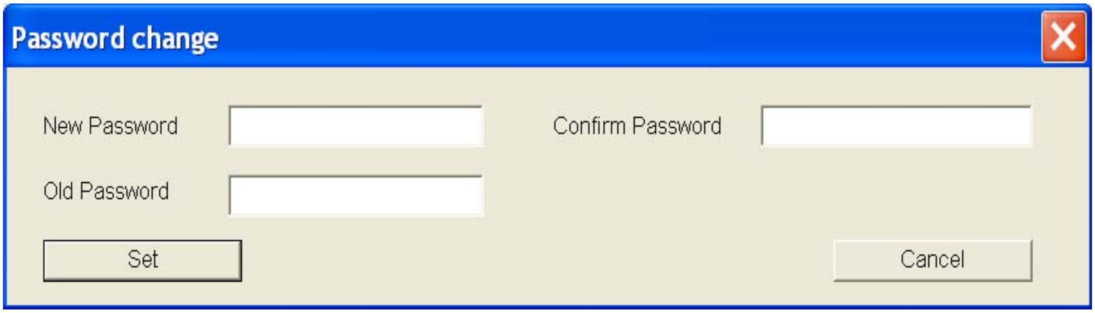


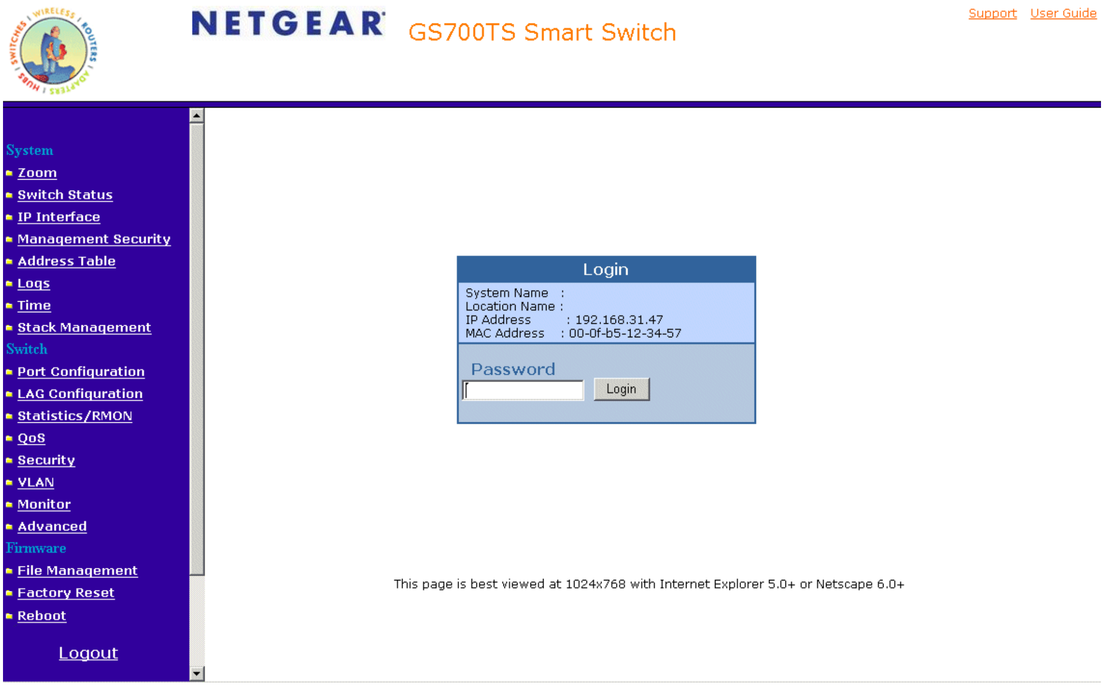
Figure 3-10

- **New Password** – Type any desired password. Passwords are case-sensitive and can have a maximum of 20 characters.
- **Confirm Password** – Re-type the new password to confirm it.
- **Old Password** – The default password is ‘password’.

2. Click Set to enable new password.

Main Screen > Switch Setting > Web Access

1. Select a listed switch from the Device List section. Then click Web Access from the Switch Setting, see *Figure •*.
2. Enter the default password “password” and click Log in.



System Name :
Location Name :
IP Address : 192.168.31.47
MAC Address : 00-0f-b5-12-34-57

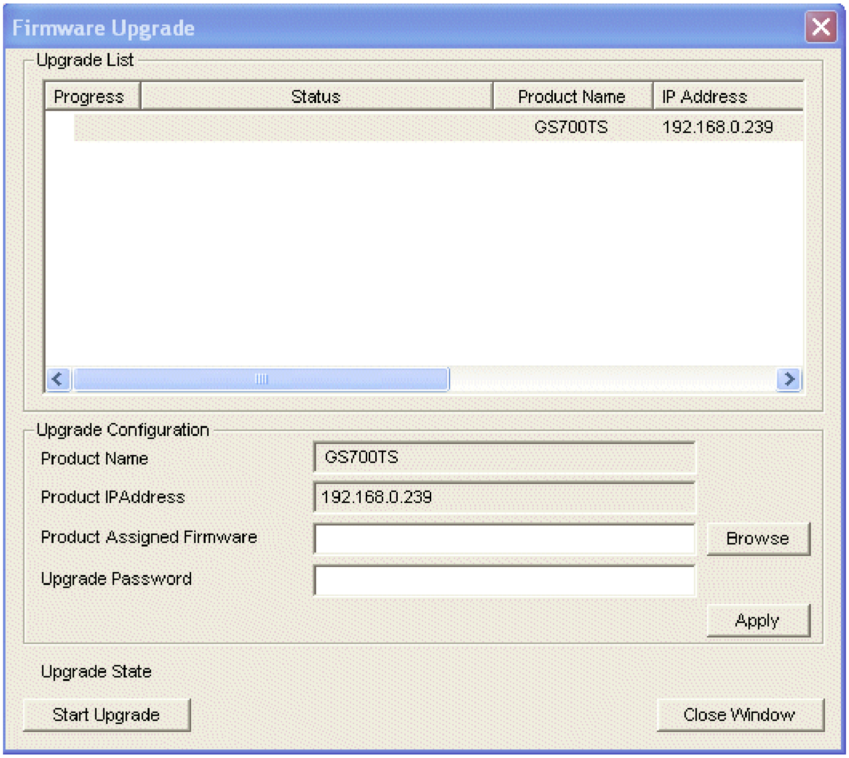
This page is best viewed at 1024x768 with Internet Explorer 5.0+ or Netscape 6.0+

-

For more on Web management, see *Configuring The Device Using Your Browser*.

Main Screen > Switch Setting > Firmware Upgrade

1. Click **Firmware Upgrade** from the Switch Settings section. The following screen opens.



Progress	Status	Product Name	IP Address
		GS700TS	192.168.0.239

Product Name: GS700TS

Product IPAddress: 192.168.0.239

Product Assigned Firmware:

Upgrade Password:

Figure 3-11

- **Firmware Path** – The location of the new firmware. If you do not know the location, you can click Browse to locate file.
- **Password** – The default password is 'password'.
- **Upgrade State** – Shows upgrading in progress.

2. Click **Start Upgrade** to start upgrading.

Main Screen > Switch Setting > Exit

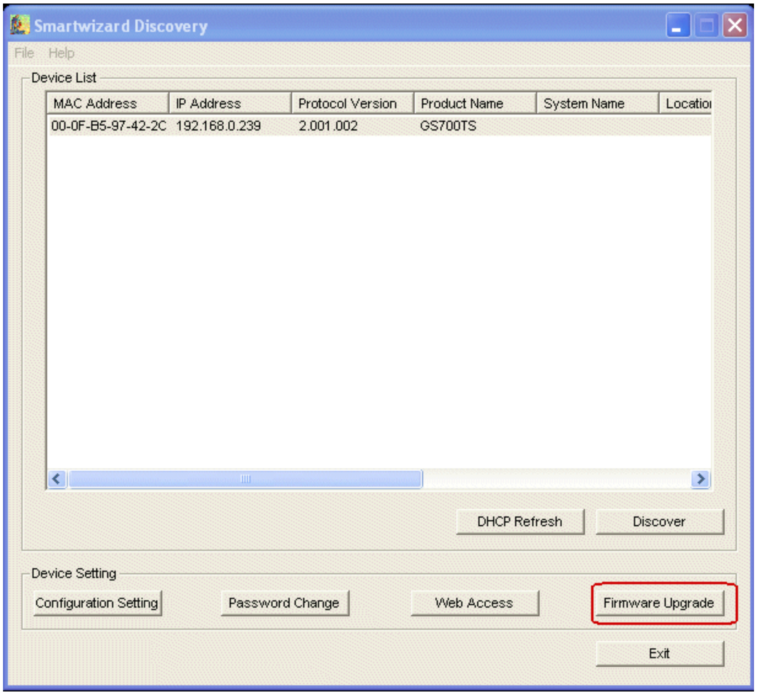
Click **Exit** from the Switch Setting section to close the Smartwizard Discovery program.

Chapter 4
Software Upgrade Procedure

The application software for the GS700TS switch is upgradeable, enabling your switch to take advantage of improvements and additional features as they become available. The application software needs to be downloaded from a TFTP server containing the software updates. The upgrade procedure and the required equipment are described in the following section.

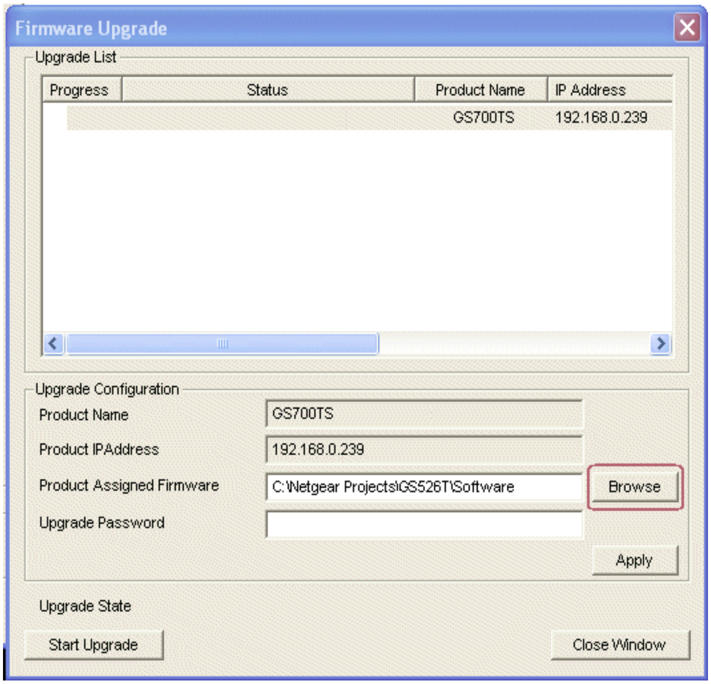
The upgrade procedure is as follows:

1. Save the new firmware to your computer.
2. Start the *Smartwizard Discovery Program* program.
3. Select your switch by clicking on it. Then click on Firmware Upgrade, see *Figure 4-12*.



MAC Address	IP Address	Protocol Version	Product Name	System Name	Locatio
00-0F-B5-97-42-2C	192.168.0.239	2.001.002	GS700TS		

Figure 4-12



Firmware Upgrade

Upgrade List

Progress	Status	Product Name	IP Address
		GS700TS	192.168.0.239

Upgrade Configuration

Product Name: GS700TS

Product IPAddress: 192.168.0.239

Product Assigned Firmware: C:\Netgear Projects\GS526T\Software

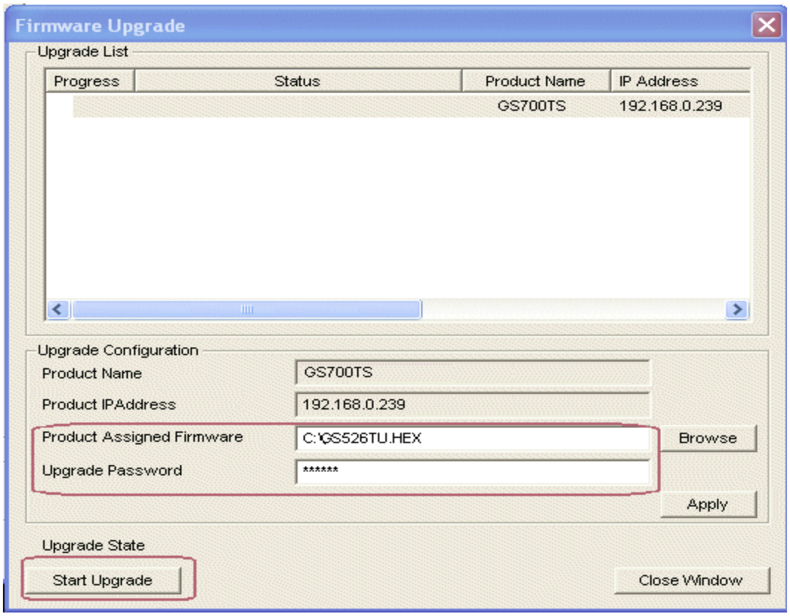
Upgrade Password:

Upgrade State

Figure 4-13

4. Enter the location of the new firmware in the Firmware path below Firmware setting. Alternatively, you can click Browse to locate the file. Enter following path: tftp://{tftp address}/{file name}.
5. Enter Password.
6. Click Apply.

7. Click Start to download the new firmware file in non-volatile memory. The system software is automatically loaded to all stacking members.



Progress	Status	Product Name	IP Address
		GS700TS	192.168.0.239

Product Name: GS700TS

Product IPAddress: 192.168.0.239

Product Assigned Firmware: C:\GS526TU.HEX

Upgrade Password: ******

Figure 4-14

Once the system finishes the firmware upgrade process, the switch automatically reboots. Smartwizard Discovery determines the success of the upgrade process based on the success of the system reboot.

Chapter 5
Configuring The Device Using Your Browser

This section contains information for configuring the device using your web browser and includes the following topics:

- Introduction
- Rebooting the System
- Defining Device Information
- Managing Stacking
- Defining RADIUS Settings
- Configuring Interfaces
- Defining IP Interface
- Defining the Forwarding Address Tables
- Configuring the Spanning Tree Protocol
- Configuring Multicast Forwarding
- Configuring Quality of Service
- Configuring SNMP Security
- Monitoring the Device
- Managing RMON Statistics
- Resetting the Factory Default Values

Introduction

This section describes setting browser interface options and using the GS700TS switch's home page. It includes the following sections:

- Opening the NETGEAR GS700TS Home Page
- Understanding the Home Page
- Using The NETGEAR Web Management System Buttons

Opening the NETGEAR GS700TS Home Page

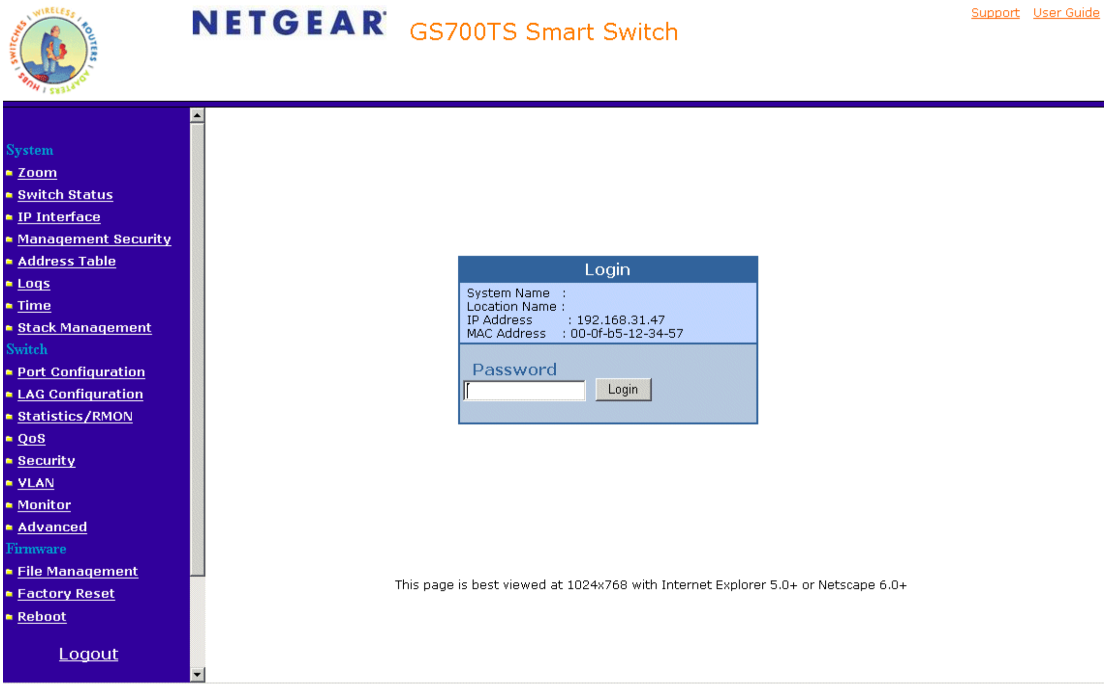
The NETGEAR GS700TS switch home page can be accessed from any PC with a web browser.

To start the NETGEAR application:

1. Open a web browser.

2. Enter the device IP address in the address bar.

3. Press Enter. The Logon Page appears.



System Name :
Location Name :
IP Address : 192.168.31.47
MAC Address : 00-0f-b5-12-34-57

This page is best viewed at 1024x768 with Internet Explorer 5.0+ or Netscape 6.0+

Figure 5-15

4. Enter a password.

5. Click Login. The NETGEAR GS700TS home page is displayed.

Understanding the Home Page

The NETGEAR GS700TS home page contains the following views:

- **Navigation Pane** – Located on the left side of The NETGEAR GS700TS home page. The Navigation Pane provides an expandable Navigation Pane of the features and their component.
- **Device View** – Located on the right side of The NETGEAR GS700TS home page. The Device View provides a view of the device, an information or table area, and of configuration instructions.
- **Information Buttons** – Located in the upper right corner of the home page, the information buttons provide connections to NETGEAR support and the online manual.

Navigation Pane

The Navigation Pane contains a list of the different features that can be configured including switching features, ports, spanning tree, VLANs, class of service, link aggregation (aggregating ports), multicast support, and statistics. The Navigation Pane branches can be expanded to view all the components under a specific feature or retracted to hide the feature's components.

Device View

The following section describes the different aspects of the Device View. The device provides information about the different components and the Work Desk. The Work Desk in the Device View provides a work area that contains device tables, general device information, and configurable device parameters.

Using The NETGEAR Web Management System Buttons

This section contains information about the different NETGEAR GS700TS browser interface buttons. The GS700TS web browser provides the following buttons:

- **Information Buttons** – Provide access to informational services including technical support, online help, device information, and closing the NETGEAR browser.
- **Device Management Buttons** – Provide an explanation of the management buttons in the NETGEAR GS700TS Switch, including the Add, Delete, Query, and Apply Changes buttons.

- **Information Buttons** – The NETGEAR GS700TS Switch web browser contains the following information buttons:

Table 5-1. Information Buttons

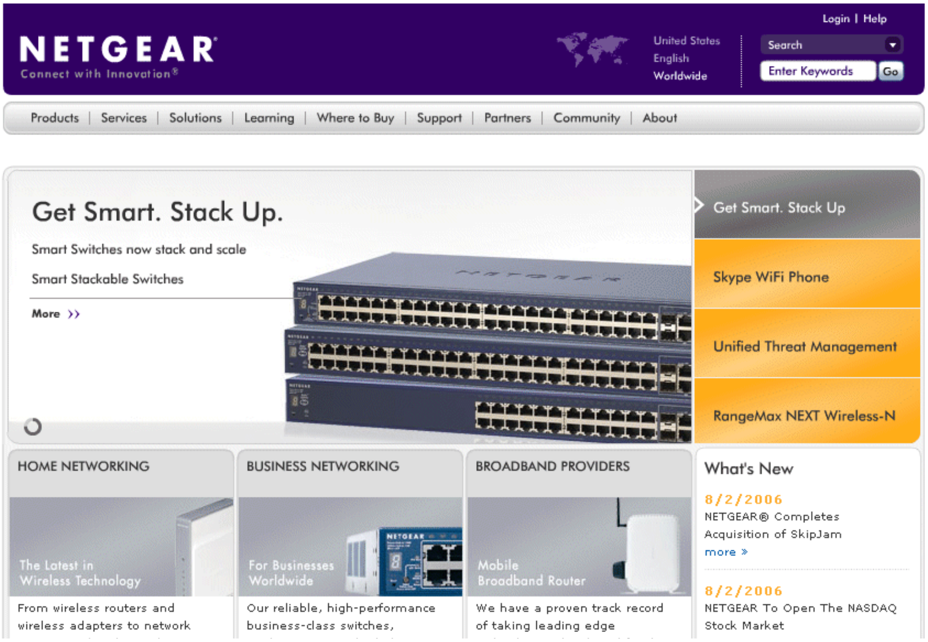
Button	Description
Support	Opens the NETGEAR support page. The NETGEAR technical support page URL is http://kbserver.netgear.com/main.asp.
User Guide	Opens the online manual.
Help	Opens the context sensitive online help.

Support Button

The Support section contains information for accessing NETGEAR technical support.

To access the technical support page:

1. Click **Support** on the NETGEAR home page. The Support section opens:



From wireless routers and wireless adapters to network

Our reliable, high-performance business-class switches,

We have a proven track record of taking leading edge

8/2/2006
NETGEAR® Completes Acquisition of SkipJam

8/2/2006
NETGEAR To Open The NASDAQ Stock Market

Figure 5-16

2. Enter the product name in the Search field. The search results are returned.

Help Button

The online help contains information to assist in configuring and managing the switch. Help topics can be located using the help search, referenced by index entry, or referenced by help topic in the help navigation pane.

To access the online help:

- Select a help topic. The selected help topic page opens.

Or

- Click . The online help opens.

Device Management Buttons

The NETGEAR GS700TS Switch web browser GUI management buttons allow network managers to easily configure the device from remote locations. The NETGEAR GS700TS Switch web browser GUI contains the following management buttons:

Table 5-2. Device Management Buttons

Button	Description
	Applies set changes to the device.
	Adds information to tables or information windows.
	Refreshes device information.
	Resets statistics counters.
	Performs copper cable test.
	Restores the factory defaults.

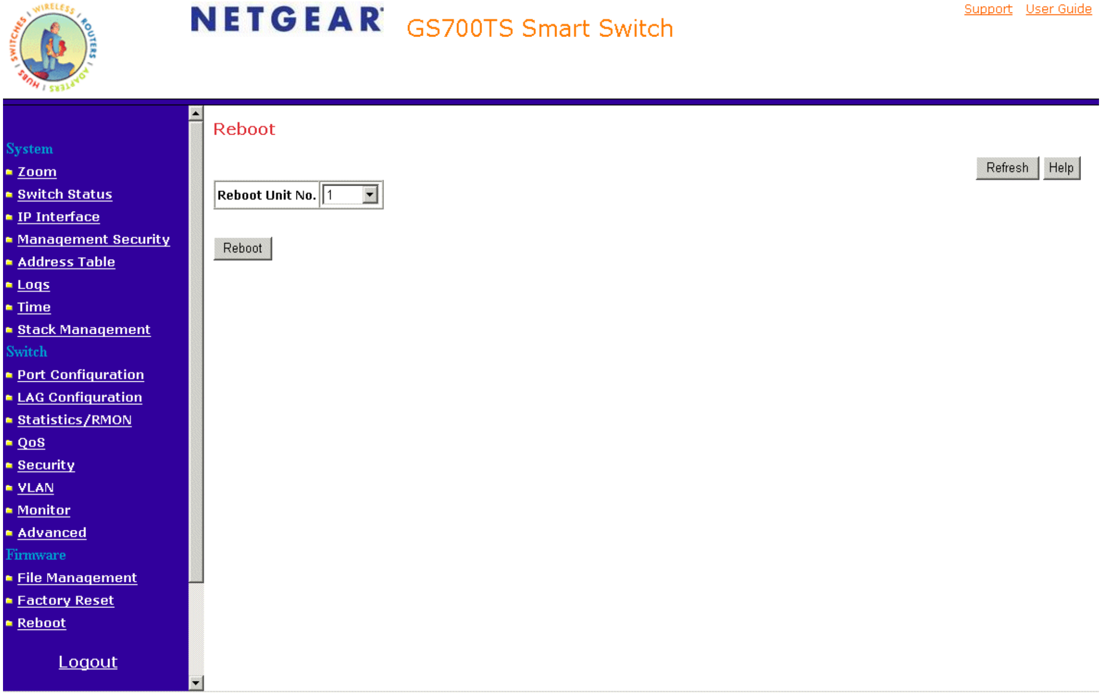
Rebooting the System

The *Reboot Page* resets the device. Ensure that configuration changes are saved to the device before rebooting. Configuration changes that are not saved are lost. There are two options to reboot.

- Rebooting a particular unit.
- Rebooting the entire stack.

To open the *Reboot Page*:

1. Click Reboot on the Navigation Pane on the left. The *Reboot Page* opens.



Reboot Unit No. 1

Figure 5-17

The *Reboot Page* contains the following field:

- **Reboot Unit No.** – Choose the port to be reset or select the option Stack to reboot all stacking members.

2. Click Reboot . The device is reset.

Defining Device Information

This section contains the following topics:

- Viewing the Device Zoom View
- Viewing the Device Information
- Configuring System Time

Viewing the Device Zoom View

The *System Zoom Page* provides a graphic representation of the device, including the port and LED statuses. Clicking on a port will bring up the Modify Port Configuration Screen.

To view the *System Zoom Page*:

1. Click **Zoom**. The *System Zoom Page* opens.

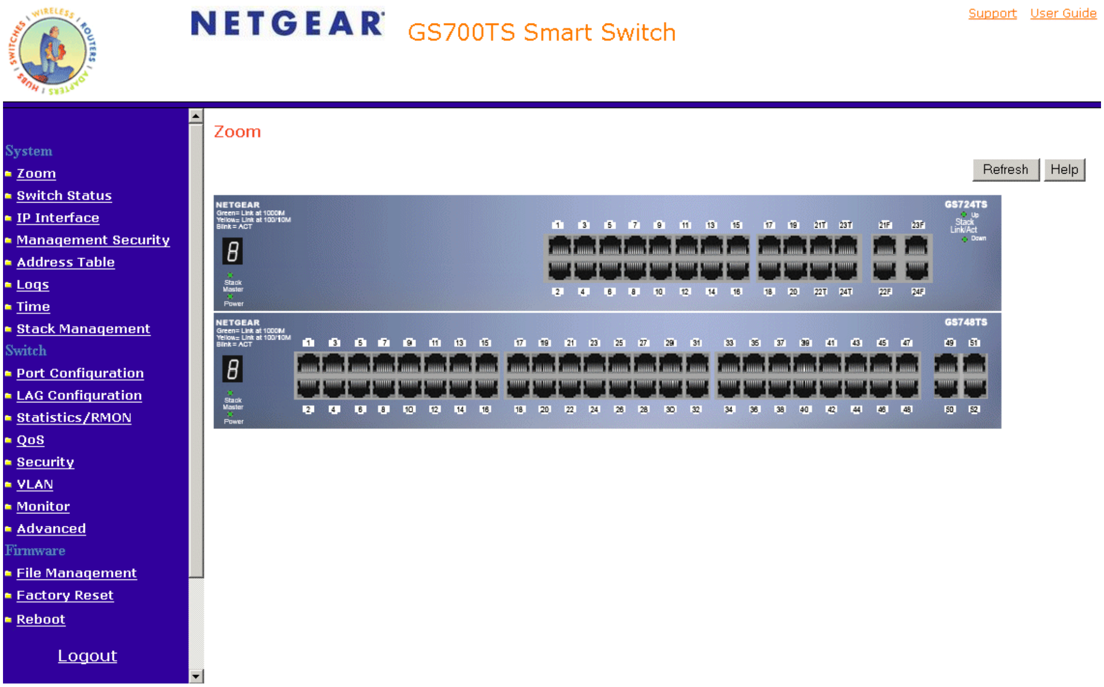


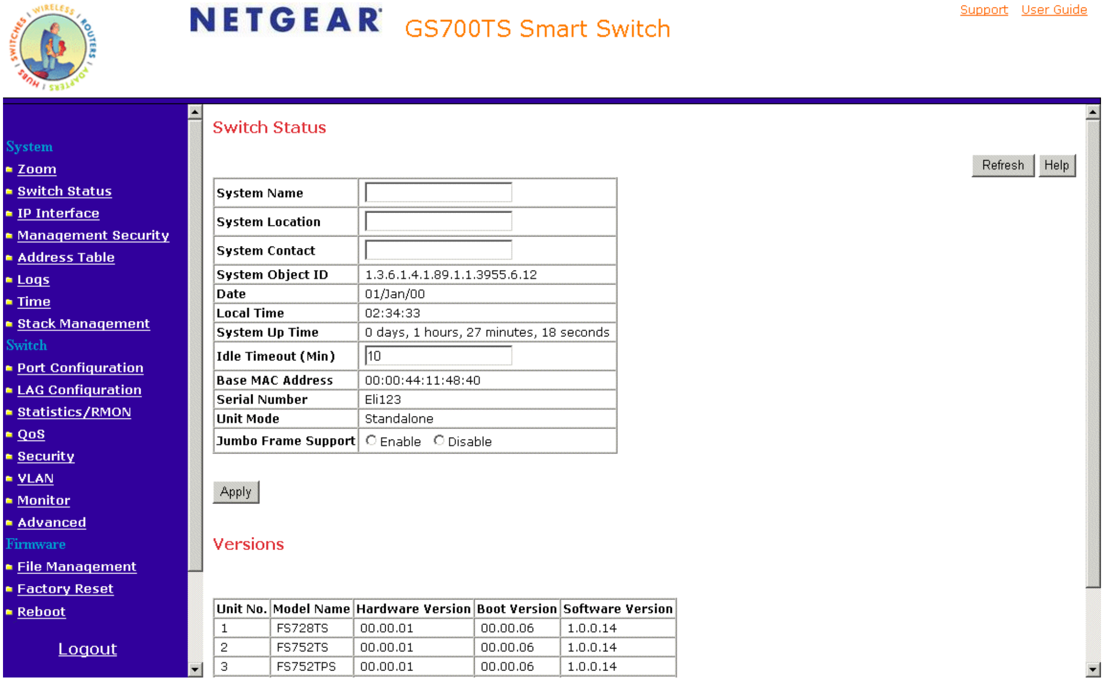
Figure 5-18

Viewing the Device Information

The *Switch Status Page* contains parameters for configuring general device information, including the system name, location, contact, the base MAC Address, System Object ID, and System Up Time, and both software and hardware versions.

To open the Switch Status Page:

1. Click **Switch Status**. The *Switch Status Page* opens.



Switch Status

System Name	
System Location	
System Contact	
System Object ID	1.3.6.1.4.1.89.1.1.3955.6.12
Date	01/Jan/00
Local Time	02:34:33
System Up Time	0 days, 1 hours, 27 minutes, 18 seconds
Idle Timeout (Min)	10
Base MAC Address	00:00:44:11:48:40
Serial Number	Eli123
Unit Mode	Standalone
Jumbo Frame Support	○ Enable ○ Disable

Versions

Unit No.	Model Name	Hardware Version	Boot Version	Software Version
1	FS728TS	00.00.01	00.00.06	1.0.0.14
2	FS752TS	00.00.01	00.00.06	1.0.0.14
3	FS752TPS	00.00.01	00.00.06	1.0.0.14

Figure 5-19

The *Switch Status Page* contains the following fields:

- **System Name** – Defines the user-defined device name. The field may contain 0-160 characters.
- **System Location** – Defines the location where the system is currently running. The field may contain 0-160 characters.
- **System Contact** – Defines the name of the contact person. The field may contain 0-160 characters.
- **System Object ID** – Displays the vendor’s authoritative identification of the network management subsystem contained in the entity.
- **Date** – Displays the current date.
- **Local Time** – Displays the Local time.

- **System Up Time** – Displays the amount of time since the most recent device reset. The system time is displayed in the following format: Days, Hours, Minutes, and Seconds. For example, 41 days, 2 hours, 22 minutes and 15 seconds.
- **Idle Timeout (Min)** – Indicates the amount of time (minutes) that elapses before an idle station is timed out. Idle stations that are timed out must login to the system. The field range is 5 **-** 30 minutes. The field default value is 10 minutes.
- **Base MAC Address** – Displays the MAC address for each stacking unit.
- **Serial Number** – Displays the device serial number.
- **Unit Mode** – Indicates if the device is currently in stand-alone or stacking mode. By default, the device runs in stacking mode.
- **Jumbo Frame Support** – Enables Jumbo Frames on the device. Jumbo Frames enable the transportation of identical data in fewer frames. This ensures less overhead, lower processing time, and fewer interruptions. The possible field values are:
  - ***Enable*** – Switch will recognize and forward Jumbo Frames.
  - *Disable*– Switch will not recognize Jumbo Frames.

The *Switch Status Page Versions* section contains the following fields:

- **Unit No**. – Indicates the stacking member’s current number. Possible values are 1-6.
- **Model Name** – Displays the device model number and name.
- **Hardware Version** – Displays the installed device hardware version number.
- **Boot Version** – Displays the current boot version running on the device.
- **Software Version** – Displays the installed software version number.

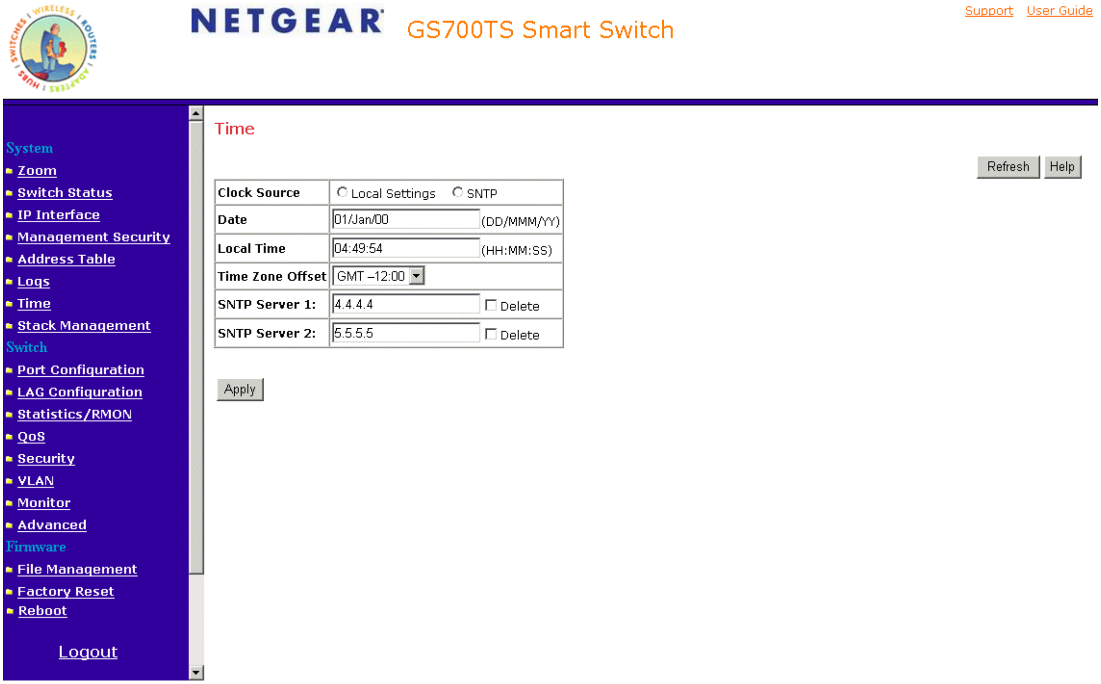
To make changes to the Device Information:

1. Define the relevant fields.

2. Click Apply.

Configuring System Time

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



Time

Clock Source	○ Local Settings ○ SNTP
Date	01/Jan/00 (DD/MMM/YY)
Local Time	04:49:54 (HH:MM:SS)
Time Zone Offset	GMT –12:00
SNTP Server 1:	4.4.4.4 □ Delete
SNTP Server 2:	5.5.5.5 □ Delete

Figure 5-20

The *Time Page* contains the following fields:

- **Clock Source** – The source used to set the system clock. The possible field values are:
  – *None* – Indicates that a clock source is not used. The clock is set locally.
  – *SNTP* – Indicates that the system time is set via an SNTP server.
- **Date** – The system date. The field format is Day/Month/Year. For example: 04/May/50 (May 4, 2050).
- **Local Time** – The system time. The field format is HH:MM:SS. For example: 21:15:03.
- **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.

- **SNTP Server 1** – Defines the Primary SNTP server IP address. The following option is available:
  - *Delete* – Removes the currently configured SNTP Server.
- **SNTP Server 2** – Defines the Secondary SNTP server IP address. The following option is available:
  - *Delete* – Removes the currently configured SNTP Server.

2. Define the relevant fields.
3. Click . The Time settings are saved, and the device is updated.

Managing Stacking

All stack members are accessed through a single IP address through which the stack is managed. Stacks are managed using:

- Web-based Interface
- SNMP Management Station

The system supports up to six stacking members per stack.

During the Stacking setup, one device is selected as the Stacking Master. All other devices are named as stack members, and assigned a unique Unit ID. The Stack Master provides a single point of control and management and a single interface in which to control and manage the stack. The device software is downloaded separately for each of the stack members. All units in the stack must be running the same software version. The Stacking Master maintains switch stacking and configuration. 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
- Removal of a Stacking Unit

Operation Modes

A switch can operate in one of the following modes:

- **Stacking Master** – Manages the stacking configuration for all stack members.
- **Secondary Master** – Operates as a backup to the Stacking Master. If the Stacking Master is no longer operating, the Secondary Master takes over the stack management.

- **Stacking Member**–Indicates a device within the stacking topology. The stacking member receives its device configuration from the Stacking Master.
  When creating stacks, ensure the same connection cable types are used throughout the stack, for example, use either all fiber cables or all copper cables.

This section provides an introduction to the user interface and includes the following topics:

- Understanding Stack Topology
- Stacking Ring Topology
- Stacking Members and Unit ID
- Removing and Replacing Stacking Members
- Inserting a Stacking Member
- Exchanging Stacking Members
- Switching the Stacking Master
- Configuring Stacking

Understanding Stack Topology

Stacked devices operate in a Ring or chain topology. The Ring topology connects all stacked devices in 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 by which to send traffic. A chain topology connects stacking members from one to the next. This provides a single data path flow. The stacking members linked in the middle of the chain are connection to the stacking member on either side of them. The members on the ends of the chain only have one connection.

Stacking Ring Topology

One of the benefits of the Ring topology is that it offers redundancy in case the connections between two units fail, including the case where a unit in the stack fails. If a failure occurs in the stacking topology, the stack reverts to Chain Stacking Topology. In the Chain topology, devices operate in a chain formation. 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 return to the Ring topology.

After the stacking issues are resolved, the device can be reconnected to the stack without interruption and the Ring topology is restored.

Stacking Members and Unit ID

Stacking Unit IDs are essential to the stacking configuration. The stacking operation is determined during the boot process. The Unit ID selected during the initialization process determines the Operation Mode.

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 Master unit boots or when inserting or removing a stack member, the Master unit 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.

Removing and Replacing Stacking Members

Stacking member 1 and stacking member 2 are Stacking Master enabled units. Unit IDs 1 and 2 are either designated as Master Unit or Secondary Master Unit. The Stacking Master assignment is performed during the configuration process. One Master enabled stack member is elected Master, and the other Master enabled stack member is elected Secondary Master, according to the following decision process:

- If only one Stacking Master enabled unit is present, this is the stacking Master.
- If two Stacking Master enabled stacking members are present, and one has been manually configured as the Stacking Master, this is the 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 joined the stack within the same ten minute interval. For example, 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 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 failure 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 Stacking 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 is part of both the configuration commands and the configuration files. Configuration files are managed only from the device Stacking Master. This includes:

- 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, the unit does not boot. For example, if a stack member (unit IDs 3 - 6) is separated from the stack due to a topology failure, the stacking member is no longer connected to the stack. The device can be booted, but it cannot be managed through the Stacking Master. The network manager can either reset the device defaults, or correct the topology failure, and reconnect the unit to the stack.

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

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 that are physically present are displayed in the GS700TS web pages, and can be configured through the web management system. By default, Unit IDs are assigned automatically. However, you can use the browser to assign a specific Unit ID; for example, the same unit ID as the unit which was recently removed.

Inserting a Stacking Member

When a stacking member is inserted into a running stack, it is automatically assigned a unit number. Note that a unit should not be powered up until it has been connected to the stack. If the user has already configured a Unit ID for the newly joined unit, a new Unit ID is not assigned. Note that all stack members must run the same version of firmware.

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 than or less ports than the previous device, the relevant port configuration is applied to the new stack member.

Switching the Stacking Master

The Secondary Master replaces the Stacking Master if one of 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.

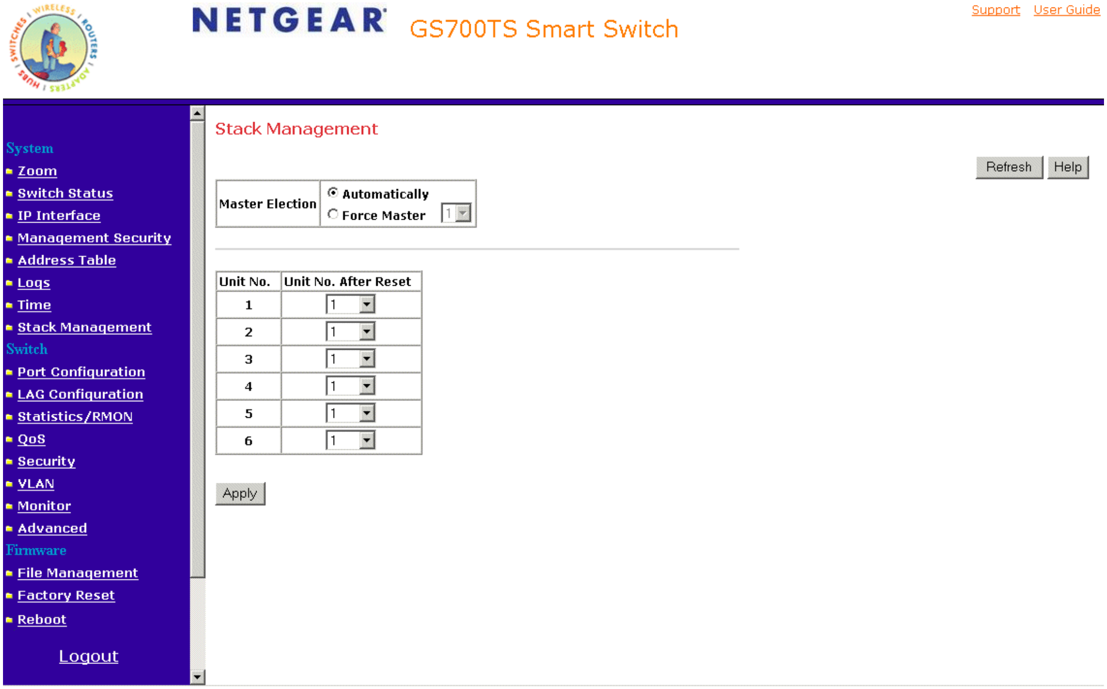
Switching between the Stacking Master and the Secondary Master results in a limited service loss. Any dynamic tables are relearned if a failure occurs. The running configuration file is synchronized between Stacking Master and the Secondary Master and continues running on the Secondary Master.

Configuring Stacking

The *Stack Management Page* 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. A unique Unit ID (1-6) identifies a stack member. This unit number determines the interface-level configuration that the stack member uses. (The configuration is saved and managed by the master unit.). The stack management default sets the stacking numbering method to auto-numbering.

To open the *Stack Management Page*:

1. Click **Stack Management**. The *Stack Management Page* opens.



Stack Management

Master Election	● Automatically ○ Force Master 1

Unit No.	Unit No. After Reset
1	1
2	1
3	1
4	1
5	1
6	1

Figure 5-21

The Stack Management Page contains the following fields:

- **Master Election** – When the stack is powered up and completes the boot-up process, the Master unit is elected within 0.5 seconds. The possible field values are:
  - *Automatically* – The master is selected automatically by software.
  - *Force Master* – Enables forcing the selection of a Stack Master.
- **Unit No**. – Indicates the stacking member’s current number. Possible values are 1-6.
- **Unit No. After Reset** – Indicates the stacking member’s future number after the stack is reset. Possible values are 1-6 or auto (automatically selected).

Switching Between Stack Masters

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 web interface.

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 Stacking Master and the Secondary Master, and continues running on the Secondary Master.

To switch between stack masters:

1. Open the Stack Management Page.

2. Select the *Force Master* radio button.

3. Select “2” from the drop-down list which enables switching the stack control to the Secondary Stack Master.

4. Click Apply. A confirmation message is displayed.

Configuring Device Security

This section contains information for managing both storm control and port security and includes the following topics:

- Defining Port Authentication Properties
- Viewing EAP Statistics
- Enabling Storm Control
- ACL Overview
- Defining MAC Based Access Control Lists
- Defining RADIUS Settings
- Defining RADIUS Settings
- Defining RADIUS Settings
- Defining TACACS+ Authentication

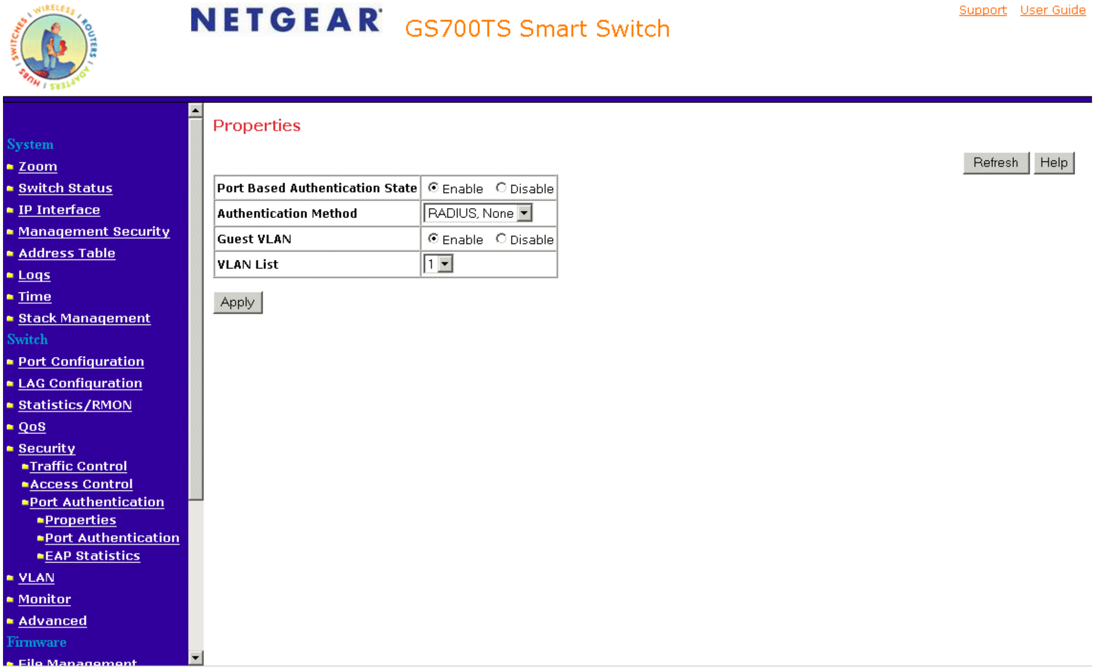
Defining Port Authentication Properties

The *Port Authentication Properties Page* allows network managers to configure network authentication parameters. In addition, Guest VLANs are enabled from the Properties Page. This section includes the following sections:

- Defining Port Authentication
- Viewing EAP Statistics (Extensible Authentication Protocol)

To define the port authentication properties:

1. Click **Security** > **Port Authentication** > **Properties**. The *Port Authentication Properties Page* opens.



Properties

Port Based Authentication State	● Enable ○ Disable
Authentication Method	RADIUS, None
Guest VLAN	● Enable ○ Disable
VLAN List	1

Figure 5-22

The *Port Authentication Properties Page* contains the following fields:

- **Port Based Authentication State** – Indicates if Port Authentication is enabled on the device. The possible field values are:
  – *Enable* – Enables port-based authentication on the device.

  - *Disable* – Disables port-based authentication on the device.
- **Authentication Method** – Specifies the authentication method used for port authentication. The possible field values are:
  - *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.
  - *RADIUS* – Provides port authentication using the RADIUS server.
  - *None* – Indicates that no authentication method is used to authenticate the port.
- **Guest VLAN** – Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
  - *Enable* – Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the VLAN List field.
  - *Disable* – Disables port-based authentication on the device. This is the default.
- **VLAN List** – Contains a list of VLANs. The Guest VLAN is selected from the VLAN list.

2. Define the relevant fields.

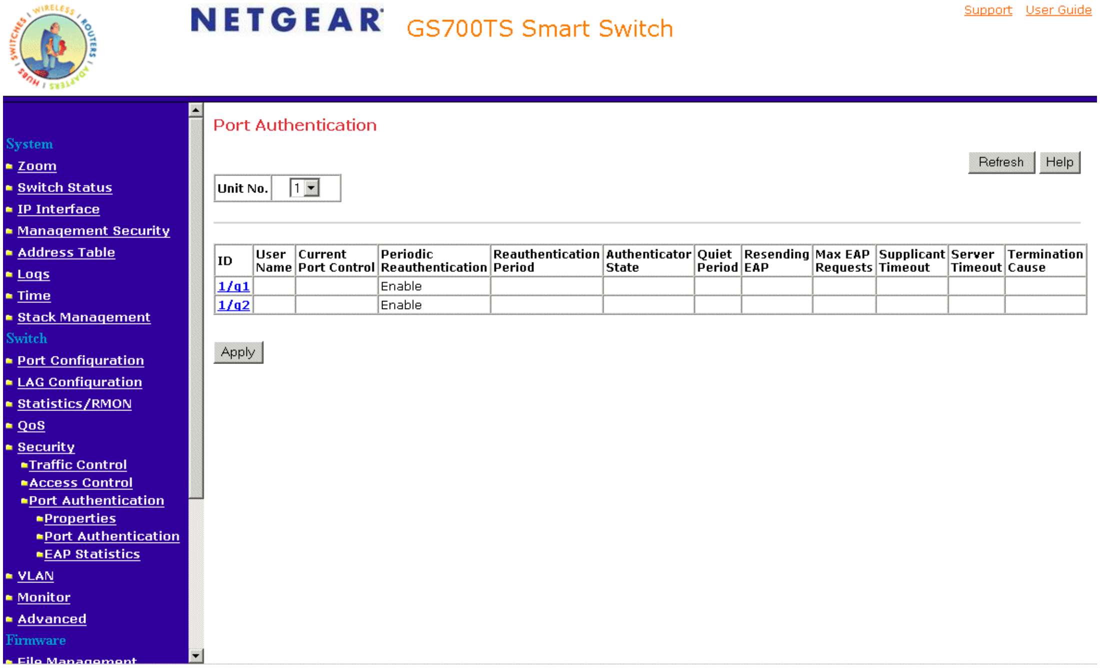
3. Click Apply. The network authentication properties are set and the device is updated.

Defining Port Authentication

The *Port Authentication Page* allows network managers to configure port-based authentication global parameters.

To define the port-based authentication global properties:

1. Click **Security** > **Port Authentication** > **Port Authentication**. The *Port Authentication Page* opens.



Port Authentication

Unit No. 1

ID	User Name	Current Port Control	Periodic Reauthentication	Reauthentication Period	Authenticator State	Quiet Period	Resending EAP	Max EAP Requests	Supplicant Timeout	Server Timeout	Termination Cause
1/g1			Enable								
1/g2			Enable								

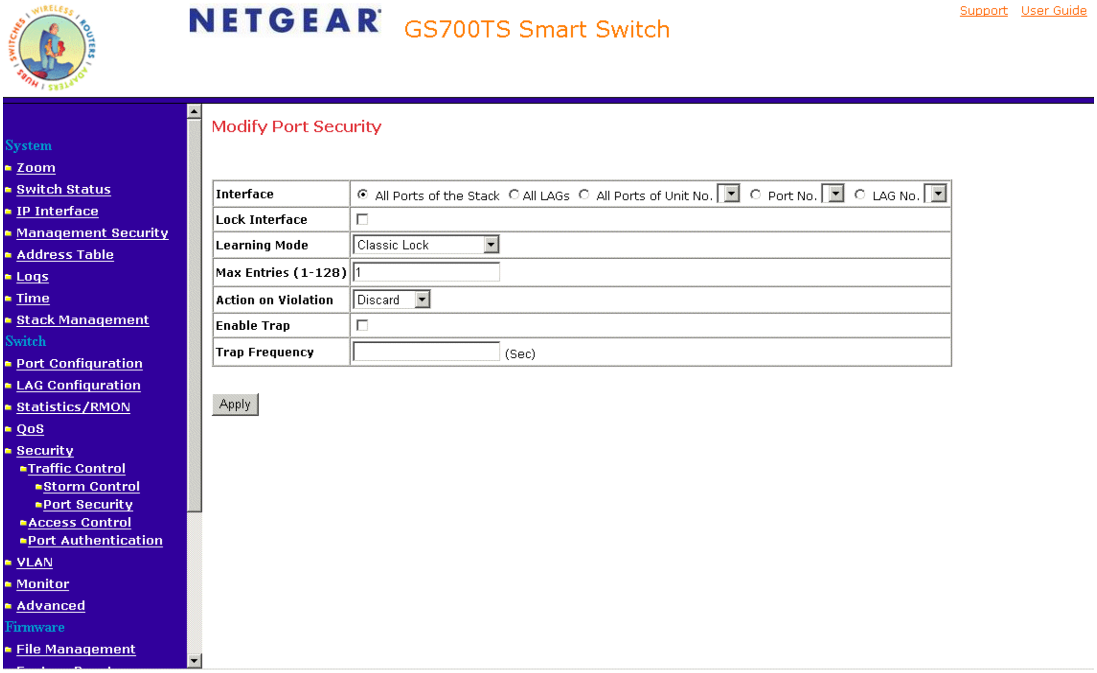
Figure 5-23

The *Port Authentication Page* contains the following fields:

- **Unit No.** – Indicates the stacking number.
- **ID** – Displays a list of interfaces on which port-based authentication is enabled.
- **User Name** – Displays the supplicant user name.
- **Current Port Control** – Displays the current port authorization state.
- **Periodic Reauthentication** – Permits immediate port reauthentication. The possible field values are:
  – *Enable* – Enables immediate 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.
- **Authenticator State** – Displays the current authenticator state.
- **Quiet Period** – Displays the number of seconds that the device remains in the quiet state following a failed authentication exchanges. 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 2 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 an ID. The Modify Port Security Page opens:



Modify Port Security

Interface	● All Ports of the Stack ○ All LAGs ○ All Ports of Unit No. ○ Port No. ○ LAG No.
Lock Interface	□
Learning Mode	Classic Lock
Max Entries (1-128)	1
Action on Violation	Discard
Enable Trap	□
Trap Frequency	(Sec)

Figure 5-24

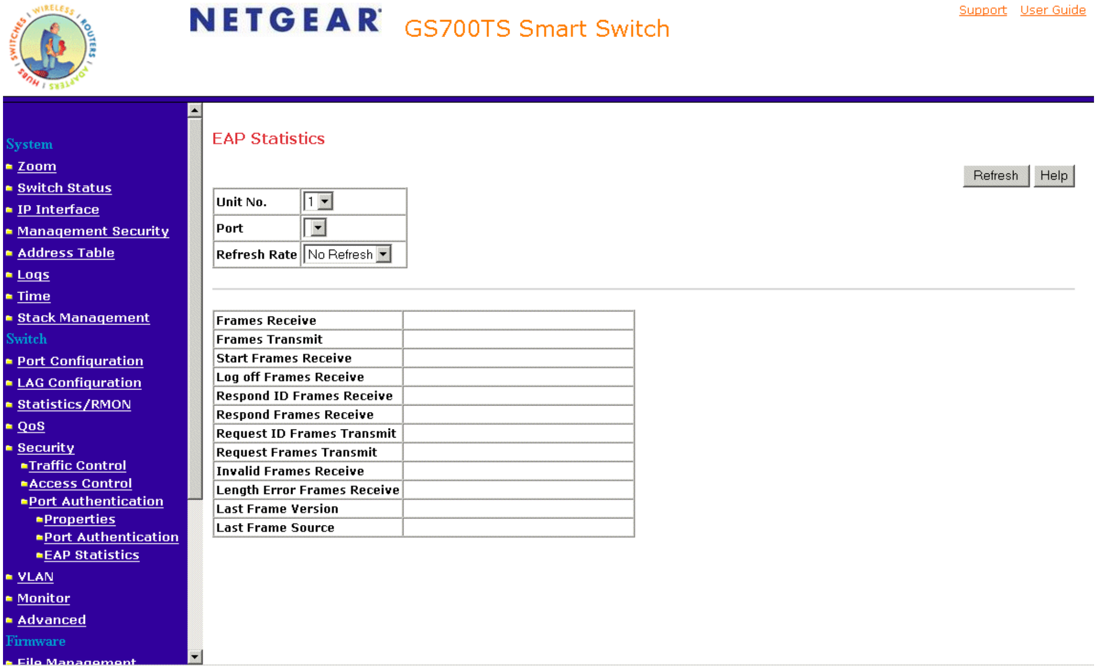
3. Modify the relevant fields.
4. Click Apply. The port authentication settings are defined and the device is updated.

Viewing EAP Statistics

The *EAP Statistics Page* contains information about EAP packets received on a specific port.

To view the EAP Statistics:

1. Click **Security** > **Port Authentication** > **EAP Statistics**. The *EAP Statistics Page* opens:



EAP Statistics

Unit No.	1
Port	
Refresh Rate	No Refresh

Frames Receive	
Frames Transmit	
Start Frames Receive	
Log off Frames Receive	
Respond ID Frames Receive	
Respond Frames Receive	
Request ID Frames Transmit	
Request Frames Transmit	
Invalid Frames Receive	
Length Error Frames Receive	
Last Frame Version	
Last Frame Source	

Figure 5-25

The *EAP Statistics Page* contains the following fields:

- **Unit No.** – Indicates the stacking number.
- **Port** – Indicates the port, which is polled for statistics.
- **Refresh Rate** – Indicates the amount of time that passes before the EAP statistics are refreshed. The possible field values are:
  - *No Refresh* – Indicates that the EAP statistics are not refreshed.
  - *15 Seconds*– Indicates that the EAP statistics are refreshed every 15 seconds.
  - *30 Seconds*– Indicates that the EAP statistics are refreshed every 30 seconds.
  - *60 Seconds* – Indicates that the EAP statistics are refreshed every 60 seconds.
- **Frames Receive** – Indicates the number of valid EAPOL frames received on the port.
- **Frames Transmit** – Indicates the number of EAPOL frames transmitted via the port.

- **Start Frames Receive** – Indicates the number of EAPOL Start frames received on the port.
- **Log off Frames Receive** – Indicates the number of EAPOL Logoff frames that have been received on the port.
- **Respond ID Frames Receive** – Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Respond Frames Receive** – Indicates the number of valid EAP Response frames received on the port.
- **Request ID Frames Transmit** – Indicates the number of EAP Req/Id frames transmitted via the port.
- **Request Frames Transmit** – Indicates the number of EAP Request frames transmitted via the port.
- **Invalid Frames Receive** – Indicates the number of unrecognized EAPOL frames that have been received via the port.
- **Length Error Frames Receive** – Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Last Frame Version** – Indicates the protocol version number attached to the most recently received EAPOL frame.
- **Last Frame Source** – Indicates the source MAC address attached to the most recently received EAPOL frame.

Enabling Storm Control

Storm Control limits the amount of 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.

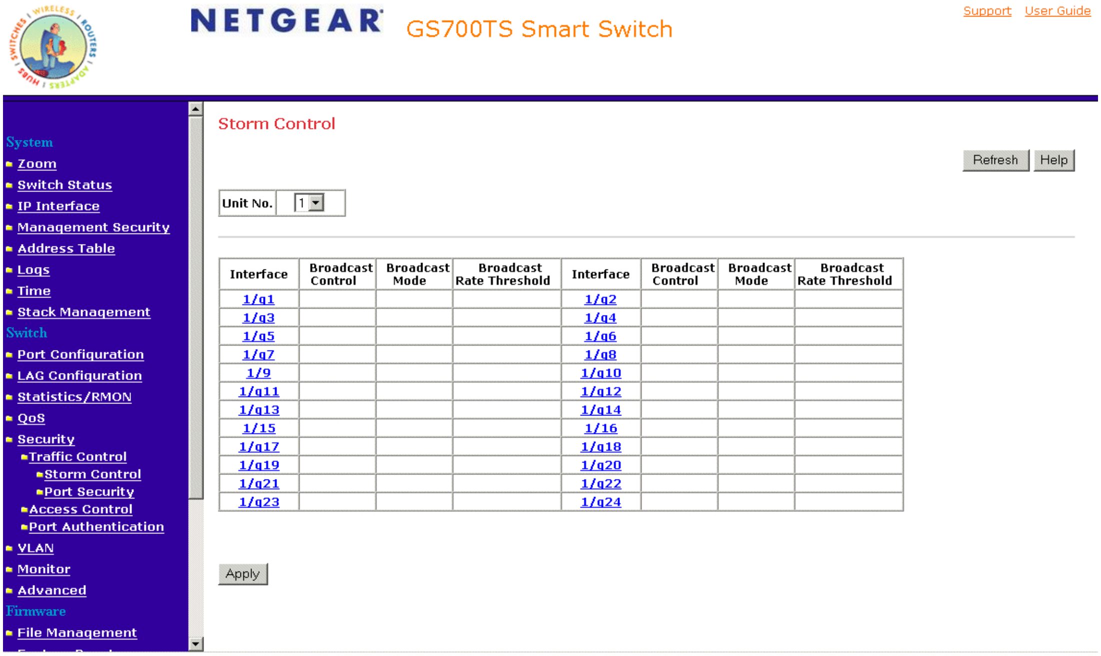
A Broadcast Storm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

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. By default, Storm Control is enabled on all ports - broadcast only - with threshold of 200 kbps. Storm Control is enabled by default.

The *Storm Control Page* provides fields for configuring broadcast Storm Control.

To enable storm control:

1. Click **Security** > **Traffic Control** > **Storm Control**. The *Storm Control Page* opens.



Storm Control

Unit No. 1

Interface	Broadcast Control	Broadcast Mode	Broadcast Rate Threshold	Interface	Broadcast Control	Broadcast Mode	Broadcast Rate Threshold
1/g1				1/g2			
1/g3				1/g4			
1/g5				1/g6			
1/g7				1/g8			
1/9				1/g10			
1/g11				1/g12			
1/g13				1/g14			
1/15				1/16			
1/g17				1/g18			
1/g19				1/g20			
1/g21				1/g22			
1/g23				1/g24			

Figure 5-26

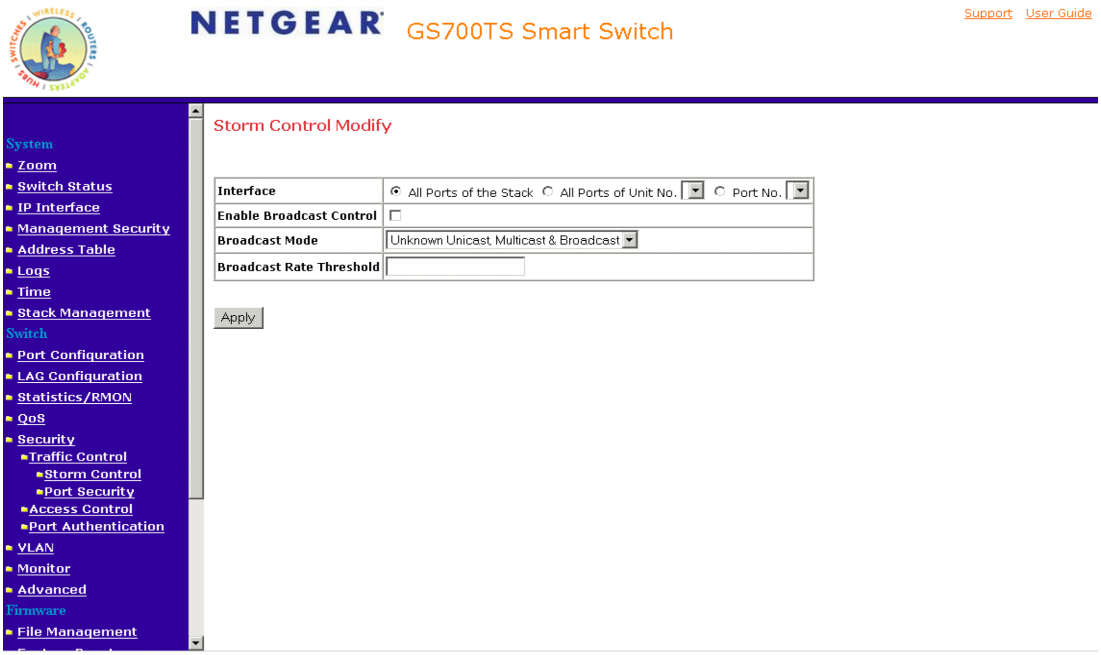
The *Storm Control Page* contains the following fields:

- **Unit No.** – Indicates the stacking number for which the Storm Control statistics are displayed.
- **Interface** – Displays the port number for which the Storm Control information is displayed.
- **Broadcast Control** – Indicates if forwarding broadcast packet types is enabled on the interface for which the Storm Control information is displayed. The possible field values are:
  - *Enable* – Enables Storm Control on all broadcast only ports with threshold of 200 kbps. Enabled is the default.
  - *Disable* – Disables Storm Control on the interface.
- **Broadcast Mode** – Specifies the broadcast mode currently enabled on the device. The possible field values are:

- *Unknown Unicast, Multicast & Broadcast* – Counts Unicast, Multicast, and Broadcast traffic.
- *Multicast & Broadcast* – Counts Broadcast and Multicast traffic together.
- *Broadcast Only* – Counts only Broadcast traffic.

- **Broadcast Rate Threshold** – Indicates the maximum rate (kilobits per second) at which unknown packets are forwarded. The range is 3500 - 250,000 kbps. The default value is 200 kbps.

2. Click an interface. The *Storm Control Modify Page* opens:



Storm Control Modify

Interface	● All Ports of the Stack ○ All Ports of Unit No. ○ Port No.
Enable Broadcast Control	□
Broadcast Mode	Unknown Unicast, Multicast & Broadcast
Broadcast Rate Threshold	

Apply

Figure 5-27

In addition to the *Storm Control Page*, The *Storm Control Modify Page* contains the following field:

- **Interface** – Displays the port number for which the storm control information is displayed. The possible field values are:
  - *All Ports of the Stack* – Indicates the ports of the stack from which storm control is enabled.

   - *All Ports of Unit No.* – Indicates the ports of the unit from which storm control is enabled.
   - *Port No.* – Indicates the port number.

3. Modify the relevant fields.
4. Click Apply. Storm control is enabled on the device.

ACL Overview

Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Packets entering an ingress port, with an active ACL, are either admitted or denied entry and the ingress port is disabled. If they are denied entry, the user can disable the port.

To implement ACLs, first define the ACL to specify what actions should be taken when packets are received and then specify which ports should follow these actions by binding the ACL to them.

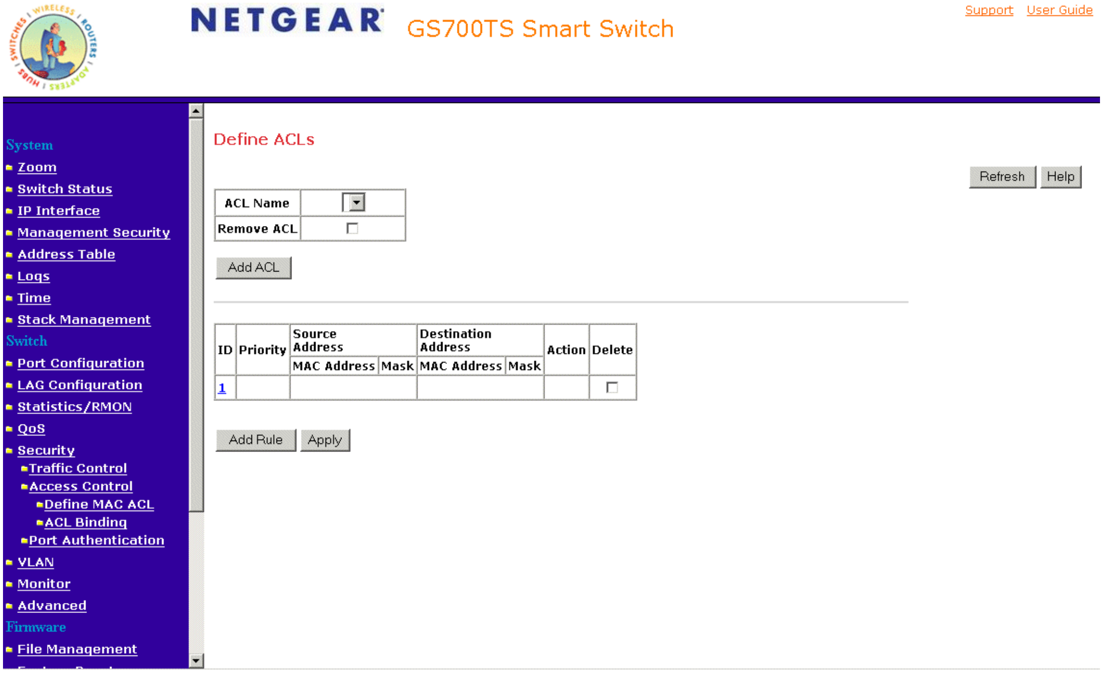
Defining MAC Based Access Control Lists

Access Control Lists are made up of a list of Access Control Elements. An Access Control Element specifies an action to apply when a packet is received from a specific MAC address or range of MAC addresses.

The *MAC Based ACL Page* page allows a MAC-based ACL to be defined. ACEs can be added only if the ACL is not bound to an interface.

To define MAC Based ACLs:

1. **Click Security** > **Access Control** > **Define MAC ACL**. The *MAC Based ACL Page* opens:



Define ACLs

ACL Name	
Remove ACL	□

ID	Priority	Source Address		Destination Address		Action	Delete
		MAC Address	Mask	MAC Address	Mask		
1							□

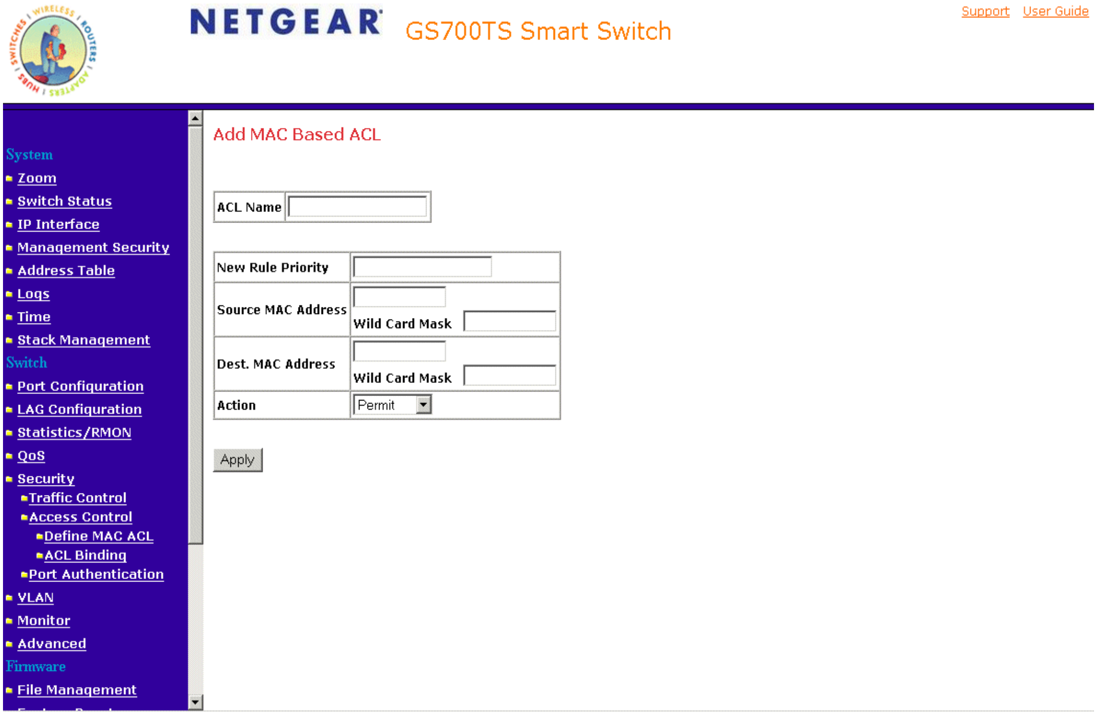
Figure 5-28

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

- **ACL Name** – Displays the user-defined MAC based ACLs.
- **Remove ACL** – Removes the ACLs. The possible field values are:
  - *Checked* – Removes the selected MAC based ACL.
  - *Unchecked* – Maintains the MAC based ACLs.
- **ID** – Matches the packet’s VLAN ID to the ACE. The possible field values are 1 to 4095.
- **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 Address**
  - **MAC Address** – Matches the source MAC address to which packets are addressed to the ACE.

  - **Mask** – Indicates the source MAC Address wild card mask. Wildcards are used to mask all or part of a source IP Address. Wild card masks specify which bits are used and which bits are ignored. A wild card mask of ff: ff:ff:ff:ff:ff indicates that no bit is important. A wildcard of 00.00.00.00.00.00 indicates that all the bits are important. For example, if the source IP address 14.36.18.19.1.1 and the wildcard mask is 255.36.184.00.00.00, the middle two bits of the IP address are used, while the last three bits are ignored.
- **Destination Address**
  - **MAC Address** – Matches the destination MAC address to which packets are addressed to the ACE.
  - **Mask** – Indicates the destination MAC Address wild card mask. Wildcards are used to mask all or part of a destination IP Address. Wild card masks specify which bits are used and which bits are ignored. A wild card mask of ff: ff:ff:ff:ff:ff indicates that no bit is important. A wildcard of 00.00.00.00.00.00 indicates that all the bits are important. For example, if the source IP address 14.36.18.19.1.1 and the wildcard mask is 255.36.184.00.00.00, the middle two bits of the IP address are used, while the last three bits are ignored.
- **Action** – Indicates the ACL forwarding action. The 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.
- **Delete** – Deletes the rule from the ACL. The possible field values are:
  - *Checked* – Deletes the rule from the ACL.
  - *Unchecked* – Does not delete the rule from the ACL.

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



Add MAC Based ACL

ACL Name	

New Rule Priority		
Source MAC Address		Wild Card Mask
Dest. MAC Address		Wild Card Mask
Action	Permit	

Figure 5-29

3. Define the relevant fields.

4. Click Apply. The MAC based ACL is defined, and the device is updated.

5. To add a rule, click Add Rule. The Add MAC Based ACL page opens.

The *Add MAC Based Rule* page contains the following fields:

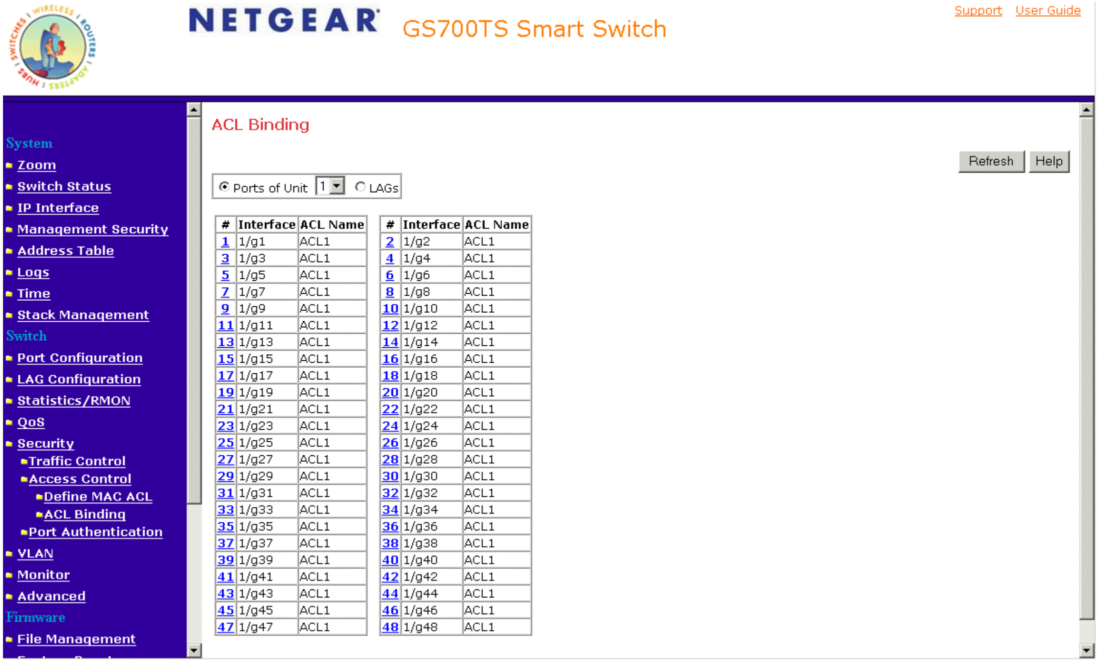
- **ACL Name** – Displays the user-defined MAC based ACLs.
- **New Rule Priority** – Indicates the rule priority, which determines which rule is matched to a packet on a firstmatch basis.
- Source MAC Address – Matches the source MAC IP address to which packets are addressed to the ACE.
- **Action** – 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 screen.

Defining Access Control Lists Binding

To define ACL Binding:

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



ACL Binding

● Ports of Unit 1 ○ LAGs

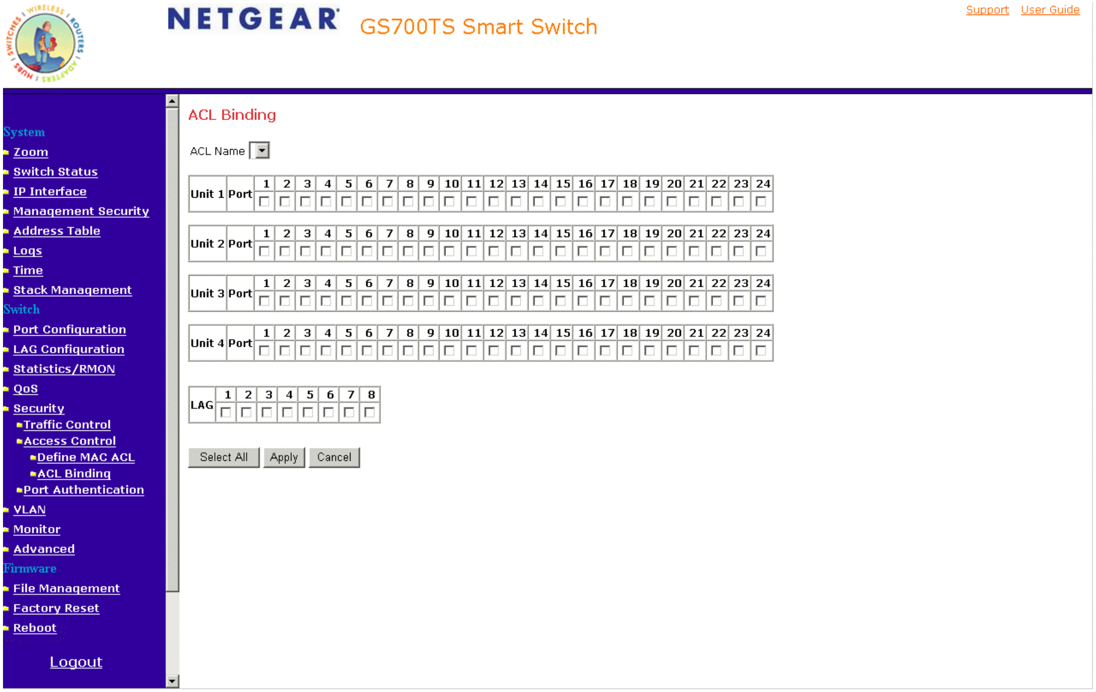
#	Interface	ACL Name	#	Interface	ACL Name
1	1/g1	ACL1	2	1/g2	ACL1
3	1/g3	ACL1	4	1/g4	ACL1
5	1/g5	ACL1	6	1/g6	ACL1
7	1/g7	ACL1	8	1/g8	ACL1
9	1/g9	ACL1	10	1/g10	ACL1
11	1/g11	ACL1	12	1/g12	ACL1
13	1/g13	ACL1	14	1/g14	ACL1
15	1/g15	ACL1	16	1/g16	ACL1
17	1/g17	ACL1	18	1/g18	ACL1
19	1/g19	ACL1	20	1/g20	ACL1
21	1/g21	ACL1	22	1/g22	ACL1
23	1/g23	ACL1	24	1/g24	ACL1
25	1/g25	ACL1	26	1/g26	ACL1
27	1/g27	ACL1	28	1/g28	ACL1
29	1/g29	ACL1	30	1/g30	ACL1
31	1/g31	ACL1	32	1/g32	ACL1
33	1/g33	ACL1	34	1/g34	ACL1
35	1/g35	ACL1	36	1/g36	ACL1
37	1/g37	ACL1	38	1/g38	ACL1
39	1/g39	ACL1	40	1/g40	ACL1
41	1/g41	ACL1	42	1/g42	ACL1
43	1/g43	ACL1	44	1/g44	ACL1
45	1/g45	ACL1	46	1/g46	ACL1
47	1/g47	ACL1	48	1/g48	ACL1

Figure 5-30

The *ACL Binding Page* contains the following fields:

- **Ports of Unit** – Indicates the unit number for which the ports are displayed.
- **LAGs** – Indicates that LAGs are being displayed.
- **Interface** – Displays the interface for which the ACL parameters are defined.
- **ACL Name** – Contains a list of the MAC based ACLs, which is bound to the interface.

2. Click on an **Interface No.** to define ACL Binding. The *Modify ACL Binding Page* opens:



ACL Binding

ACL Name

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1 Port	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 2 Port	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 3 Port	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 4 Port	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

	1	2	3	4	5	6	7	8
LAG	□	□	□	□	□	□	□	□

Figure 5-31

The *Modify ACL Binding Page* contains the following fields:

- **ACL Name** – Contains a list of the MAC-based ACLs, which is bound to the interface.
- **Unit No**.– Indicates the unit number for which the ports are displayed.
- **Port** – Indicates the port for which the ports are displayed.

3. Select the *ACL Name* and ports to be bound.
4. Click **Apply**. The ACL Binding is defined, and the device is updated.

Port-based 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. It provides the following options for unauthorized packets arriving at a locked port:

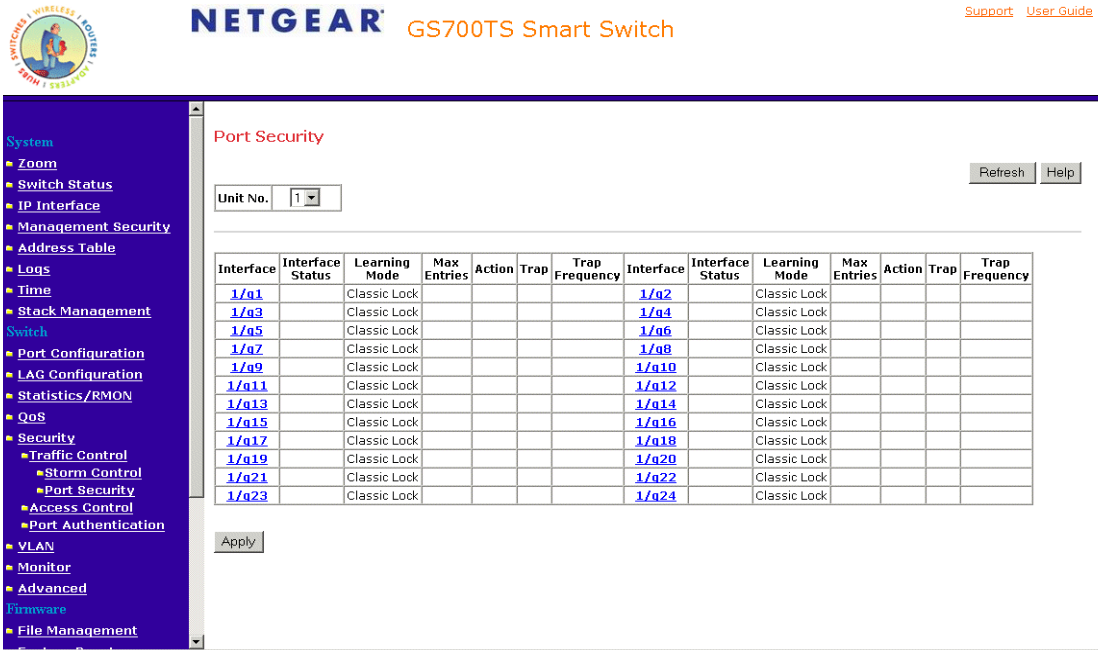
- Forwarded
- Discarded with no trap
- Discarded with a trap
- Shuts down the port

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.

To define port security:

1. Click **Security** > **Traffic Control** > **Port Security**. The *Port Security Page* opens.



Port Security

Unit No. 1

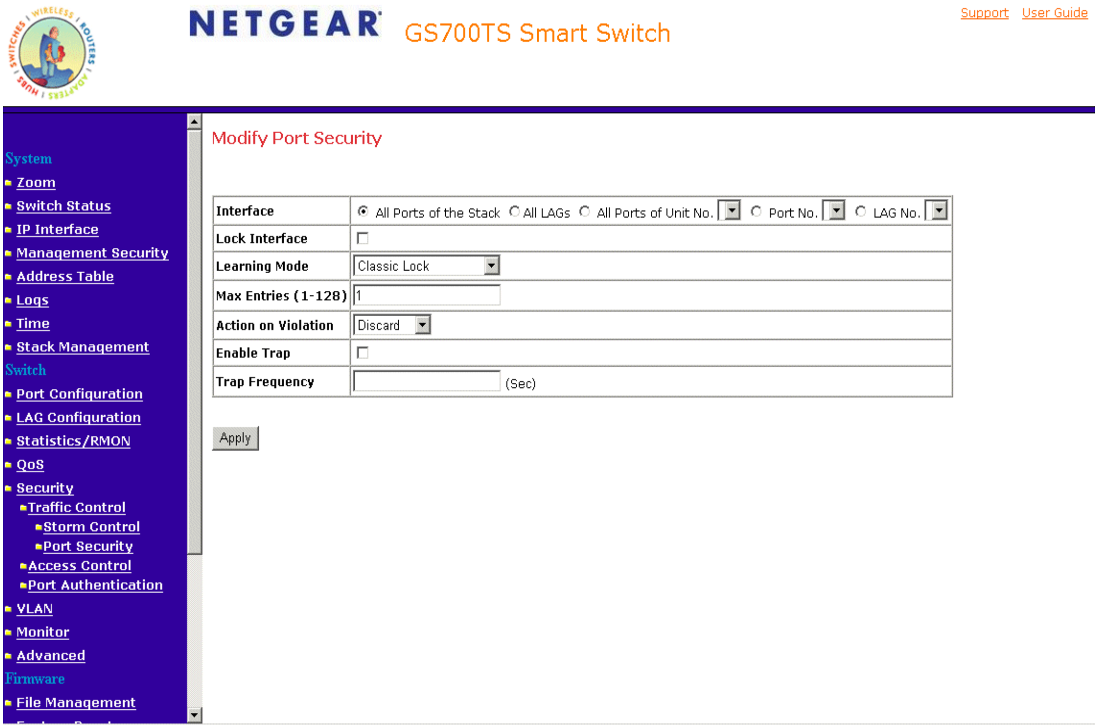
Interface	Interface Status	Learning Mode	Max Entries	Action	Trap	Trap Frequency	Interface	Interface Status	Learning Mode	Max Entries	Action	Trap	Trap Frequency
1/g1		Classic Lock					1/g2		Classic Lock				
1/g3		Classic Lock					1/g4		Classic Lock				
1/g5		Classic Lock					1/g6		Classic Lock				
1/g7		Classic Lock					1/g8		Classic Lock				
1/g9		Classic Lock					1/g10		Classic Lock				
1/g11		Classic Lock					1/g12		Classic Lock				
1/g13		Classic Lock					1/g14		Classic Lock				
1/g15		Classic Lock					1/g16		Classic Lock				
1/g17		Classic Lock					1/g18		Classic Lock				
1/g19		Classic Lock					1/g20		Classic Lock				
1/g21		Classic Lock					1/g22		Classic Lock				
1/g23		Classic Lock					1/g24		Classic Lock				

Figure 5-32

The *Port Security Page* contains the following fields:

- **Unit No.** – Indicates the unit number.
- **Interface** – Displays the port or LAG name.
- **Interface Status** – Indicates the host status.
- **Learning Mode** – Defines the locked port type. The Learning Mode field is enabled only if Locked is selected in the Set Port field. The possible field values are:
  - *Classic Lock* – Locks the port, and only forwards packets that have been learned statically or dynamically, prior to locking the port. The lock is effective immediately.
  - *Limited Dynamic Lock* – Indicates the port is unlocked. Locks the port after a user-defined number of MAC addresses have been dynamically learned on the port. After the port is locked, packets are forwarded only from MAC addressees that have been learned prior to locking the port.
- **Max Entries** – Specifies the number of MAC address that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the Set Port field. In addition, the Limited Dynamic Lock mode is selected. The default is 1.
- **Action** – Indicates the action to be applied to packets arriving on a locked port. The possible field 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.
- **Trap** – Enables traps when a packet is received on a locked port. The possible field values are:
  - *Checked* – Enables traps.
  - *Unchecked* – Disables traps.
- **Trap Frequency (Sec)** – The amount of time (in seconds) between traps. The default value is 10 seconds.

2. Click an interface you want to modify. The *Modify Port Security Page* opens:



Modify Port Security

Interface	● All Ports of the Stack ○ All LAGs ○ All Ports of Unit No. ○ Port No. ○ LAG No.
Lock Interface	□
Learning Mode	Classic Lock
Max Entries (1-128)	1
Action on Violation	Discard
Enable Trap	□
Trap Frequency	(Sec)

Apply

Figure 5-33

In addition to the *Port Security Page*, The *Modify Port Security Page* contains the following fields:

- **Interface** – Displays the port or LAG name. The possible field values are:
  - *All Ports of the Stack* – Indicates the ports of the stack from which Storm Control is enabled.
  - *All LAGs* – Indicates the LAGs of the stack from which Storm Control is enabled.
  - *All Ports of Unit No.* – Indicates the ports of the unit from which Storm Control is enabled.
  - *Port No.* – Indicates the port number.
  - *LAG No.* – Indicates the LAG number.
- **Lock Interface** – Locks the selected interface. To make a change, the Lock Interface must be unchecked.

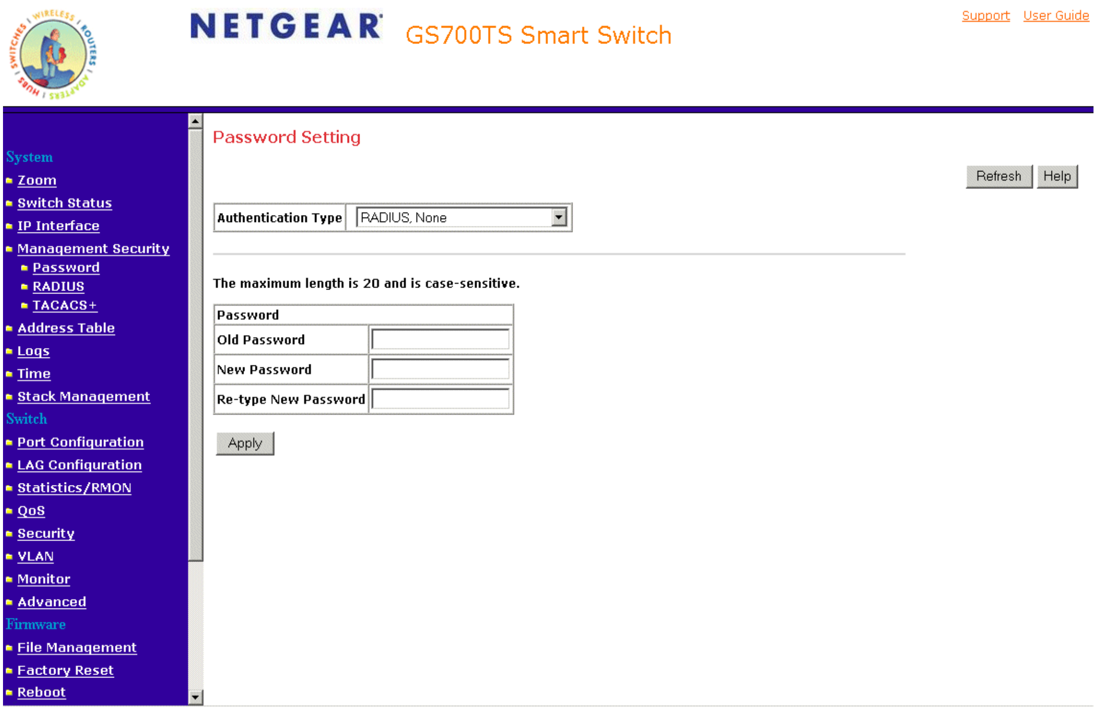
3. Modify the relevant fields.
4. Click Apply . The port security settings are defined and the device is updated.

Configuring Passwords

The *Password Settings Page* contains parameters for configuring device passwords.

To define device passwords:

1. Click **Management Security** > **Password**. The *Password Settings Page* opens:



Password Setting

Authentication Type	RADIUS, None

The maximum length is 20 and is case-sensitive.

Password	
Old Password	
New Password	
Re-type New Password	

Figure 5-34

The *Password Settings Page* contains the following fields:

- **Authentication Type** – Displays the authentication type used and the order by which authentication is performed. If the first authentication method is not available, the second one is used, until the full list is exhausted. For example, if "RADIUS, TACACS+, None" list is selected, the RADIUS server is used to authenticate a user. If the RADIUS server is unavailable, or there is no RADIUS server on the network, the TACACS+ server is used to authenticate a user. If the TACACS+ server is unavailable, or there is no TACACS+ server on the network, then the user logs in with no authentication. The possible field values are:
  - *Local* – Authentication occurs locally.
  - *RADIUS* – Authentication occurs at the RADIUS server.
  - *TACACS+* – Authentication occurs at the TACACS+ server.
  - *None* – No authentication type is applied.
- **Old Password** – Indicates the current password used to access the system.
- **New Password** – Defines a new password for accessing the system.
- **Re-type New Password** – Verifies the new password used to access the system. The maximum password length is 20 characters and is case-sensitive.

2. Define the relevant fields.

Authentication on this device uses only a password, not a username. Therefore, to configure RADIUS/TACACS+ authentication, the user name should be configured as $enab15$ on the RADIUS/TACACS+ server.

3. Click Apply. The password is defined and the device is updated.

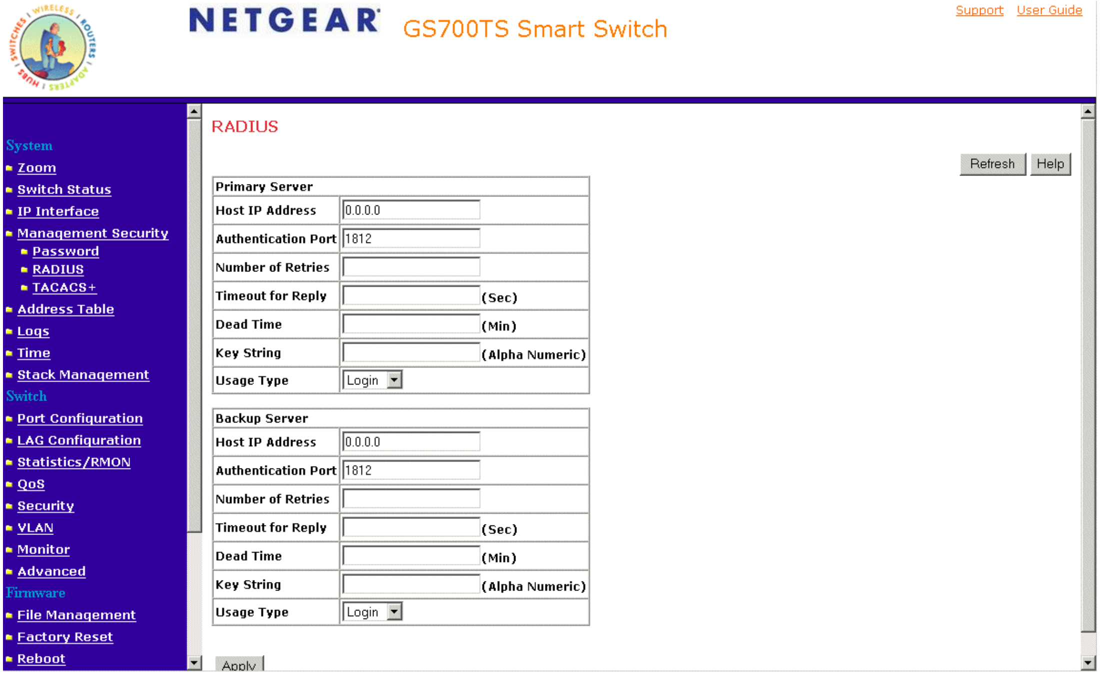
Defining RADIUS Settings

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

The default parameters are user-defined, and are applied to newly defined RADIUS servers. If new default parameters are not defined, the system default values are applied to newly defined RADIUS servers.

To configure RADIUS servers:

1. Click **Management Security > RADIUS**. The *RADIUS Page* opens:



RADIUS

Primary Server	
Host IP Address	0.0.0.0
Authentication Port	1812
Number of Retries	
Timeout for Reply	(Sec)
Dead Time	(Min)
Key String	(Alpha Numeric)
Usage Type	Login

Backup Server	
Host IP Address	0.0.0.0
Authentication Port	1812
Number of Retries	
Timeout for Reply	(Sec)
Dead Time	(Min)
Key String	(Alpha Numeric)
Usage Type	Login

Figure 5-35

The *RADIUS Page* contains the following fields:

- **Primary Server** – Defines the RADIUS Primary Server authentication fields.
- **Backup Server** – Defines the RADIUS Backup Server authentication fields.
- **Host IP Address** – Defines the RADIUS Server IP address.
- **Authentication Port** – Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **Number of Retries** – Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are 1-10. The default value is 3.
- **Timeout for Reply** – Defines the amount of time (in seconds) the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. Possible field values are 1-30. The default value is 3.

- **Dead Time** – Defines the default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default value is 0.
- **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.
- **Usage Type** – Specifies the RADIUS server authentication type. The default value is *Log in*. The possible field values are:
  - *Login* – 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 802.11X port authentication.

2. Define the relevant fields.
3. Click Apply. The RADIUS Servers are enabled, and the system is updated.

Defining TACACS+ Authentication

Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation. The system supports up-to 4 TACACS+ servers.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

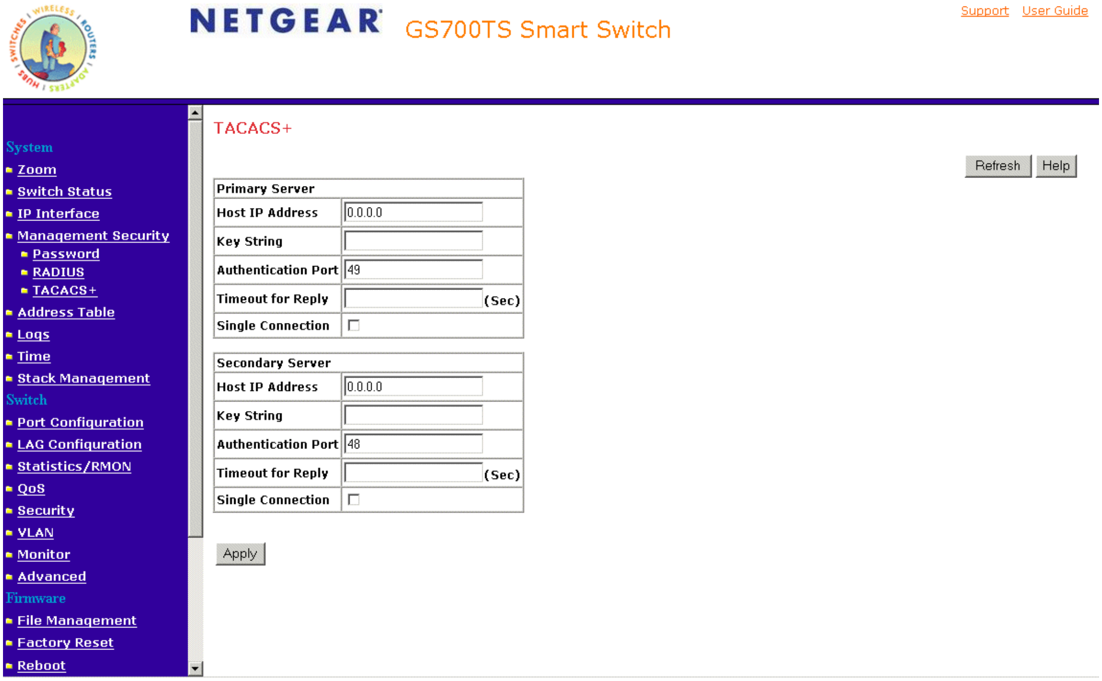
- **Authentication** – Provides authentication during login and via user names and user-defined passwords.
- **Authorization** – Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name.

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

The TACACS+ default parameters are user-assigned defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ new servers.

To define TACACS+ Settings:

1. Click **Management Security > TACACS+**. The *TACACS+ Page* opens:



TACACS+

Primary Server	
Host IP Address	0.0.0.0
Key String	
Authentication Port	49
Timeout for Reply	(Sec)
Single Connection	□

Secondary Server	
Host IP Address	0.0.0.0
Key String	
Authentication Port	48
Timeout for Reply	(Sec)
Single Connection	□

Figure 5-36

The *TACACS+ Page* contains the following fields:

- **Primary Server** – Defines the RADIUS Primary Server authentication fields.
- **Secondary Server** – Defines the RADIUS Backup Server authentication fields.
- **Host IP Address** – Defines the TACACS+ Server IP address.
- **Key String** – Defines the default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.
- **Authentication Port** – Defines the port number via which the TACACS+ session occurs. The default port is port 49 (Range: 0-65535).
- **Timeout for Reply** – Defines the default time that passes before the connection between the device and the TACACS+ times out.
- **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.

2. Define the relevant fields.
3. Click Apply. The TACACS+ Server is enabled, and the device is updated.

Viewing System Logs

Event messages have a unique format, as per the SYSLOG RFC recommended message format for all error reporting, for example, Syslog+ local device reporting. Messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. Messages are filtered based on their urgency or relevancy. The following table contains the Log Severity Levels:

Table 6: Severity Levels

Severity	Severity Level	Severity Level
Emergency	0	Indicates that the system is not functioning.
Alert	1	Indicates that the system needs immediate attention.
Critical	2	Indicates that the system is in a critical state.
Error	3	Indicates that a system error has occurred.
Warning	4	indicates that a system warning is logged.
Notice	5	Indicates that the system is functioning properly, but system notice is logged.
Informational	6	Provides device information.
Debug	7	Provides detailed log information.

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

This section includes the following topics:

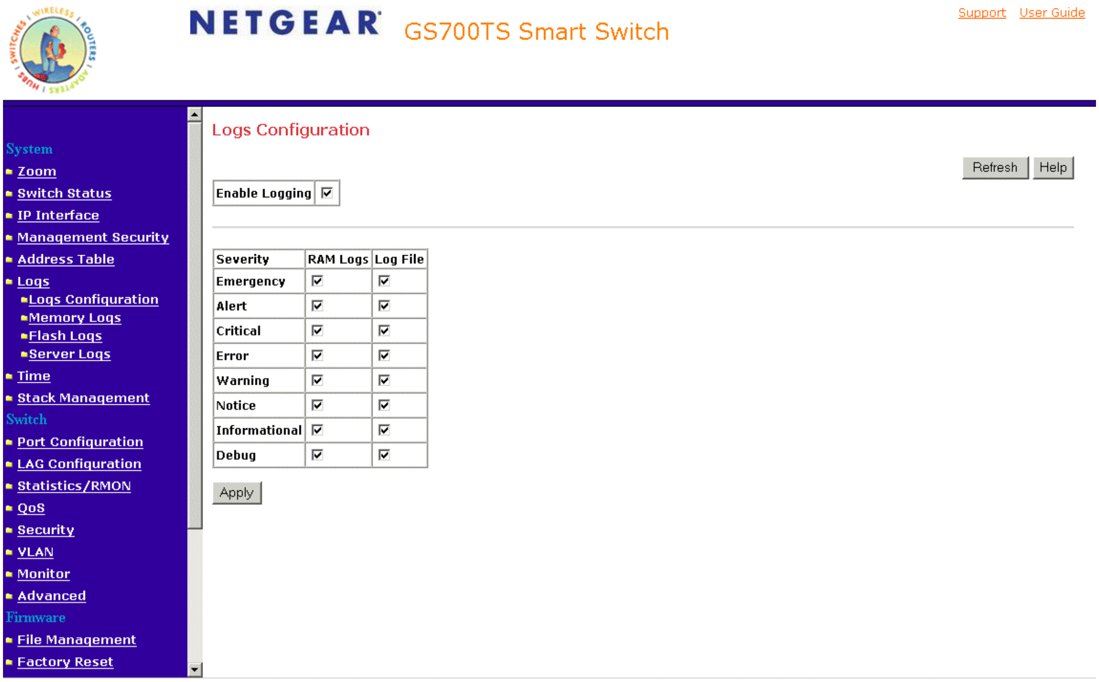
- Logs Configuration
- Viewing the Memory Logs
- Viewing Flash Logs
- Defining Server Logs

Logs Configuration

The Logs Configuration Page contains fields for defining which events are recorded to which logs. It contains fields for enabling logs globally, and parameters for defining logs. Log messages are listed from the highest severity to the lowest severity level. When a severity level is selected, all severity level choices above the selection are selected automatically.

To enable event logging:

1. Click **Logs > Logs Configuration**. The *Logs Configuration Page* opens.



Logs Configuration

Enable Logging ☑

Severity	RAM Logs	Log File
Emergency	☑	☑
Alert	☑	☑
Critical	☑	☑
Error	☑	☑
Warning	☑	☑
Notice	☑	☑
Informational	☑	☑
Debug	☑	☑

Figure 5-37

The *Logs Configuration Page* contains the following fields:

- **Enable Logging** – Indicates if device global logs for Cache, File, and Server Logs are enabled. Console logs are enabled by default. The possible field values are:
  – *Checked* – Enables device logs.
  – *Unchecked* – Disables device logs.
- **Severity** – The following are the available RAM Logs and Log File severity levels:

- – *Emergency* – The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
- – *Alert* – The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.
- – *Critical* – The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.
- – *Error* – A device error has occurred; for example, if a single port is offline.
- – *Warning* – The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- – *Notice* – Provides device information.
- – *Informational* – Provides device information.
- – *Debug* – Provides debugging messages.

- **RAM Logs** – Defines the minimum severity level from which logs are sent to the RAM Log kept in RAM (Cache).
- **Log File -** Defines the minimum severity level from which logs are sent to the log file kept in FLASH memory.

2. Define the relevant fields.

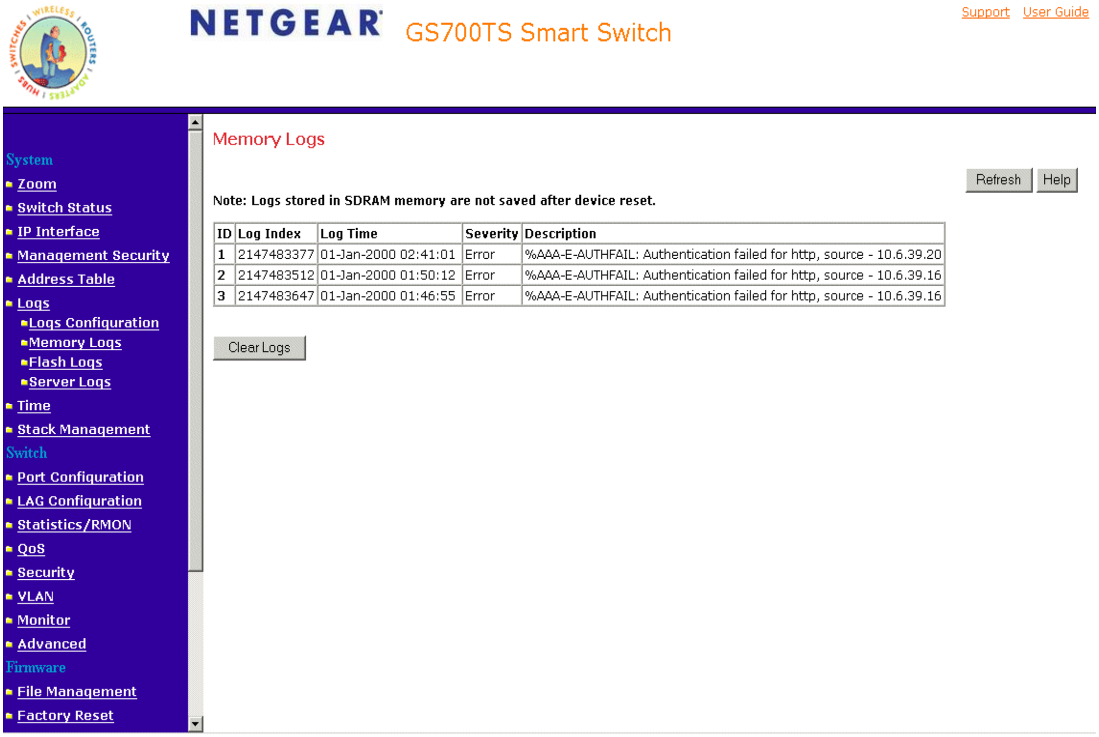
3. Click Apply. The log parameters are set and the device is updated.

Viewing the Memory Logs

The *Memory Logs Page* contains all system logs in a chronological order that are saved in RAM (Cache). Logs stored in SDRAM memory are not saved after device reset.

To open the *Memory Logs Page*:

1. Click **Logs** > **Memory Logs**. The *Memory Logs Page* opens:



Memory Logs

Note: Logs stored in SDRAM memory are not saved after device reset.

ID	Log Index	Log Time	Severity	Description
1	2147483377	01-Jan-2000 02:41:01	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 10.6.39.20
2	2147483512	01-Jan-2000 01:50:12	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 10.6.39.16
3	2147483647	01-Jan-2000 01:46:55	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 10.6.39.16

Figure 5-38

The *Memory Logs Page* contains the following fields:

- **ID** – Displays the table entry number.
- **Log Index** – Displays the log number.
- **Log Time** – Displays the time at which the log was generated.
- **Severity** – Displays the log severity.
- **Description** – Displays the log message text.

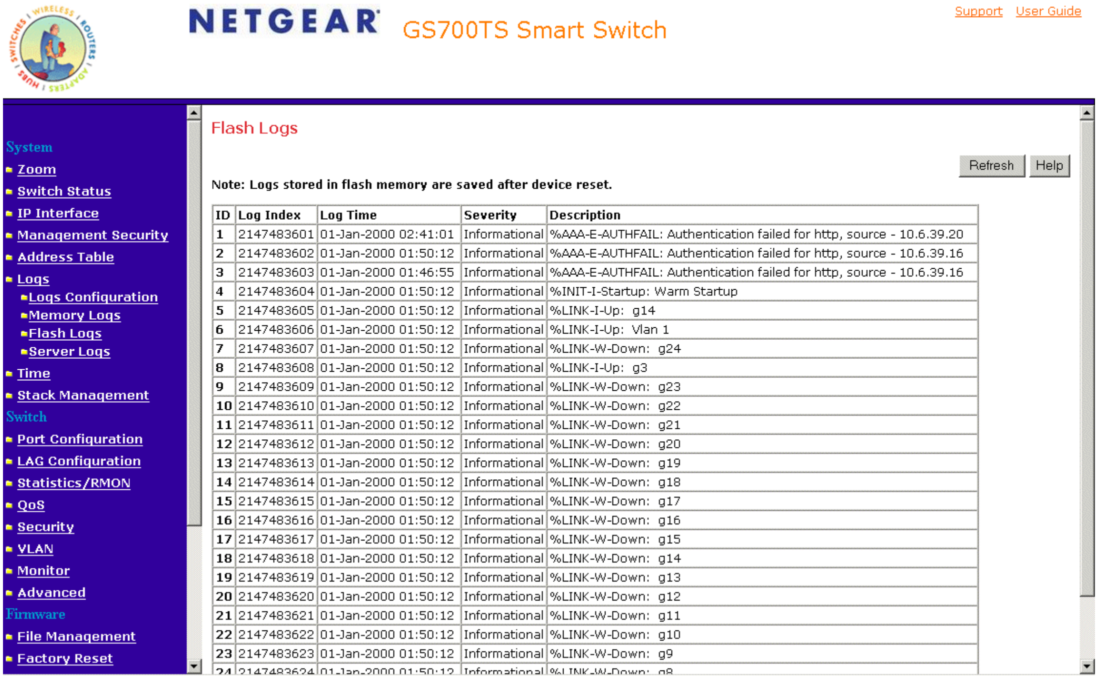
2. Click Clear Logs. The Memory Logs are cleared.

Viewing Flash Logs

The *Flash Logs Page* contains information about log entries saved to the log file in Flash, including the time the log was generated, the log severity, and a description of the log message. The message log is available after reboot.

To view the message logs:

3. Click **Logs** > **Flash Logs**. The *Flash Logs Page* opens:



Flash Logs

Note: Logs stored in flash memory are saved after device reset.

ID	Log Index	Log Time	Severity	Description
1	2147483601	01-Jan-2000 02:41:01	Informational	%AAA-E-AUTHFAIL: Authentication failed for http, source - 10.6.39.20
2	2147483602	01-Jan-2000 01:50:12	Informational	%AAA-E-AUTHFAIL: Authentication failed for http, source - 10.6.39.16
3	2147483603	01-Jan-2000 01:46:55	Informational	%AAA-E-AUTHFAIL: Authentication failed for http, source - 10.6.39.16
4	2147483604	01-Jan-2000 01:50:12	Informational	%INIT-I-Startup: Warm Startup
5	2147483605	01-Jan-2000 01:50:12	Informational	%LINK-I-Up: g14
6	2147483606	01-Jan-2000 01:50:12	Informational	%LINK-I-Up: Vlan 1
7	2147483607	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g24
8	2147483608	01-Jan-2000 01:50:12	Informational	%LINK-I-Up: g3
9	2147483609	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g23
10	2147483610	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g22
11	2147483611	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g21
12	2147483612	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g20
13	2147483613	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g19
14	2147483614	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g18
15	2147483615	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g17
16	2147483616	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g16
17	2147483617	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g15
18	2147483618	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g14
19	2147483619	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g13
20	2147483620	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g12
21	2147483621	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g11
22	2147483622	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g10
23	2147483623	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g9
24	2147483624	01-Jan-2000 01:50:12	Informational	%LINK-W-Down: g8

Figure 5-39

The *Flash Logs Page* contains the following fields:

- **ID** – Displays the table entry number.
- **Log Index** – Displays the log number.
- **Log Time** – Displays the time at which the log was generated.
- **Severity** – Displays the log severity.
- **Description** – Displays the log message text.
  Logs stored in flash memory are saved after device reset.

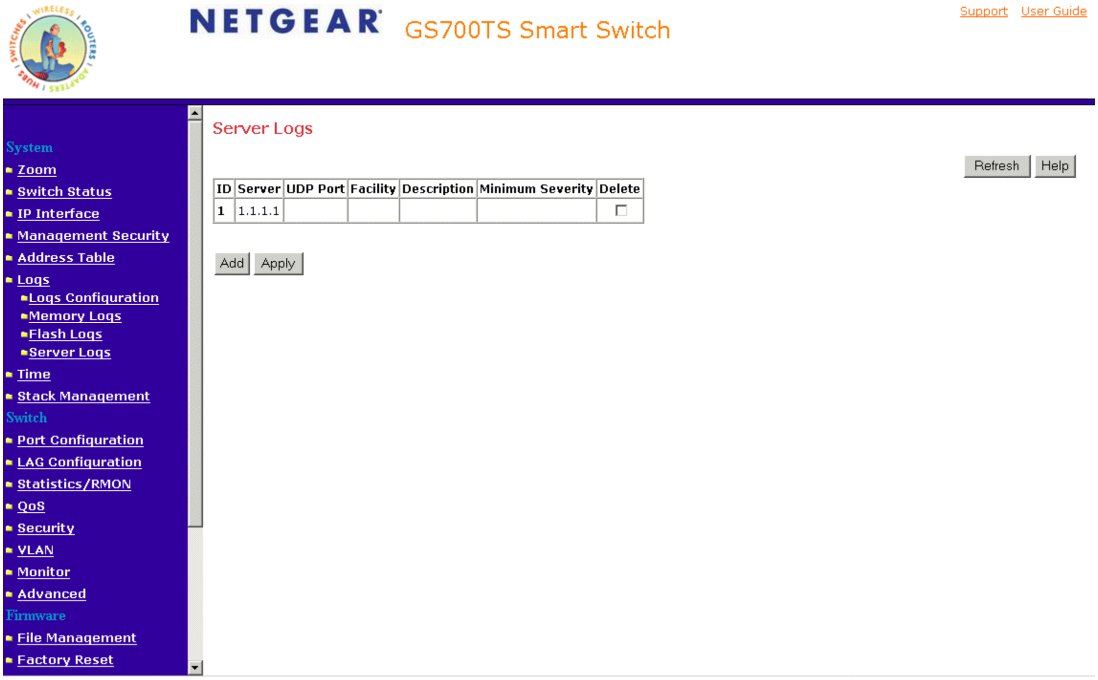
4. Click Clear Logs. The Flash Logs are cleared.

Defining Server Logs

The *Server Logs Page* contains information for viewing and configuring the remote log servers. New log servers can be defined and the log severity sent to each server.

To open the Server Logs Page:

1. Click **Logs** > **Server Logs**. The *Server Logs Page* opens:



ID	Server	UDP Port	Facility	Description	Minimum Severity	Delete
1	1.1.1.1					□

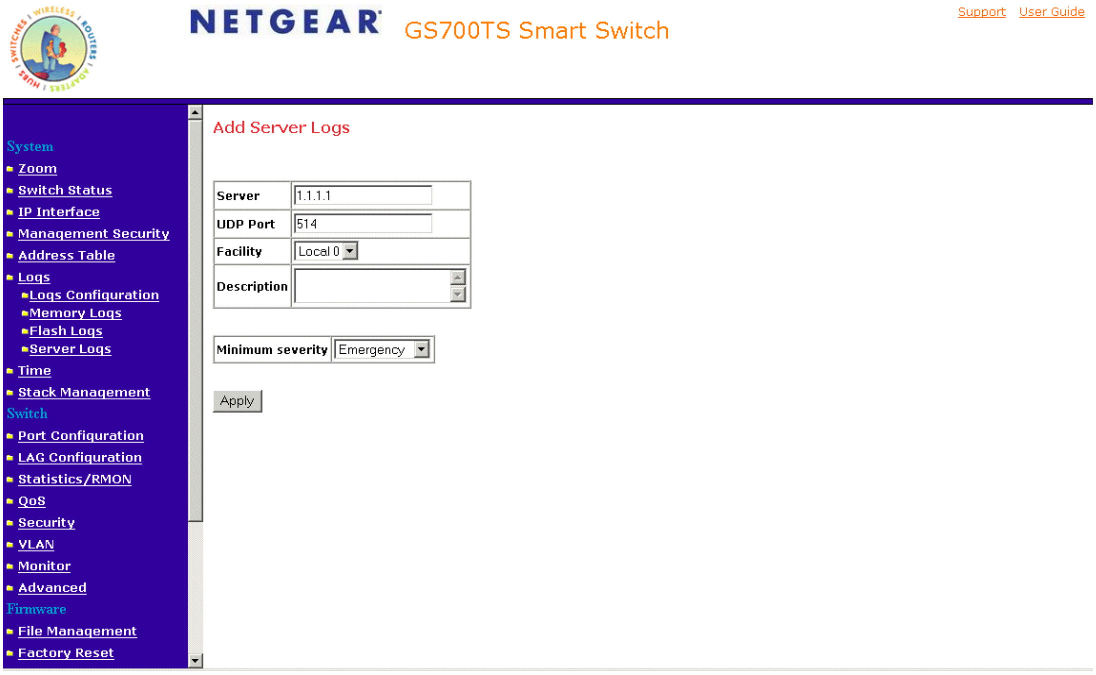
Figure 5-40

The *Server Logs Page* contains the following fields:

- **ID** – Displays the table entry number.
- **Server** – Specifies the server’s IP address to which logs can be sent.
- **UDP Port** – Defines the UDP port to which the server logs are sent. The possible range is 1 - 65535. The default value is 514.

- **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.
- **Description** – A user-defined server description.
- **Minimum Severity** – Indicates the minimum severity from which logs are sent to the server. For example, if Notice is selected, all logs with a severity level of Notice and higher are sent to the remote server. The default value is Informational.
- **Delete** – Deletes the currently selected servers from the Servers list. The possible field values are:
  - *Checked* – Removes the selected server from the Servers Log Parameters Page. Once removed, logs are no longer sent to the removed server.
  - *Unchecked* – Maintains the remote servers.

2. Click Add. The *Add Server Logs Page* opens:



Add Server Logs

Server	1.1.1.1
UDP Port	514
Facility	Local 0
Description	

Minimum severity	Emergency

Figure 5-41

3. Define the relevant fields.

4. Click Apply. The log is defined and the device is updated.

Configuring Interfaces

This section contains information for configuring ports and contains the following topic:

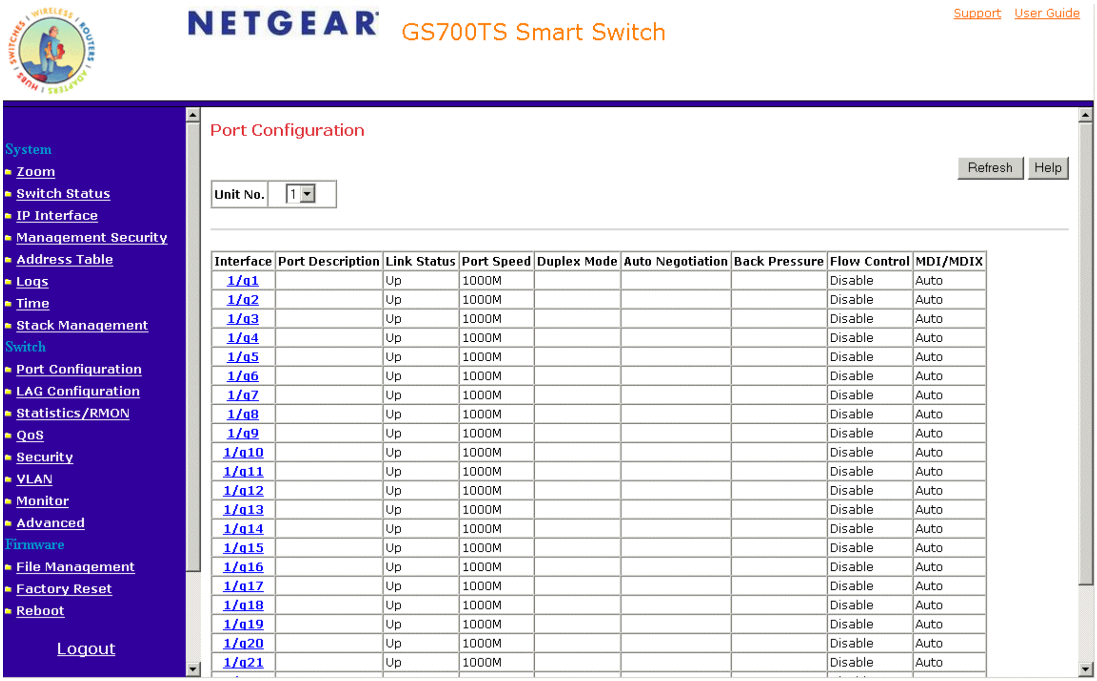
- Defining Port Parameters
- Defining LAG Members

Defining Port Parameters

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

To define port parameters:

1. Click **Port Configuration**. The *Port Configuration Page* opens:



Unit No. 1

Interface	Port Description	Link Status	Port Speed	Duplex Mode	Auto Negotiation	Back Pressure	Flow Control	MDI/MDIX
1/g1		Up	1000M				Disable	Auto
1/g2		Up	1000M				Disable	Auto
1/g3		Up	1000M				Disable	Auto
1/g4		Up	1000M				Disable	Auto
1/g5		Up	1000M				Disable	Auto
1/g6		Up	1000M				Disable	Auto
1/g7		Up	1000M				Disable	Auto
1/g8		Up	1000M				Disable	Auto
1/g9		Up	1000M				Disable	Auto
1/g10		Up	1000M				Disable	Auto
1/g11		Up	1000M				Disable	Auto
1/g12		Up	1000M				Disable	Auto
1/g13		Up	1000M				Disable	Auto
1/g14		Up	1000M				Disable	Auto
1/g15		Up	1000M				Disable	Auto
1/g16		Up	1000M				Disable	Auto
1/g17		Up	1000M				Disable	Auto
1/g18		Up	1000M				Disable	Auto
1/g19		Up	1000M				Disable	Auto
1/g20		Up	1000M				Disable	Auto
1/g21		Up	1000M				Disable	Auto

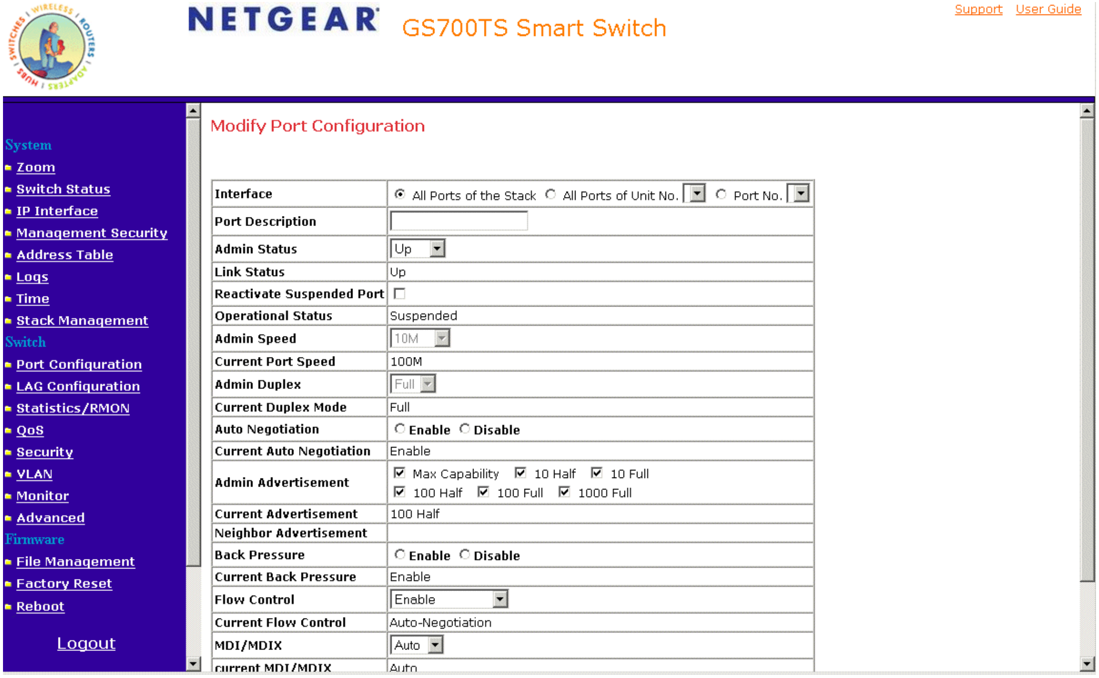
Figure 5-42

The *Port Configuration Page* contains the following fields:

- **Unit No.** – Indicates the stacking number or LAG number.
- **Interface** – Displays the port number.
- **Port Description** – Provides a user-defined device description.
- **Link 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.
- **Port Speed** – Displays the configured rate for the port. The port type determines which speed setting options are available. Port speeds can only be configured when auto negotiation is disabled. The possible field values are:
  - *10* – Indicates the port is currently operating at 10 Mbps.
  - *100* – Indicates the port is currently operating at 100 Mbps.
  - *1000* – Indicates the port is currently operating at 1000 Mbps.
- **Duplex Mode** – Displays 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 LAGs. 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.
- **Auto Negotiation** – Displays 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.
- **Back Pressure** – Displays the Back Pressure mode on the Port. Back Pressure mode is used with half duplex mode to send collision frames to the transmitting station, causing it to pause transmission and then resend the packets. Back Pressure mode is enabled by default.
- **Flow Control** – Displays the flow control status on the port. When flow control is enabled, a pause frame is sent to the transmitting station when the receiving packet buffer memory falls below a certain level. Flow control may operate only when the port is in full duplex mode. FC is enabled by default.

- **MDI/MDIX** – Displays the MDI/MDIX status of the port. The wiring of hubs and switches differ to the wiring of end stations. This is to ensure that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used and the pairs will match 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 Uplink* – 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.

2. Click an interface. The *Modify Port Configuration Page* opens:



Modify Port Configuration

Interface	● All Ports of the Stack ○ All Ports of Unit No. ○ Port No.
Port Description	
Admin Status	Up
Link Status	Up
Reactivate Suspended Port	□
Operational Status	Suspended
Admin Speed	10M
Current Port Speed	100M
Admin Duplex	Full
Current Duplex Mode	Full
Auto Negotiation	○ Enable ○ Disable
Current Auto Negotiation	Enable
Admin Advertisement	☑ Max Capability ☑ 10 Half ☑ 10 Full ☑ 100 Half ☑ 100 Full ☑ 1000 Full
Current Advertisement	100 Half
Neighbor Advertisement	
Back Pressure	○ Enable ○ Disable
Current Back Pressure	Enable
Flow Control	Enable
Current Flow Control	Auto-Negotiation
MDI/MDIX	Auto
current MDI/MDIX	Auto

Figure 5-43

In addition to the fields in the Interface Configuration Page, the *Modify Port Configuration Page* includes the following fields:

- **Interface** – Displays the port number. The possible field values are:
  - *All Ports of the Stack* – Indicates the ports of the stack.

  - *All Ports of Unit No.* – Indicates the ports of the unit.
  - *Port No.* – Indicates the port number.
- **Admin 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 a port if the port has been disabled through the locked port security option. The possible field values are:
  - *Checked* – Returns a suspended port to active status.
  - *Unchecked* – The suspended port status remains unchanged.
- **Operational Status** – Indicates the port operational status. Possible field values are:
  - *Suspended* – The port is currently active, and is currently not receiving or transmitting traffic.
  - *Active* – The port is currently active and is currently receiving and transmitting traffic.
  - *Disable* – The port is currently disabled, and is not currently receiving or transmitting traffic.
- **Admin Speed** – Displays the configured rate for the port. The port type determines what speed setting options are available. Port speeds can only be configured 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.
  - *1000*M – Indicates the port is currently operating at 1000 Mbps.
- **Current Port Speed** – Indicates the current port speed.
- **Admin Duplex** – Displays 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 LAGs. 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** – Indicates the current duplex mode.

- **Auto Negotiation** – Displays 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. The possible field values are:
  - *Enable* – Enables auto negotiation.
  - *Disable* – Disables auto negotiation.
- **Current Auto Negotiation** – Indicates the current auto negotiation status on the port.
- **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 Advertisements** – Indicates the current auto negotiation setting the port advertises.
- **Neighbor Advertisement** – Indicates the neighboring ports advertisement settings. The field values are identical to the Admin Advertisement field values.
- **Current Back Pressure** – Indicates the current back pressure mode on the port.
- **Current Flow Control** – Indicates the current flow control status on the port.
- **Current MDI/MDIX** – Indicates the current MDI/MDIX status of the port.
- **Port Type** – Displays the port type. The possible field values are:
  - *Copper* – Indicates the port has a copper port connection.
  - *Fiber* – Indicates the port has a fiber optic port connection.

3. Define the relevant fields.
4. Click Apply. The parameters are saved and the device is updated.

Defining LAG Members

Link Aggregation optimizes port usage by linking a group of ports together to form a single LAG. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy. Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports. Ensure the following when configuring LAGs:

- All ports within a LAG must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different LAG.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- The device supports up to eight LAGs with eight ports in each LAG.

This section includes the following sections:

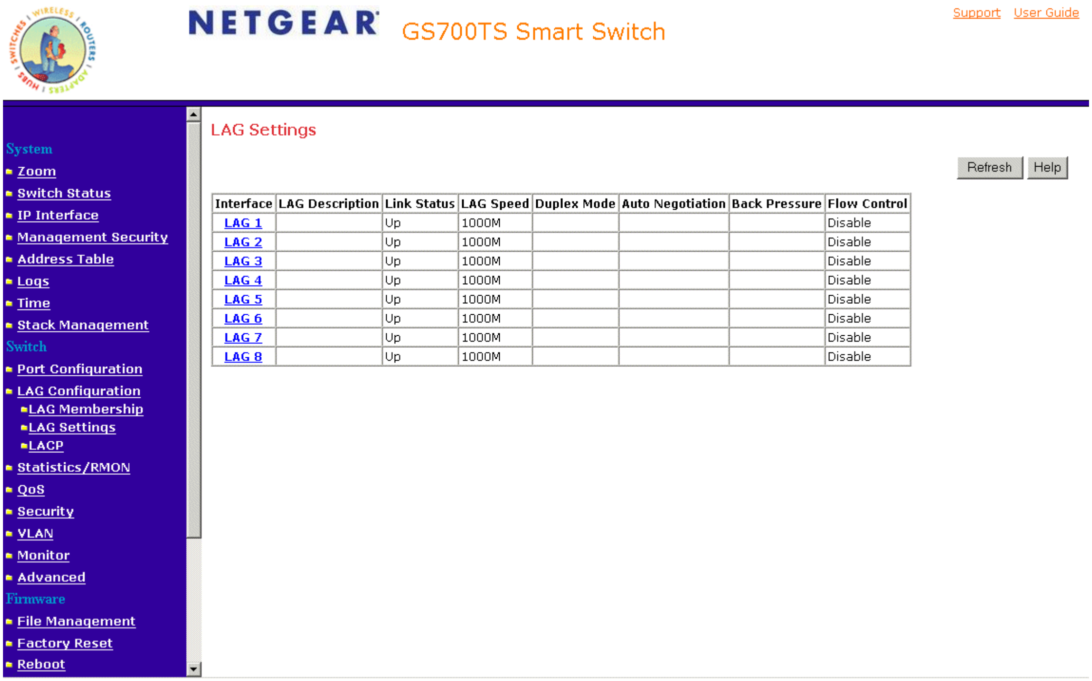
- Configuring LACP
- Viewing LAG Membership
- Configuring LACP

Aggregating Ports

The *LAG Settings Page* contains fields for configuring parameters for configured LAGs. The system supports up to 8 LAGs, and each LAG can contain up to 8 ports.

To define LAG parameters:

1. Click **LAG Configuration > LAG Settings**. The *LAG Settings Page* opens:



LAG Settings

Interface	LAG Description	Link Status	LAG Speed	Duplex Mode	Auto Negotiation	Back Pressure	Flow Control
LAG 1		Up	1000M				Disable
LAG 2		Up	1000M				Disable
LAG 3		Up	1000M				Disable
LAG 4		Up	1000M				Disable
LAG 5		Up	1000M				Disable
LAG 6		Up	1000M				Disable
LAG 7		Up	1000M				Disable
LAG 8		Up	1000M				Disable

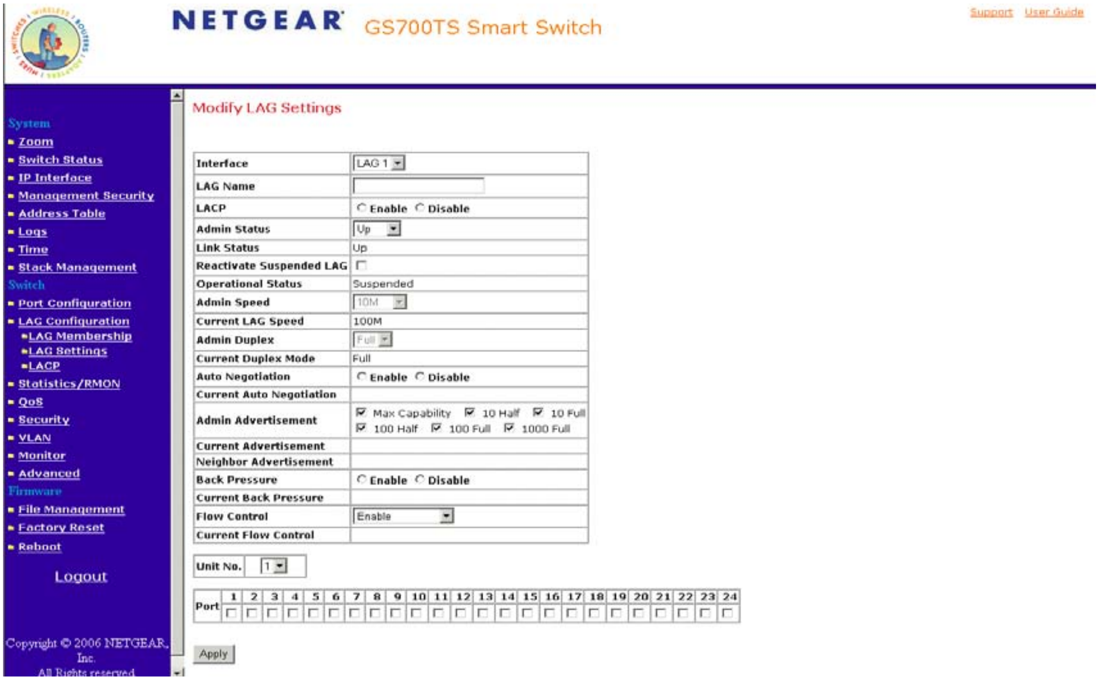
Figure 5-44

The *LAG Settings Page* contains the following fields:

- **Interface** – Displays the LAG number.
- **LAG Description** – Displays the user-defined LAG name.
- **Link Status** – Displays the link operational status. The possible field values are:
  - *Up* – Indicates the LAG is currently linked and forwarding traffic.
  - *Down* – Indicates the LAG is currently not linked.
- **LAG Speed** – Displays the configured rate for the LAG. The port type determines what speed setting options are available. LAG speeds can only be configured when auto negotiation is disabled. The possible field values are:
  - *10* – Indicates the LAG is currently operating at 10 Mbps.
  - *100* – Indicates the LAG is currently operating at 100 Mbps.
  - *1000* – Indicates the LAG is currently operating at 1000 Mbps.

- **Duplex Mode** – Displays 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 LAGs. 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.
- **Auto Negotiation** – Displays the auto negotiation status on the LAG. 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.
- **Back Pressure** – Displays the Back Pressure mode on the LAG. Back Pressure mode is used with half duplex mode to send collision frames to the transmitting station, causing it to pause transmission and then resend the packets.
- **Flow Control** – Displays the flow control status on the LAG. When flow control is enabled, a pause frame is sent to the transmitting station when the receiving packet buffer memory falls below a certain level. Flow control may operate only when the LAG is in full duplex mode. Enabled by default.

2. Click a LAG. The *Modify LAG Settings Page* opens:



Modify LAG Settings

Interface	LAG 1
LAG Name	
LACP	○ Enable ○ Disable
Admin Status	Up
Link Status	Up
Reactivate Suspended LAG	□
Operational Status	Suspended
Admin Speed	10M
Current LAG Speed	100M
Admin Duplex	Full
Current Duplex Mode	Full
Auto Negotiation	○ Enable ○ Disable
Current Auto Negotiation	
Admin Advertisement	☑ Max Capability ☑ 10 Half ☑ 10 Full ☑ 100 Half ☑ 100 Full ☑ 1000 Full
Current Advertisement	
Neighbor Advertisement	
Back Pressure	○ Enable ○ Disable
Current Back Pressure	
Flow Control	Enable
Current Flow Control	

Unit No.	1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 5-45

In addition to the fields in the LAG Settings Page, the *Modify LAG Settings Page* contains the following additional fields:

- **LAG Name** – Displays the user-defined Lag name.
- **LACP** – Enables LACP on the LAG. Link Aggregation Control Protocol automatically bundles ports together in a LAG.
- **Admin 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 a port if the port has been disabled through the locked port security option. The possible field values are:
  - *Checked* – Returns a suspended port to active status.
  - *Unchecked* – The suspended port status remains unchanged.

- **Operational Status** – Indicates the port operational status. Possible field values are:
  - *Suspended* – The port is currently active, and is currently not receiving or transmitting traffic.
  - *Active* – The port is currently active and is currently receiving and transmitting traffic.
  - *Disable* – The port is currently disabled, and is not currently receiving or transmitting traffic.
- **Admin Speed** – Displays the configured rate for the port. The port type determines what speed setting options are available. Port speeds can only be configured 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.
  - *1000*M – Indicates the port is currently operating at 1000 Mbps.
- **Current LAG Speed** – Indicates the current configured rate for the LAG.
- **Admin Duplex** – Displays 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 LAGs. 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.
- **Current Auto Negotiation** – Displays the current Auto Negotiation setting. Auto negotiation of Flow Control (FC) is enabled by default.
- **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.

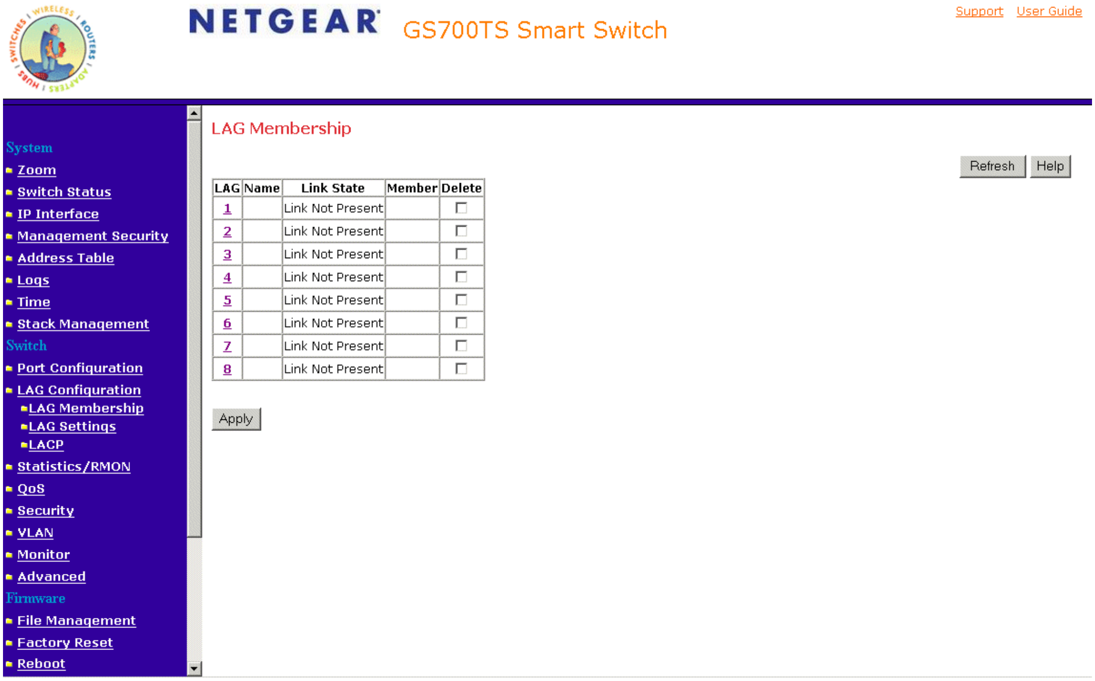
  - *100 Half* – Indicates that the port advertises for a 100 mbps speed port and half duplex mode setting.
  - *100 Full* – Indicates that the port advertises for a 100 mbps speed port and full duplex mode setting.
  - *1000 Full* – Indicates that the port advertises for a 1000 mbps speed port and full duplex mode setting.
- **Current Advertisement** – 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. The field values are identical to the Admin Advertisement field values.
- **Current Back Pressure** – Indicates the current back pressure mode on the port.
- **Current Flow Control** – Indicates the current flow control status on the port.
- **Unit No.** – Indicates the unit number. Possible values are 1-6.
- **Port** – Indicates the port number.

3. Define the relevant fields.
4. Select the ports to be assigned to the LAG.
5. Click Apply. The LAG membership settings are saved and the device is updated.

Viewing LAG Membership

The *LAG Membership Page* presents which ports are assigned to each LAG.

1. Click **LAG Configuration** > **LAG Membership**. The *LAG Membership Page* opens:



LAG Membership

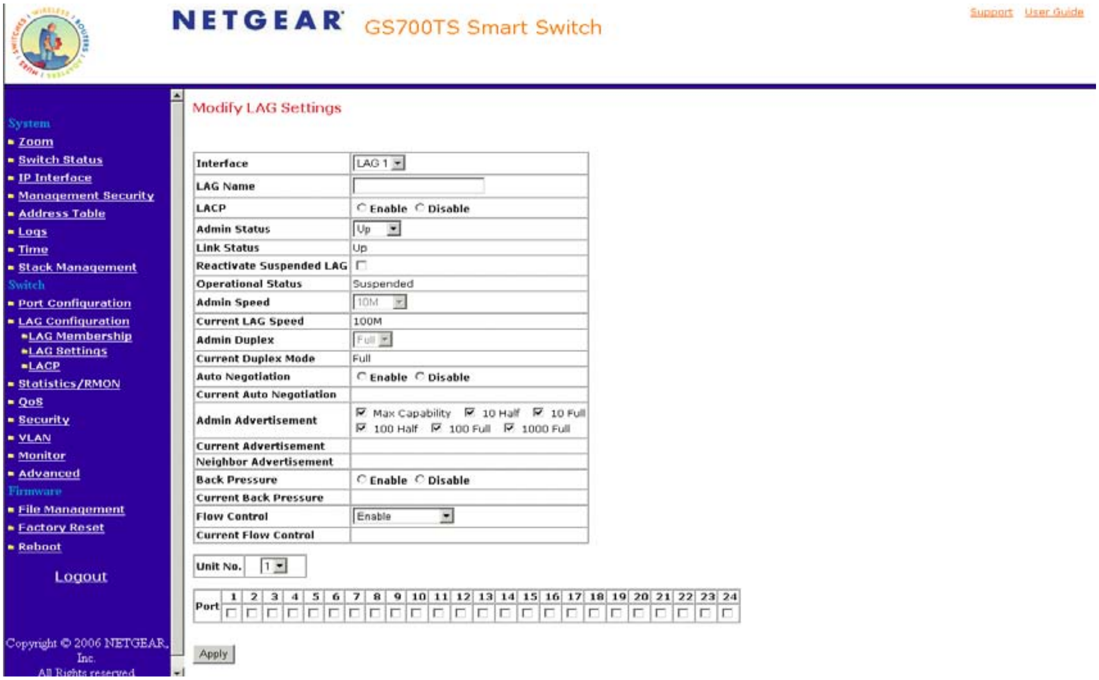
LAG	Name	Link State	Member	Delete
1		Link Not Present		□
2		Link Not Present		□
3		Link Not Present		□
4		Link Not Present		□
5		Link Not Present		□
6		Link Not Present		□
7		Link Not Present		□
8		Link Not Present		□

Figure 5-46

The *LAG Membership Page* contains the following fields:

- **LAG** – Displays the LAG number.
- **Name** – Displays LAG the name.
- **Link State** – Displays the LAG operational status. The possible field values are:
  - *Link Present* – Indicates the LAG is currently linked and forwarding traffic.
  - *Link Not Present* – Indicates the LAG is currently not linked.
- **Member** – Displays the ports that are attached to the LAG.
- **Delete** – Removes the selected LAG.
  - *Checked* – Removes the selected LAG.
  - *Unchecked* – Maintains the LAGs.

2. To change the LAG settings, click on a **LAG**. The *Figure 5-47* opens:



Modify LAG Settings

Interface	LAG 1
LAG Name	
LACP	○ Enable ○ Disable
Admin Status	Up
Link Status	Up
Reactivate Suspended LAG	□
Operational Status	Suspended
Admin Speed	10M
Current LAG Speed	100M
Admin Duplex	Full
Current Duplex Mode	Full
Auto Negotiation	○ Enable ○ Disable
Current Auto Negotiation	
Admin Advertisement	☑ Max Capability ☑ 10 Half ☑ 10 Full ☑ 100 Half ☑ 100 Full ☑ 1000 Full
Current Advertisement	
Neighbor Advertisement	
Back Pressure	○ Enable ○ Disable
Current Back Pressure	
Flow Control	Enable
Current Flow Control	

Unit No.	1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Apply

Figure 5-47

3. Modify the relevant fields.

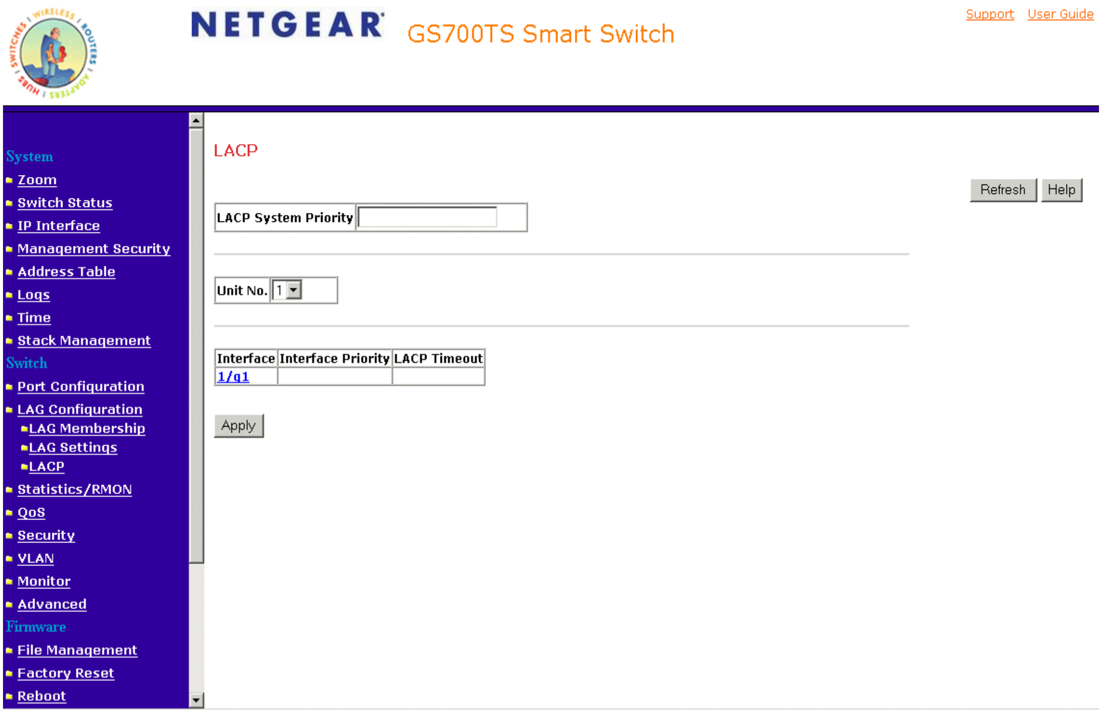
4. Click Apply. The LAG is defined and the device is updated.

Configuring LACP

LAG 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 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 Parameters Page* contains fields for configuring LACP LAGs.

To configure LACP for LAGs:

1. Click **LAG Configuration > LACP**. The *LACP Parameters Page* opens:



LACP

LACP System Priority	

Unit No.	1

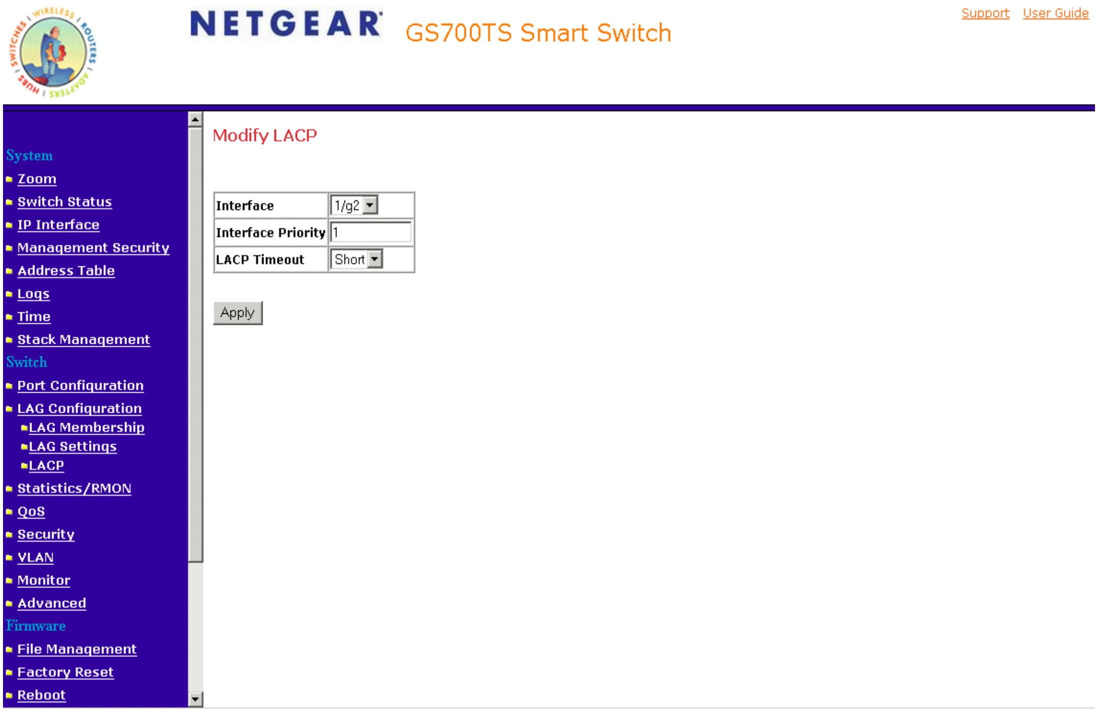
Interface	Interface Priority	LACP Timeout
1/g1		

Figure 5-48

The *LACP Parameters Page* contains the following fields:

- **LACP System Priority** – Specifies system priority value. The field range is 1-65535. The highest priority is 1 and the lowest is 65535. The field default is 1.
- **Unit No.** – Displays the stacking member for which the LAG parameters are defined.
- **Interface** – Displays the interface number to which timeout and priority values are assigned.
- Interface Priority – Displays the LACP priority value for the interface. The field range is 1-65535. The highest priority is 1 and the lowest is 65535. The field default is 1.
- **LACP Timeout** – Displays the administrative LACP timeout. The short timeout time is 3 seconds and the long time out time is 90 seconds.

2. Click an Interface. The *Modify LACP Page* opens:



Modify LACP

Interface	1/g2
Interface Priority	1
LACP Timeout	Short

Figure 5-49

3. Modify the relevant fields.
4. Click Apply. The LACP settings are saved, and the device is updated.

Configuring 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 groups. VLAN tagging attaches a 4-byte tag to packet headers. The VLAN tag indicates to which VLAN the packets 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.

The NETGEAR GS700TS Switch supports up to 128 active VLANs.

This section contains the following topics:

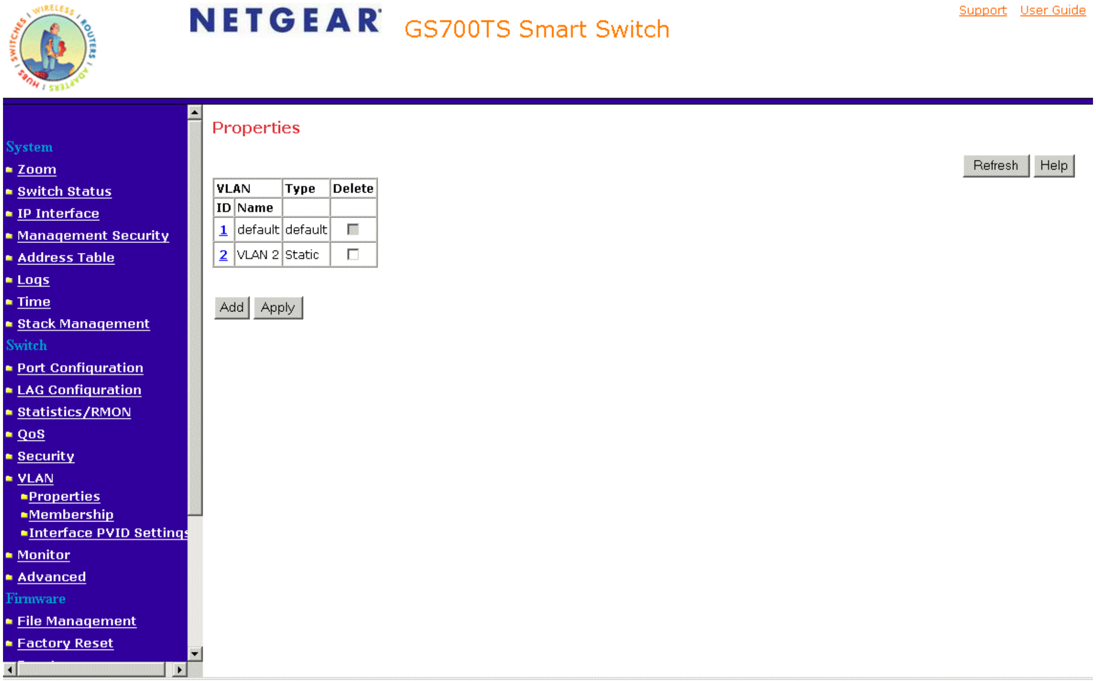
- Defining VLAN Properties
- Defining VLAN Membership
- Defining VLAN PVID Settings

Defining VLAN Properties

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

To define VLAN properties:

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



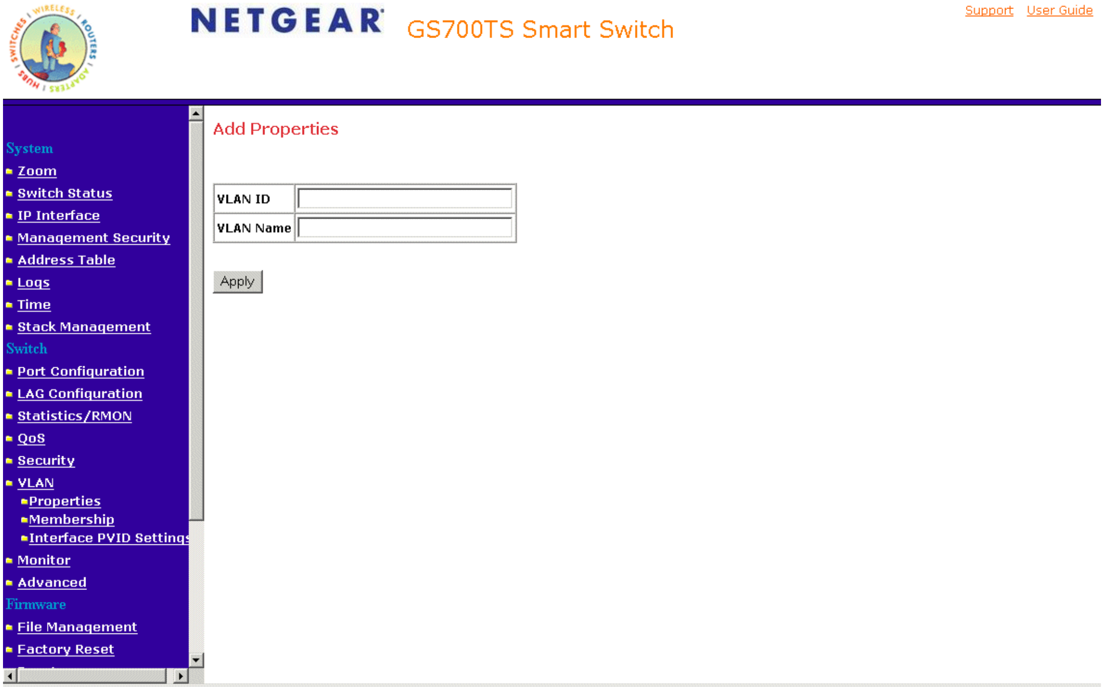
VLAN		Type	Delete
ID	Name		
1	default	default	□
2	VLAN 2	Static	□

Figure 5-50

The *VLAN Properties Page* contains the following fields:

- **ID** – Displays the VLAN ID.
- **Name** – Displays the user-defined VLAN name.
- **Type**– Displays the VLAN type. The possible field values are:
  - *Static* – Indicates the VLAN is user-defined.
  - *Default* – Indicates the VLAN is the default VLAN. The default VLAN is enabled by default.
- **Delete**– Removes VLANs. The possible field values are:
  - *Checked* – Removes the selected VLAN.
  - *Unchecked* – Maintains VLANs.

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



Add Properties

VLAN ID	
VLAN Name	

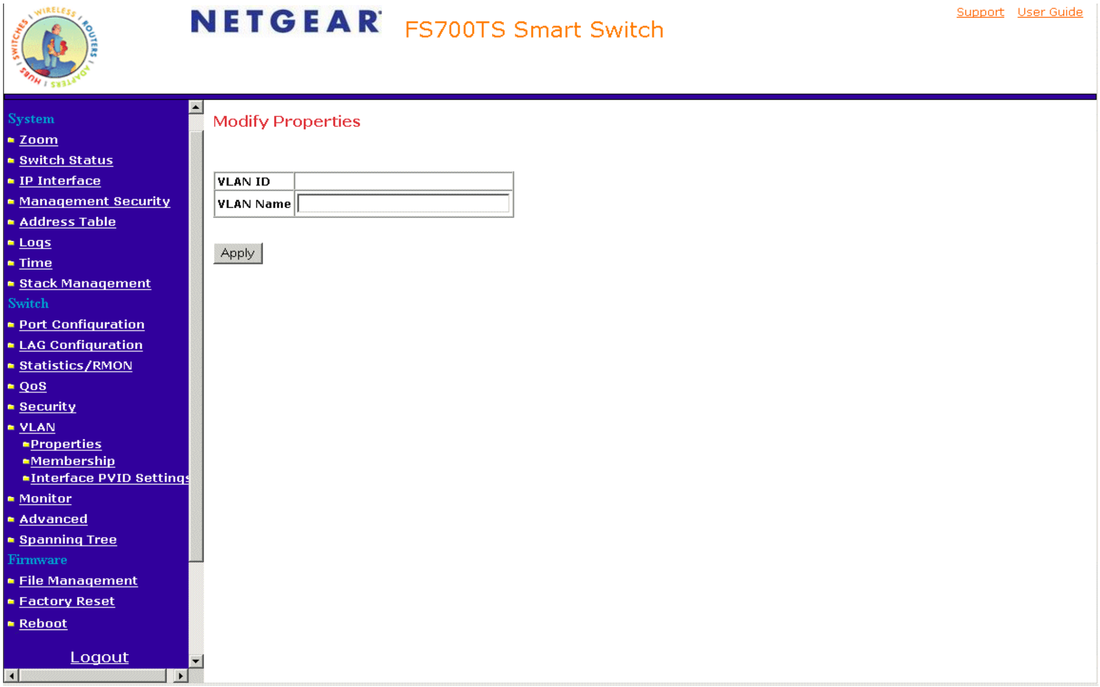
Figure 5-51

3. Define the relevant fields.

4. Click Apply. The VLAN ID is defined and the device is updated.

To modify VLAN properties:

1. Click **VLAN** > **Properties**. The *VLAN Properties Page* opens.
2. Click on an Interface to access the *Figure 5-52*. The *Figure 5-52* opens:



Modify Properties

VLAN ID	
VLAN Name	

Figure 5-52

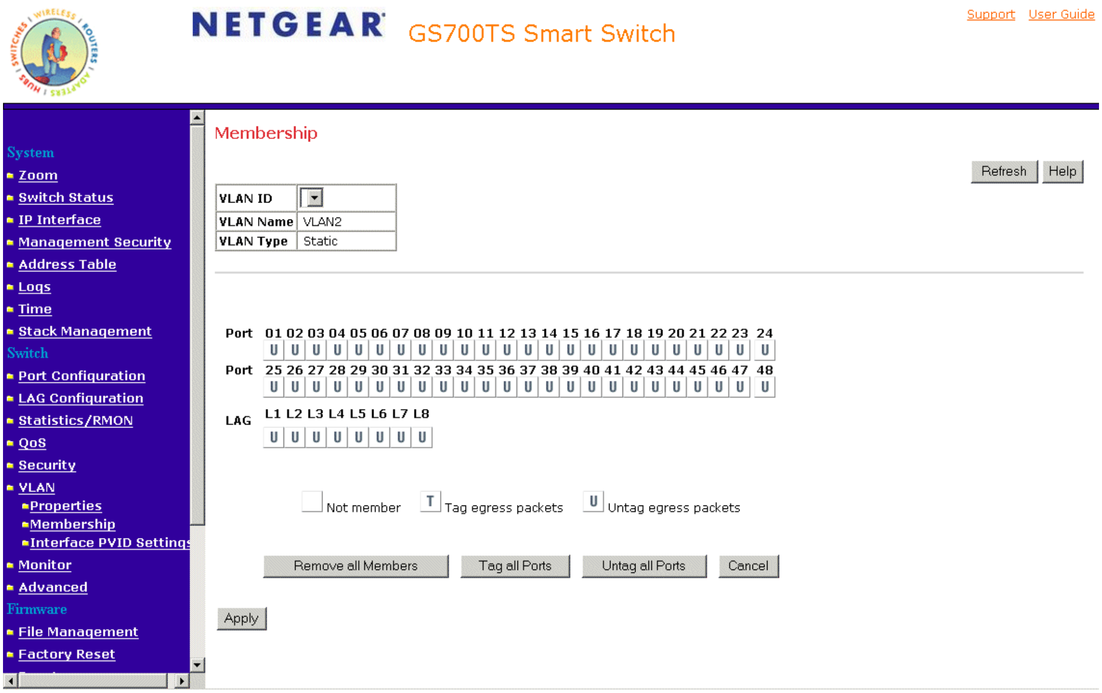
3. Modify the relevant fields.
4. Click Apply, The VLAN Settings are modified, and the device is updated.

Defining VLAN Membership

The *VLAN Membership Page* contains a table that maps VLAN parameters to ports. Ports are assigned VLAN membership by toggling through the Port Control settings.

To define VLAN membership:

1. Click **VLAN** > **Membership**. The *VLAN Membership Page* opens:



Membership

VLAN ID	
VLAN Name	VLAN2
VLAN Type	Static

Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
Port	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
LAG	L1	L2	L3	L4	L5	L6	L7	L8																
	U	U	U	U	U	U	U	U																

□ Not member T Tag egress packets U Untag egress packets

Figure 5-53

The *VLAN Membership Page* contains the following fields:

- **VLAN ID** – Displays the user-defined VLAN ID.
- **VLAN Name** – Displays the name of the VLAN.
- **VLAN Type**– Indicates the VLAN type. The possible field values are:
  - *Static* – Indicates the VLAN is user-defined.
  - *Default* – Indicates the VLAN is the default VLAN. The default VLAN is enabled.

2. Define the membership of the ports by clicking on the box beneath the port or LAG numbers. The status is toggled between the following values:

- **Tag egress packets (Tagged)** – Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.

- **Untag egress packets (Untagged)** – Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
- **Not member** – Indicates the interface is not a member of the VLAN.
  - Click Remove all Members. All members of the VLAN are removed.
  - Click Tag all Ports. All ports are tagged.
  - Click Untag all Ports. All ports are untagged.
  - Click Cancel. All changes are cancelled and return to the previous settings.

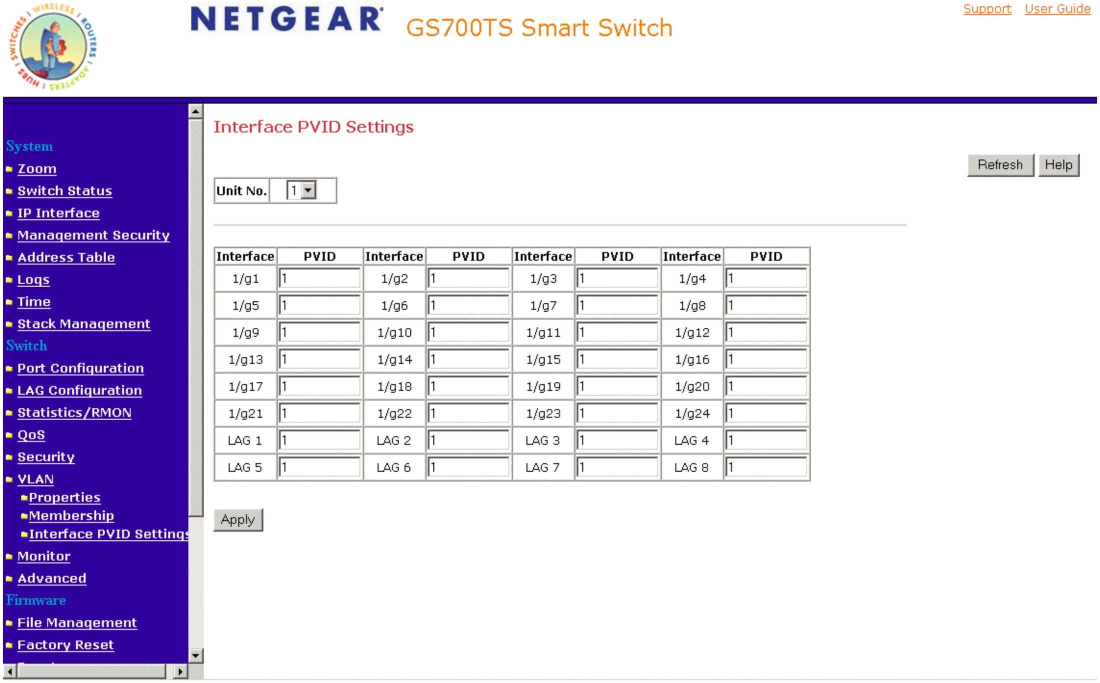
3. Click Apply. The VLAN Membership is defined and the device is updated.

Defining VLAN PVID Settings

The *Interface PVID Settings Page* contains parameters for assigning Port VLAN ID (PVID) values to interfaces. The PVID is the VLAN on which untagged incoming traffic will be forwarded. All ports must have a defined PVID. If no other value is configured the default VLAN PVID is used. VLAN number 1 is the default VLAN and cannot be deleted from the system.

To open the *Interface PVID Settings Page*:

1. Click **VLAN** > **Interface PVID Settings**. The *Interface PVID Settings Page* opens:



Interface PVID Settings

Unit No. 1

Interface	PVID	Interface	PVID	Interface	PVID	Interface	PVID
1/g1	1	1/g2	1	1/g3	1	1/g4	1
1/g5	1	1/g6	1	1/g7	1	1/g8	1
1/g9	1	1/g10	1	1/g11	1	1/g12	1
1/g13	1	1/g14	1	1/g15	1	1/g16	1
1/g17	1	1/g18	1	1/g19	1	1/g20	1
1/g21	1	1/g22	1	1/g23	1	1/g24	1
LAG 1	1	LAG 2	1	LAG 3	1	LAG 4	1
LAG 5	1	LAG 6	1	LAG 7	1	LAG 8	1

Figure 5-54

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

- **Unit No.** – Displays the stacking member for which the PVID information is displayed.
- **Interface** – Displays the interface to which the PVID tag is assigned. The possible field values are:
  - *Port* –Displays the port to which the PVID tag is attached.
  - *LAG* – Displays the LAG to which the PVID tag is attached.
- **PVID** – Displays the PVID value. The possible field range is 1-4094.

2. Enter the PVID for the corresponding interfaces.

3. Click Apply. The PVID settings are saved and the device is updated.

Defining IP Interface

This section contains the following topics:

- Configuring IP Interfaces

Configuring IP Interfaces

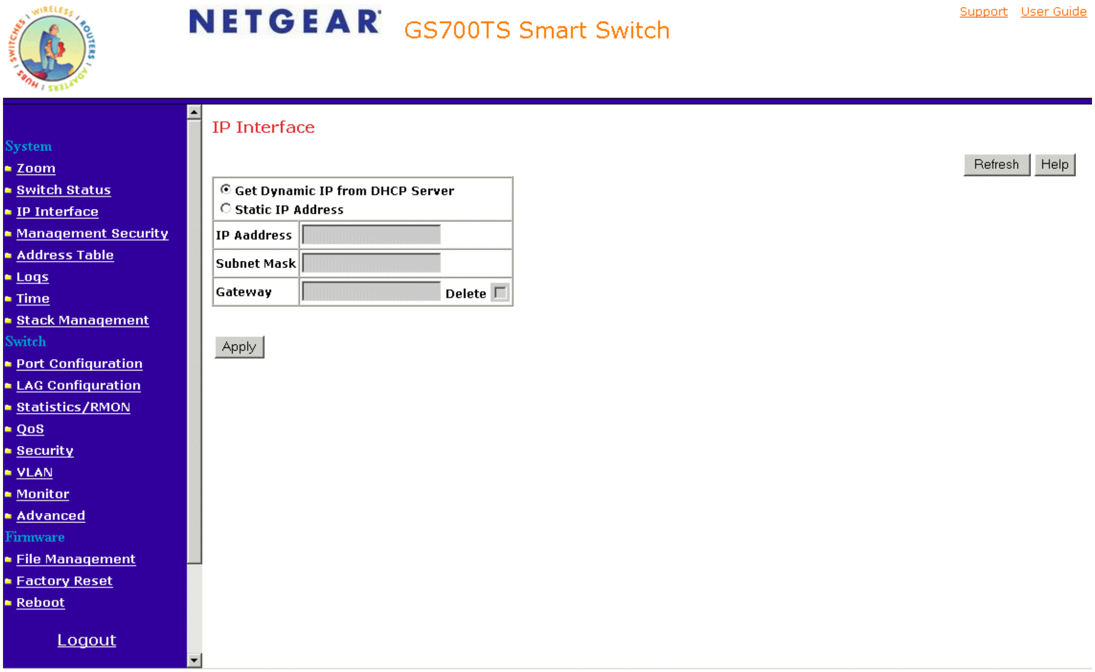
The *IP Interface Page* contains fields for assigning the IP address of the switch. The IP address may either be statically defined or may be retrieved using the Dynamic Host Configuration Protocol (DHCP). The IP Interface Page also contains information for defining the default gateway. When using DHCP, network devices can have a different IP address every time the device connects to the network.

Note the following when configuring IP Addresses:

- If the device was accessed using the Smartwizard Discovery, the IP address retrieved through DHCP is displayed.
- If the device fails to retrieve an IP address through DHCP, the default IP address is 192.168.0.239.

To define the IP interface:

1. Click **IP Interface**. The *IP Interface Page* opens:



IP Interface

● Get Dynamic IP from DHCP Server ○ Static IP Address	
IP Aaddress	
Subnet Mask	
Gateway	Delete □

Figure 5-55

The *IP Interface Page* contains the following fields:

- **Get Dynamic IP from DHCP Server** – Retrieves the IP addresses using DHCP.
- **Static IP Address** – The IP Address is set manually.
- **IP Address** – Displays the currently configured IP address.
- **Subnet Mask** – Displays the currently configured IP address mask.
- **Gateway** – Defines the default gateway IP address.
- **Delete** – Removes the selected IP address from the interface. The possible field values are:
  - *Checked* – Removes the IP address from the interface.
  - *Unchecked* – Maintains the IP address assigned to the interface.

If the IP address is deleted, the default IP address is assigned.

2. Define the relevant fields.

3. Click Apply. The IP configuration fields are saved and the device is updated.

Defining the Forwarding Address Tables

Packets addressed to destinations stored in either the Static or Dynamic databases are immediately forwarded to the port. The Dynamic MAC Address Table can be sorted by interface, VLAN, or MAC Address, whereas MAC addresses are dynamically learned as packets from sources that arrive at the device. Static addresses are configured manually.

An address becomes associated with a port by learning the port from the frame’s source address but if a frame that is addressed to a destination MAC address is not associated with a port, that frame is flooded to all relevant VLAN ports. To prevent the bridging table from overflowing, a dynamic MAC address, from which no traffic arrives for a set period, is erased.

The Defining the Forwarding Address Tables Page contains parameters for defining the age interval on the device.

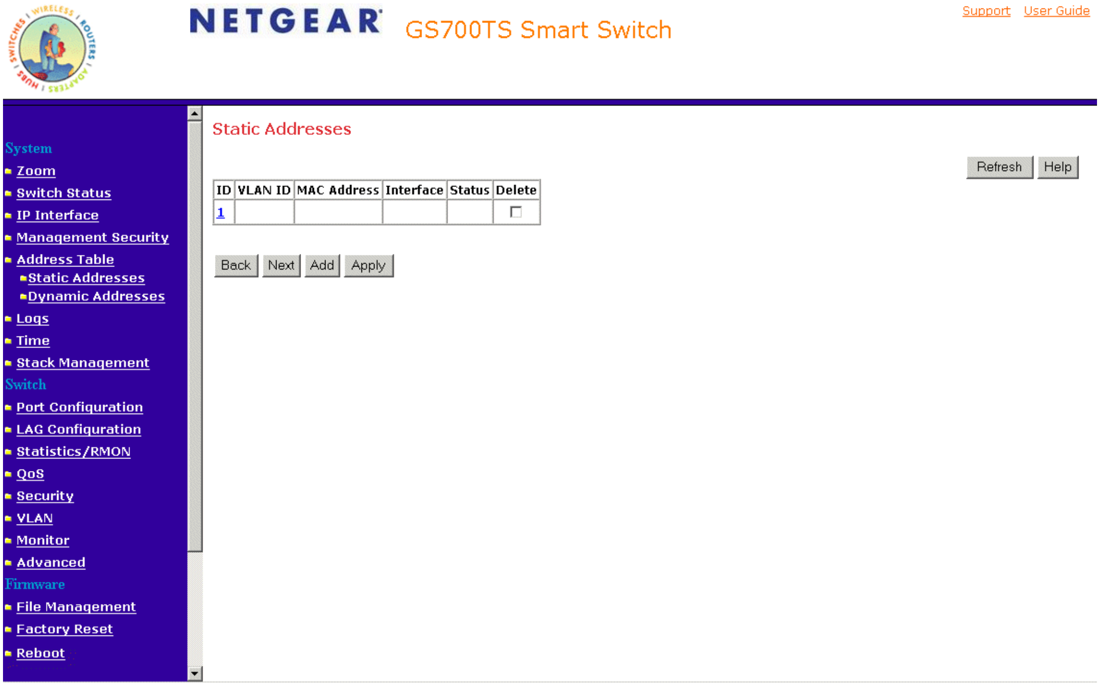
To prevent static MAC addresses from being deleted when the device is reset, ensure that the port attached to the MAC address is locked. This section includes the following topics:

- Configuring Static Addresses
- Viewing Dynamic Addresses

Configuring Static Addresses

To configure the static addresses:

1. Click **Address Table > Static Addresses**. The *Static Addresses Page* opens:



ID	VLAN ID	MAC Address	Interface	Status	Delete
1					□

Figure 5-56

The *Static Addresses Page* contains the following fields:

- **ID** – Indicates the stacking number.
- **VLAN ID** – Displays the VLAN ID number to which the entry refers.
- **MAC Address** – Displays the MAC address to which the entry refers.
- **Interface** – Displays the interface to which the entry refers.
- **Status** – Displays how the entry was created. The possible field values are:
  - *Secure* – The MAC Address is defined for locked ports.
  - *Permanent* – The MAC address is permanent and is never deleted.
  - *Delete on Reset* – The MAC address is deleted when the device is reset.

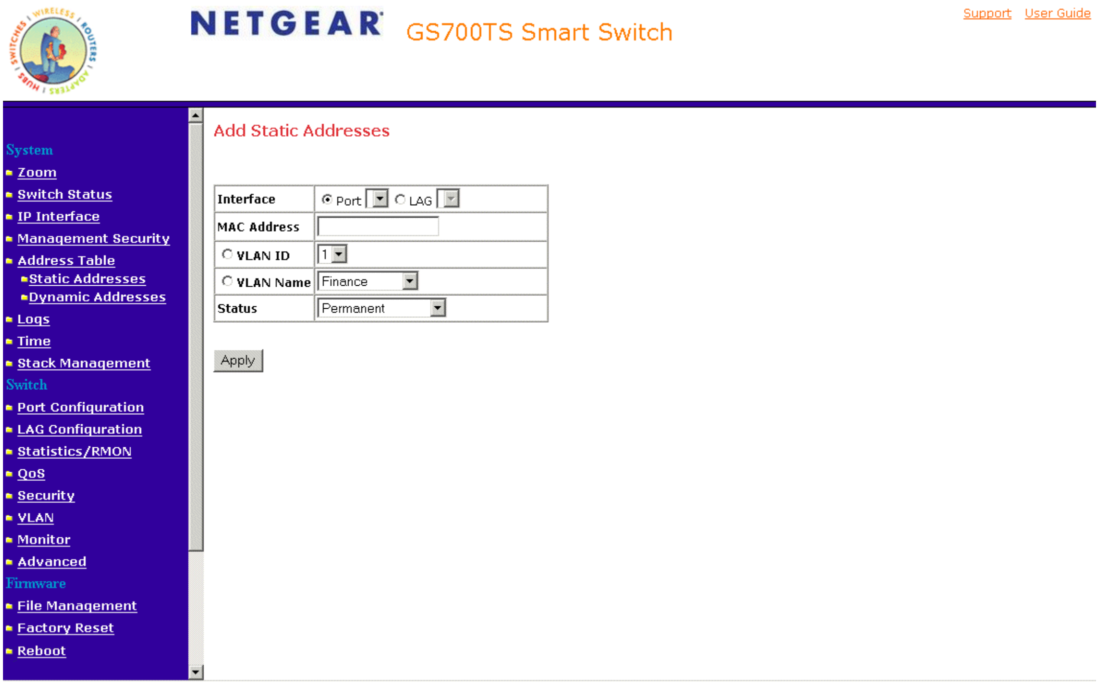
   – *Delete on Timeout* – The MAC address is deleted when a timeout occurs.

- **Delete** – Removes the entry. The possible field values are:
   – *Checked* – Removes the selected entry.
   – *Unchecked* – Maintains the current static forwarding database.
- **Back** – Displays the previous page of VLANs in the Statistics Address table, if there is a previous page.
- **Next** – Displays the following page of VLANs in the Statistics Address table, if there is a page following the current page.

To prevent static MAC addresses from being deleted when the device is reset, ensure the port attached to the MAC address is set to secure.

To add a new static address entry:

1. Click **Address Table > Static Addresses**. The *Add Static Addresses Page* opens.
2. Click Add . The *Add Static Addresses Page* opens:



Add Static Addresses

Interface	● Port ▾ ○ LAG ▾
MAC Address	
○ VLAN ID	1 ▾
○ VLAN Name	Finance ▾
Status	Permanent ▾

Figure 5-57

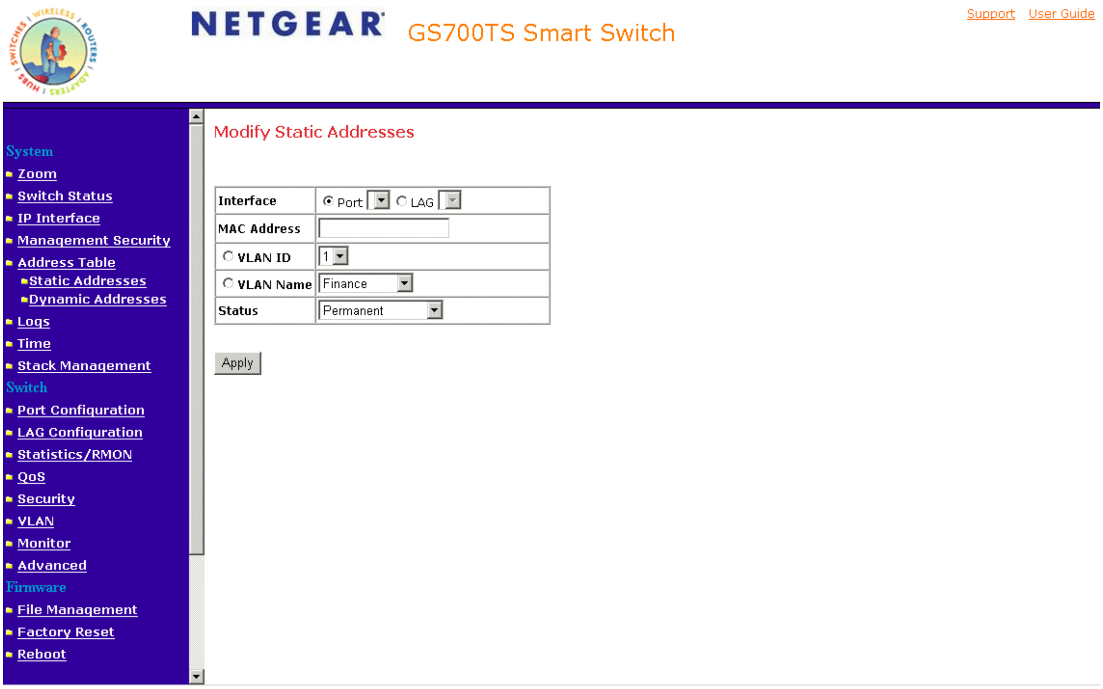
In addition to the *Static Addresses Page*, the *Add Static Addresses Page* contains the following field:

- **VLAN Name** – Indicates the name of the VLAN. The possible field values are:
  - *Finance*
  - *Development*

3. Define the relevant fields.
4. Click Apply. The forwarding database information is modified and the device is updated.

To modify a static address entry:

1. Click **Address Table > Static Addresses**. The *Static Addresses Page* opens.
2. Select and existing IP address. The *Modify Static Addresses Page* opens:



Modify Static Addresses

Interface	● Port ○ LAG
MAC Address	
○ VLAN ID	1
○ VLAN Name	Finance
Status	Permanent

Figure 5-58

In addition to the *Static Addresses Page*, the *Modify Static Addresses Page* contains the following field:

- **VLAN Name** – Indicates the name of the VLAN. The possible field values are:

   - *Finance*
   - *Development*

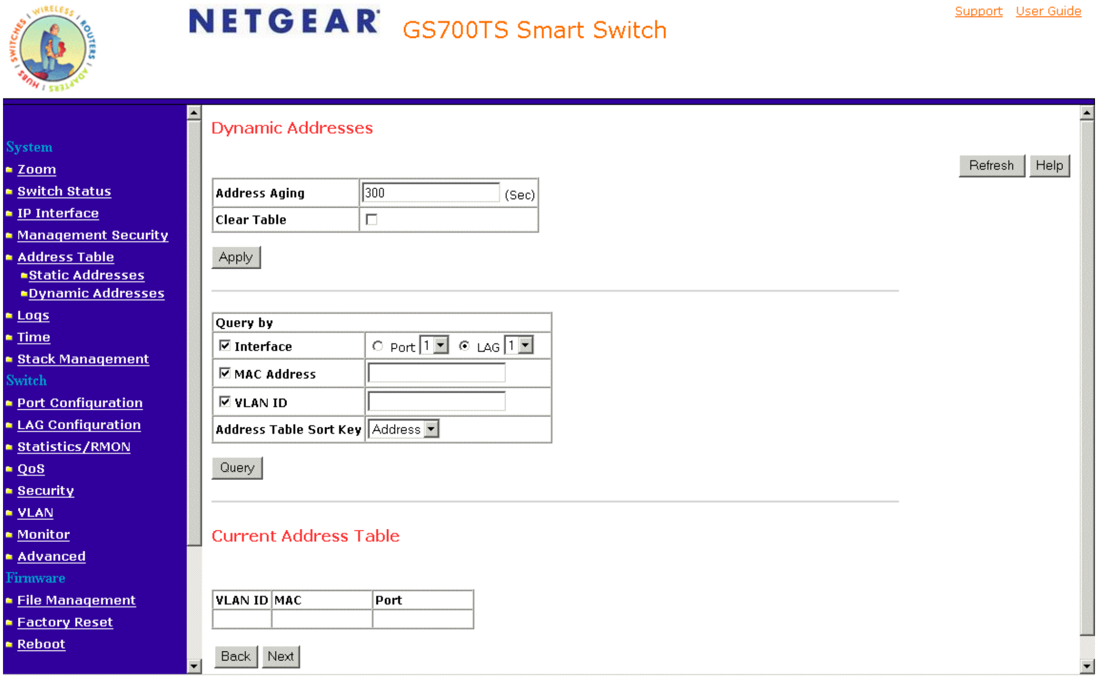
3. Modify the relevant fields.
4. Click Apply. The forwarding database information is modified and the device is updated.

Viewing Dynamic Addresses

The Dynamic Addresses Page contains parameters for querying information in the Dynamic MAC Address Table, including the interface type, MAC addresses, VLAN, and table storing. The Dynamic MAC Address table contains information about the aging time before a dynamic MAC address is erased and includes parameters for querying and viewing the Dynamic MAC Address table. The Dynamic MAC Address table contains address parameters by which packets are directly forwarded to the ports. The Dynamic MAC Address table can be sorted by Interface, VLAN, and MAC Address.

To view the Dynamic MAC Address Table:

1. Click **Address Table > Dynamic Addresses**. The *Dynamic Addresses Page* opens:



Dynamic Addresses

Address Aging	300 (Sec)
Clear Table	□

Query by

☑ Interface	○ Port 1 ● LAG 1
☑ MAC Address	
☑ VLAN ID	
Address Table Sort Key	Address

Current Address Table

VLAN ID	MAC	Port

Figure 5-59

The *Dynamic Addresses Page* contains the following fields:

- **Address Aging** – Specifies the amount of time the MAC address remains in the Dynamic MAC Address table before it is timed out if no traffic from the source is detected. The default value is 300 seconds.
- **Clear Table** – Removes the current values from the table.
- **Interface** – Specifies the interface for which the table is queried. There are two interface types from which to select.
  - *Port* – Indicates the Port for which the table is currently queried
  - *LAG* – Indicates the LAG for which the table is currently queried
- **MAC Address** – Specifies the MAC address for which the table is queried.
- **VLAN ID** – Specifies the VLAN ID for which the table is queried.

- **Address Table Sort Key** – Specifies the means by which the Dynamic MAC Address Table is sorted. The address table can be sorted by address, VLAN, or interface.
  - *Address*– Displays the current address.
  - *VLAN* – Shows the ID of the current VLAN.
  - *Interface* – Indicates the interface for which the table is currently queried.

The device shortens user wait time by providing Data Display on Demand. When the system retrieves vast amounts of configuration data, the data is divided into groups. The system administrator can view the configuration information either selecting a specific interface or using the Next and Back link.

- **VLAN ID** – Shows the ID of the current VLAN.
- **MAC** – Displays the current MAC address.
- **Port** – Indicates the interface for which the table is currently queried.
- **Back** – Displays the previous page of the configuration information, if there is a previous page.
- **Next** – Displays the following page of the configuration information, if there is a page following the current page.

2. Define the relevant fields.

3. Click Apply. The Dynamic Address Aging field is defined and the device is updated.

To query the Dynamic MAC Address Table:

1. Click **Address Table > Dynamic Addresses**. The Dynamic Addresses Page opens.

2. Define the relevant fields.

3. Click Query. The Dynamic MAC Address Table is queried and the results are displayed.

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.

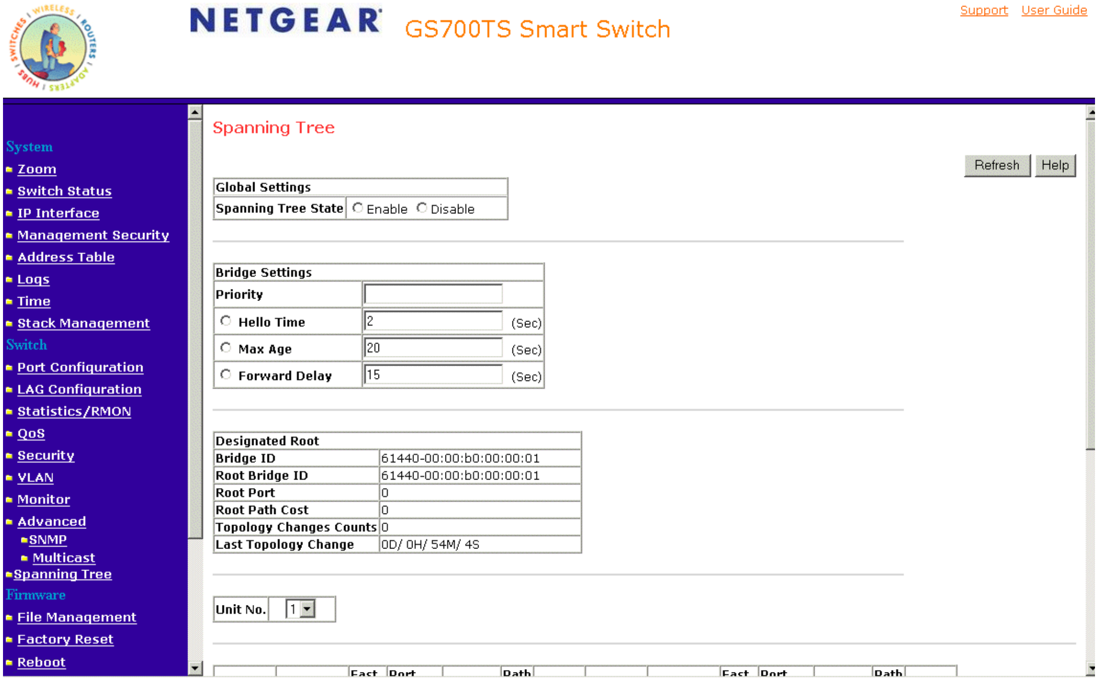
This section contains the following topics:

- Configuring the Spanning Tree Protocol
- Defining STP on Interfaces

Configuring the Spanning Tree Protocol

To configure STP on the device:

1. Click **Advanced** > **Spanning Tree**. The *Spanning Tree Page* opens:



Spanning Tree

Global Settings	
Spanning Tree State	○ Enable ○ Disable

Bridge Settings		
Priority		
○ Hello Time	2	(Sec)
○ Max Age	20	(Sec)
○ Forward Delay	15	(Sec)

Designated Root	
Bridge ID	61440-00:00:b0:00:00:01
Root Bridge ID	61440-00:00:b0:00:00:01
Root Port	0
Root Path Cost	0
Topology Changes Counts	0
Last Topology Change	0D/ 0H/ 54M/ 4S

Unit No. 1

Figure 5-60

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.
- **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 16. For example, 16, 32, 64, 80, etc.

- **Hello Time (1-10)** – Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a Root The device waits between configuration messages. The default is 2 seconds.
- **Max Age (6-40)** – Specifies the device Maximum Age Time. The Maximum Age Time is the amount of time in seconds a bridge waits before sending configuration messages. The default Maximum Age Time is 20 seconds.
- **Forward Delay (4-30)** – Specifies the device Forward Delay Time. The Forward Delay Time is the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.
- **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 amount of time 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. The current root port and current root cost display as zero when this device is not connected to the network.

Interface Status

- **Unit No.** – Indicates the stacking member for which the STP information is displayed.
- **Interface** – Indicates the port or LAG for which the STP information is displayed.
- **STP Status** – Enables or disables STP on the port.
- **Fast Link** – 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* – Indicates that Fast Link is enabled on the port.
  - *Disable* – Indicates that Fast Link is disabled on the port.

- **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:
  - *Forwarding* – Indicates that STP is enabled on the port, and the port is forwarding packets based on the STP topology.
  - *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 STP is enabled.
- **Speed** – Indicates the speed at which the port is operating.
- **Path Cost** – 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 default path cost assigned to an interface varies according to the selected method (Hello Time, Max Age, or Forward Delay).
- **Priority (0-65535)**– 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.

2. Define the relevant fields.

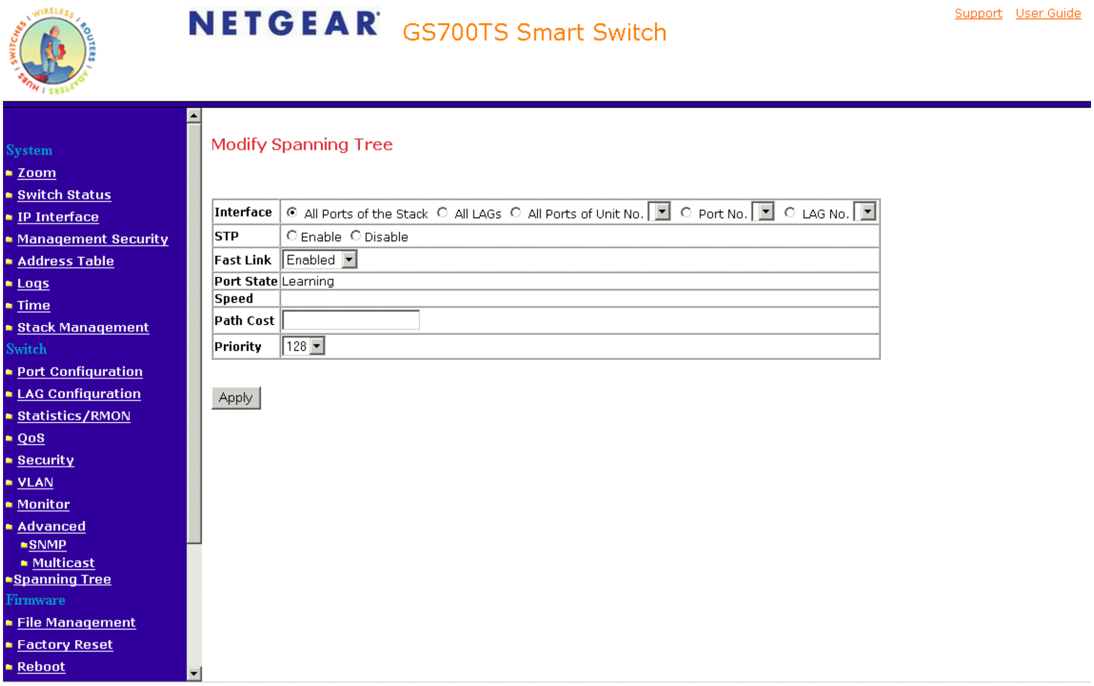
3. Click Apply. STP is enabled and the device is updated.

Defining STP on Interfaces

Network administrators can assign STP settings to specific interfaces using the *Modify Spanning Tree Page*. The Global LAGs section displays the STP information for Link Aggregated Groups.

To assign STP settings to an interface:

1. Click **Advanced** > **Spanning Tree** and click an interface. The *Modify Spanning Tree Page* opens:



Modify Spanning Tree

Interface	● All Ports of the Stack ○ All LAGs ○ All Ports of Unit No. ○ Port No. ○ LAG No.
STP	○ Enable ○ Disable
Fast Link	Enabled
Port State	Learning
Speed	
Path Cost	
Priority	128

Figure 5-61

The *Modify Spanning Tree Page* contains the following fields:

- **Interface** – The interface for which the information is displayed. The possible field values are:
  - *All Ports of the Stack* – Selects all ports on the stack.
  - *All LAGs* – Selects all LAGs on the stack.
  - *All Ports of Unit No.* – Selects all ports of the selected unit number.
  - *Port No.* – Indicates the port number to which the setting should be applied.
  - *LAG No.* – Indicates the LAG number to which the setting should be applied.
- **STP** – Indicates if STP is enabled on the port. The possible field values are:
  - *Enable* – Enables STP on the port.

  - *Disable* – Disables STP on the port. This is the default value.
- **Fast Link** – 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 Fast Link on the interface.
  - *Auto* – Automatically enables or disables Fast Link on the interface.
  - *Disable* – Disables Fast Link on the interface.
- **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:
  - *Learned* – Indicates the port is currently in the learning mode. The port 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.
  - *Blocking* – Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses. Blocking is displayed when STP is enabled.
- **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 re-routed.
- **Priority** – Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 -240. The priority value is determined in increments of 16.

2. Define the relevant fields.

3. Click Apply. STP is enabled on the interface and the device is updated.

Configuring Quality of Service

Quality of Service (QoS) provides the ability to implement QoS and priority queuing within a network. For example, certain types of traffic that require minimal delay, such as Voice, Video, and real-time traffic can be assigned a high priority queue, while other traffic can be assigned a lower priority queue. The result is an improved traffic flow for traffic with high demand. QoS is defined by:

- **Classification** – Specifies which packet fields are matched to specific values. All packets matching the user-defined specifications are classified together.

- **Action** – Defines traffic management where packet forwarding is based on packet information and packet field values such as *VLAN Priority Tag* (VPT) and *DiffServ Code Point* (DSCP).

After packets are assigned to a specific egress queue, 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 email (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. If WRR is selected, the following weights are assigned to the queues: 1, 2, 4, 8.

This section contains information for defining general QoS settings, and includes the following topics:

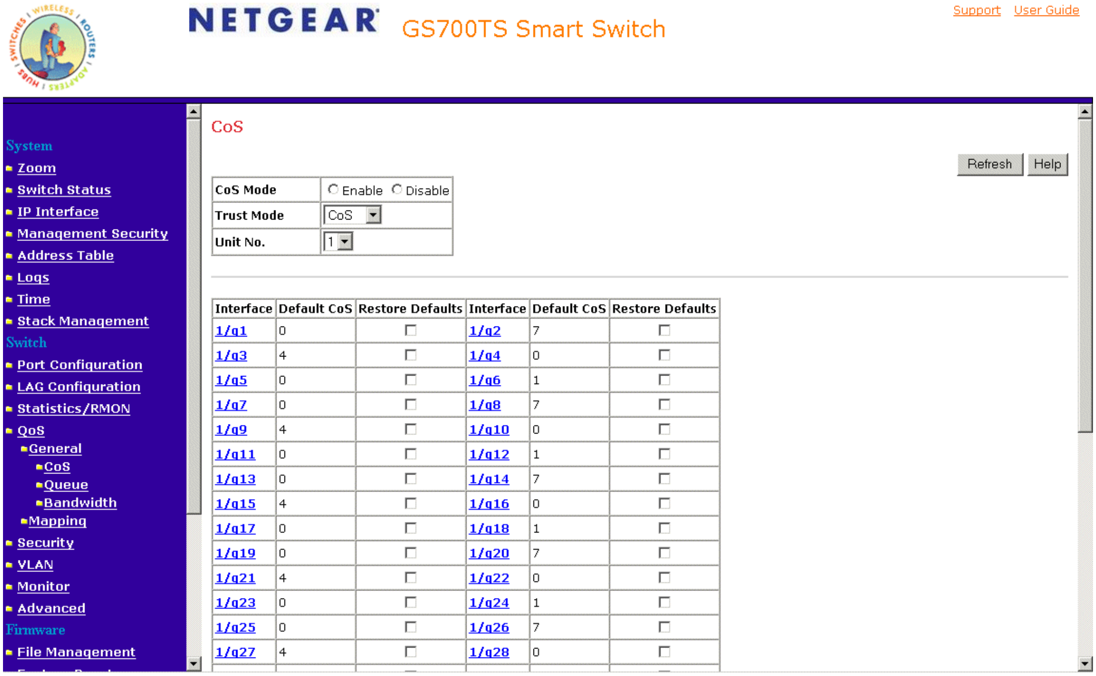
- Defining General QoS Settings
- Defining QoS Queues
- Configuring Bandwidth Settings

Defining General QoS Settings

The *CoS Page* contains information for enabling QoS globally and on specific interfaces. After QoS has been configured, the original device QoS default settings can be reassigned to the interface in the CoS Page.

To enable QoS:

1. Click **QoS** > **General** > **CoS**. The *CoS Page* opens:



CoS

CoS Mode	○ Enable ○ Disable
Trust Mode	CoS
Unit No.	1

Interface	Default CoS	Restore Defaults	Interface	Default CoS	Restore Defaults
1/g1	0	□	1/g2	7	□
1/g3	4	□	1/g4	0	□
1/g5	0	□	1/g6	1	□
1/g7	0	□	1/g8	7	□
1/g9	4	□	1/g10	0	□
1/g11	0	□	1/g12	1	□
1/g13	0	□	1/g14	7	□
1/g15	4	□	1/g16	0	□
1/g17	0	□	1/g18	1	□
1/g19	0	□	1/g20	7	□
1/g21	4	□	1/g22	0	□
1/g23	0	□	1/g24	1	□
1/g25	0	□	1/g26	7	□
1/g27	4	□	1/g28	0	□

Figure 5-62

The *CoS Page* contains the following:

- **CoS Mode** – Determines whether QoS is enabled on the device. The possible field values are:
  – *Enable* – Enables QoS on the device.
  – *Disable* – 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 (VPT) tag value.
  – *DSCP* – Classifies traffic based on the DSCP tag value.
- **Unit No.** – Displays the stacking member for which the QoS information is displayed.

- **Interface** – Displays the interface for which the global QoS parameters are defined.
  - *Port* – Selects the port for which the global QoS parameters are defined.
  - *LAG* – Selects the LAG for which the global QoS parameters are defined.
- **Default CoS** – Determines the default CoS value for incoming packets for which a VLAN tag is not defined.
- **Restore Defaults –** Restores the factory CoS default settings to the selected port.
  - *Checked* – Restores the factory CoS default settings to the ports.
  - *Unchecked*– Maintains the current CoS settings.

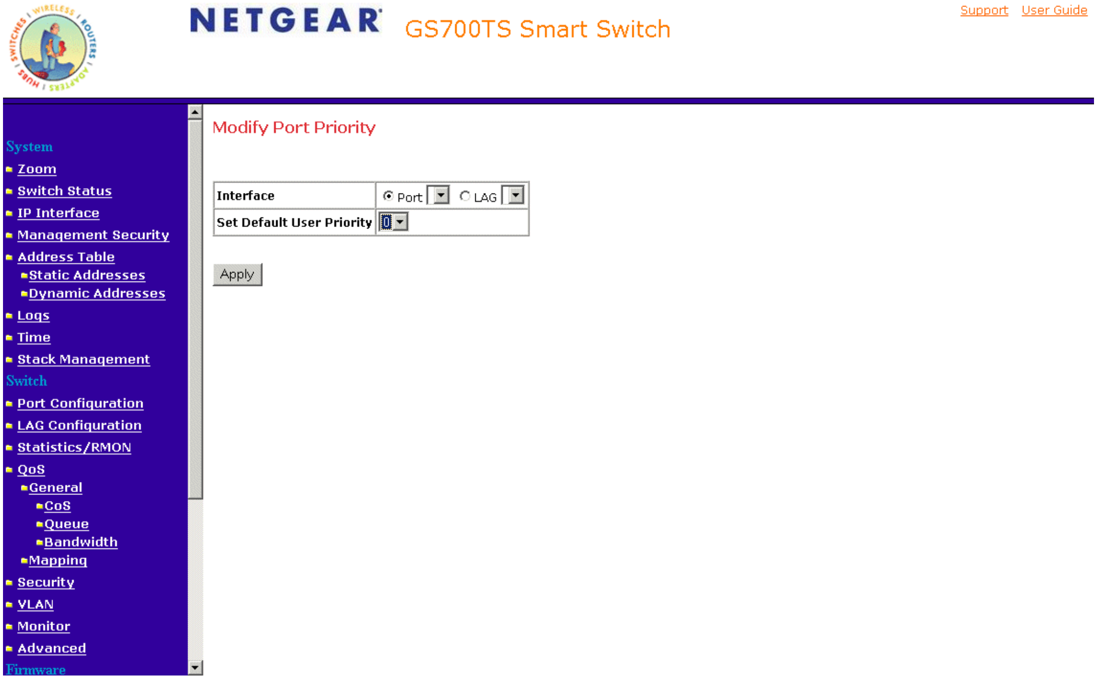
2. Define the relevant fields.

3. Click Apply. Quality of Service is enabled on the device.

To modify QoS:

1. Click **QoS** > **General** > **CoS**. The *CoS Page* opens.

2. Click an interface. The *Modify Port Priority Page* opens:



Modify Port Priority

Interface	● Port ○ LAG
Set Default User Priority	0

Apply

Figure 5-63

In addition to the *CoS Page*, the *Modify Port Priority Page* has the following field:

- **Set Default User Priority** – Sets the default user priority. The possible field values are 0-7. The default CoS value is 0. With the default settings, 0 is the lowest and 7 is the highest priority.

3. Modify the relevant fields.

4. Click Apply. Quality of Service settings are saved on the device.

Defining QoS Queues

The Defining *Queue Page* contains fields for defining the QoS queue forwarding types.

To set the queue settings:

1. Click **QoS** > **General** > **Queue**. The *Queue Page* opens:

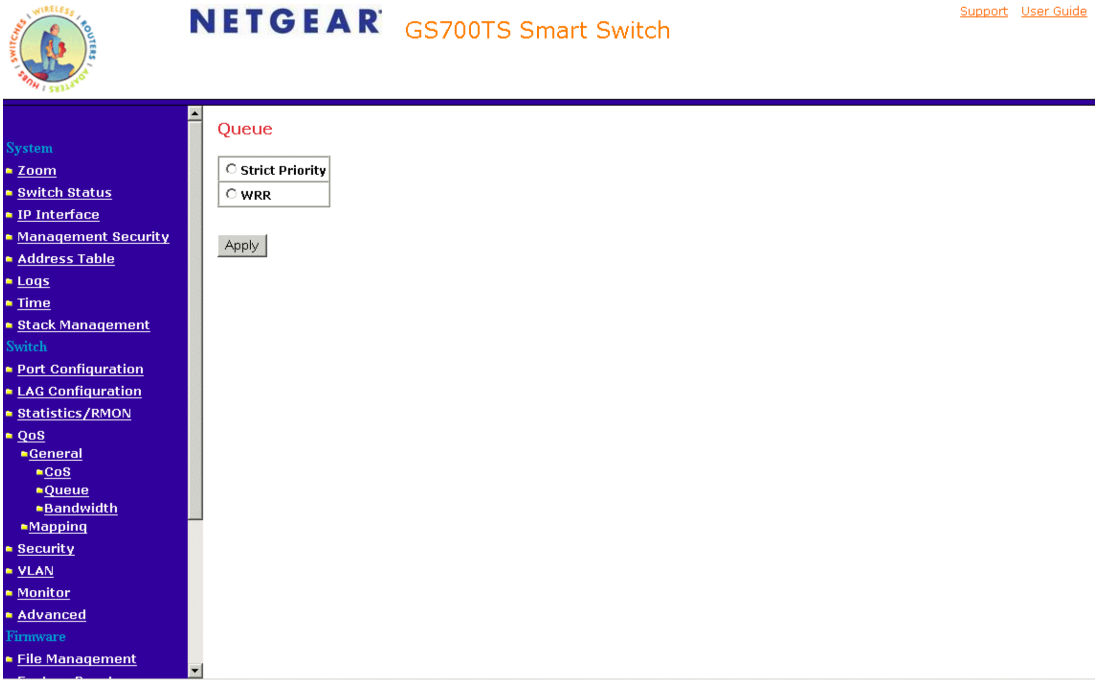


Figure 5-64

The *Queue Page* contains the following fields:

- **Strict Priority** – Specifies whether traffic scheduling is based strictly on the queue priority.
- **WRR** – Assigns WRR weights to queues to prevent a specific application from consuming all of a port's forwarding capability. The queue weights are preconfigured and are set to 0,2,4, and 7.

2. Define the relevant fields.

3. Click Apply. The queue settings are set and the device is updated.

Configuring Bandwidth Settings

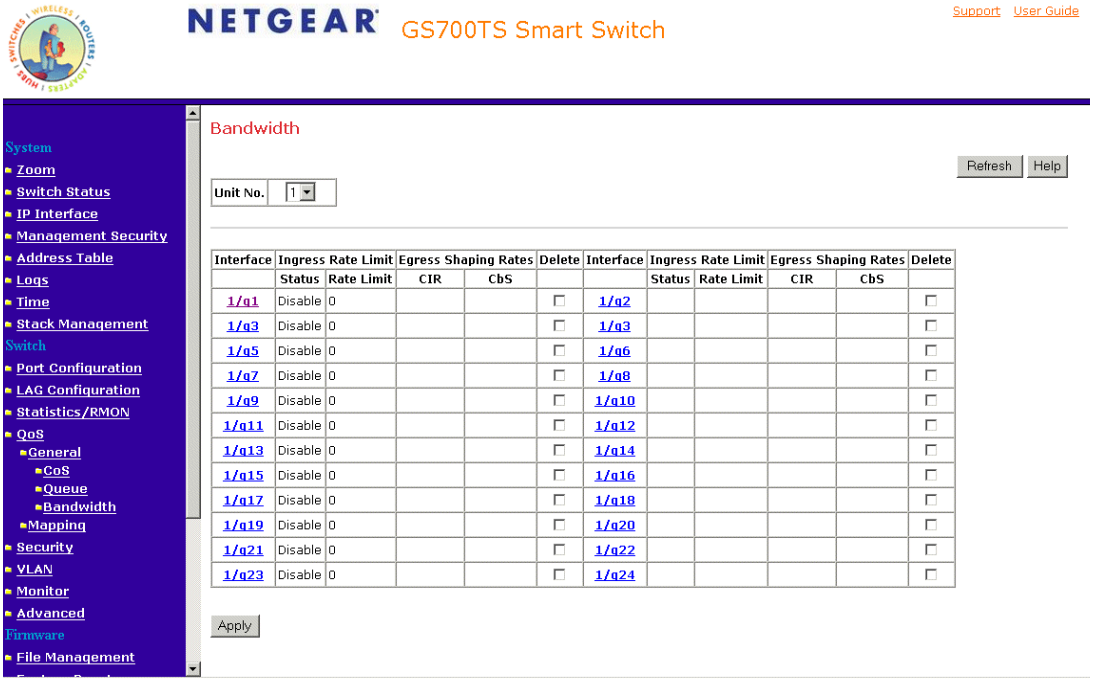
After packets are assigned to a queue, a scheduling scheme can be assigned to an interface, using either:

- **Committed Burst Size** – Indicates the maximum number of data bits transmitted within a specific time interval.
- **Committed Information Rate** – Indicates the rate that data is transmitted. The rate is averaged over a minimum time increment.

The *Bandwidth Page* allows network managers to define the bandwidth settings for a specified egress interface. Modifying queue scheduling affects the queue settings globally. Queue shaping can be based per queue and/or per interface. Shaping is determined by the lower specified value. The queue shaping type is selected in the *Bandwidth Page*.

To define bandwidth settings:

1. Click **QoS** > **General** > **Bandwidth**. The *Bandwidth Page* opens:



Unit No. 1

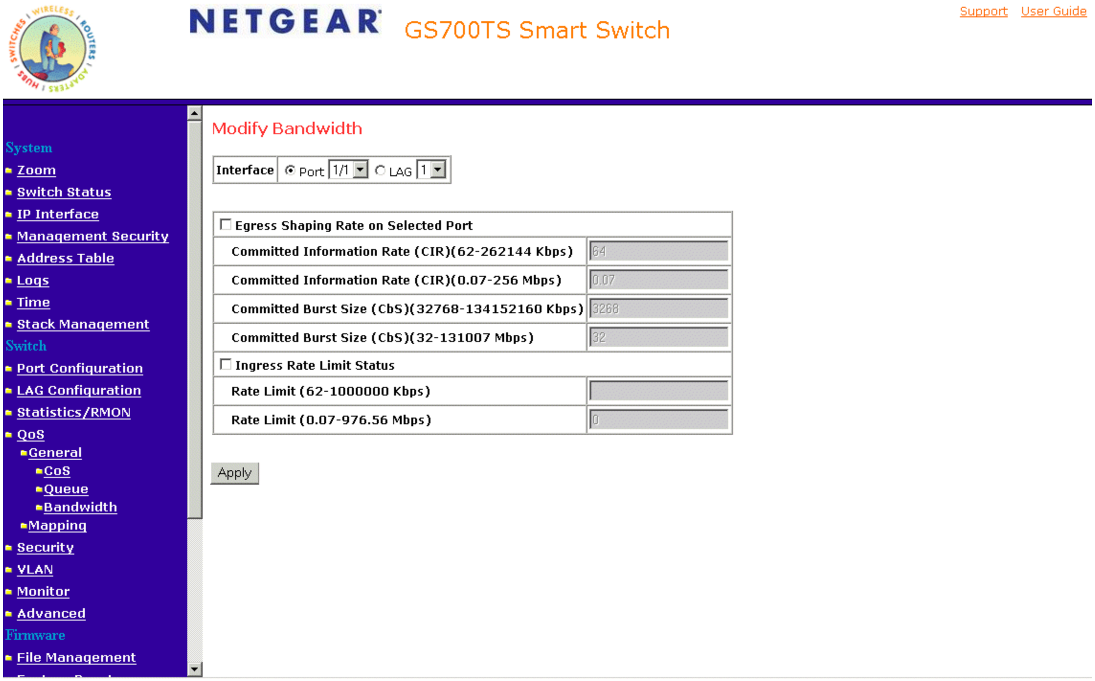
Interface	Ingress Rate Limit		Egress Shaping Rates		Delete	Interface	Ingress Rate Limit		Egress Shaping Rates		Delete
	Status	Rate Limit	CIR	CbS			Status	Rate Limit	CIR	CbS	
1/g1	Disable	0			□	1/g2					□
1/g3	Disable	0			□	1/g3					□
1/g5	Disable	0			□	1/g6					□
1/g7	Disable	0			□	1/g8					□
1/g9	Disable	0			□	1/g10					□
1/g11	Disable	0			□	1/g12					□
1/g13	Disable	0			□	1/g14					□
1/g15	Disable	0			□	1/g16					□
1/g17	Disable	0			□	1/g18					□
1/g19	Disable	0			□	1/g20					□
1/g21	Disable	0			□	1/g22					□
1/g23	Disable	0			□	1/g24					□

Figure 5-65

The *Bandwidth Page* contains the following fields:

- **Unit No.** – Indicated the unit number.
- **Interface** – Indicates the stacking members for which the bandwidth settings are displayed.
- **Ingress Rate Limit Status** – Determines the ingress port bandwidth settings for the selected interface.
  - *Rate Limit* – Defines the interface rate limiting to kilobits per second. The field range is 3500 - 1,000,000 Kbps.
- **Egress Shaping Rate on Selected Port** – Determines the egress port bandwidth settings for the selected interface. The possible field values are:
  - *Committed Information Rate (CIR)* – Defines the CIR. The field range is 62 - 1,000,000.
  - *Committed Burst Size (CBS)* – Defines the CBS. The field range is 64 -1,000,000.
- **Delete** – Deletes the bandwidth settings from the interface. The possible field values are:
  - *Checked* – Deletes the bandwidth settings from the selected interface.
  - *Unchecked* – Maintains the bandwidth settings from the selected interface. This is the default value.

2. Click an interface. The *Modify Bandwidth Page* opens:



Modify Bandwidth

Interface ● Port 1/1 ○ LAG 1

□ Egress Shaping Rate on Selected Port	
Committed Information Rate (CIR)(62-262144 Kbps)	64
Committed Information Rate (CIR)(0.07-256 Mbps)	0.07
Committed Burst Size (CbS)(32768-134152160 Kbps)	3268
Committed Burst Size (CbS)(32-131007 Mbps)	32
□ Ingress Rate Limit Status	
Rate Limit (62-1000000 Kbps)	
Rate Limit (0.07-976.56 Mbps)	0

Figure 5-66

In addition to the *Bandwidth Page*, the *Modify Bandwidth Page* has the following fields:

- **Interface** – Displays the port or LAG name. The possible field values are:
  - *Port No.* – Indicates the port number.
  - *LAG No.* – Indicates the LAG number.
- **Egress Shaping Rate on Selected Port** – Indicates if rate limiting is enabled on the interface. The possible field values are:
  - *Enable* – Enables engress rate limiting on the interface.
  - *Disable* – Disables engress rate limiting on the interface.
- **Committed Information Rate (CIR)** – Defines CIR as the queue shaping type.
- **Committed Burst Size (CbS)** – Defines CBS as the queue shaping type.
- **Ingress Rate Limit Status** – Indicates if rate limiting is defined on the interface. The possible field values are:

  - *Enable* – Enables ingress rate limiting on the interface.
  - *Disable* – Disables ingress rate limiting on the interface.
- **Rate Limit** – Defines the amount of bandwidth assigned to the interface.

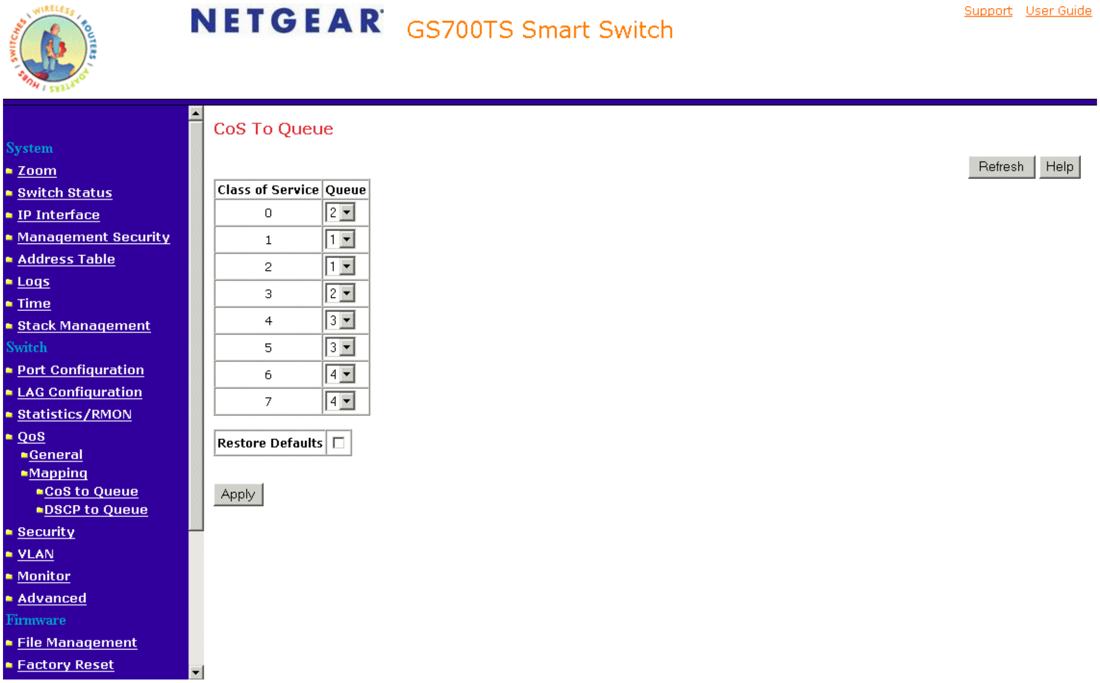
3. Define the relevant fields.
4. Click Apply. The bandwidth settings are saved to interface and the device is updated.

Mapping CoS Values to Queues

The *CoS to Queue Page* contains fields for mapping CoS values to traffic queues.

To map CoS values to queues:

1. Click **QoS** > **Mapping** > **CoS to Queue**. The *CoS to Queue Page* opens:



CoS To Queue

Class of Service	Queue
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

Restore Defaults □

Apply

Figure 5-67

The *CoS to Queue Page* contains the following fields:

- **Class of Service** – Specifies the CoS priority tag values, where 0 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. The lowest priority is 1 and is the highest is 4.
- **Restore Defaults** – Restores the device factory defaults for mapping CoS values to a forwarding queue.

2. Define the relevant fields.

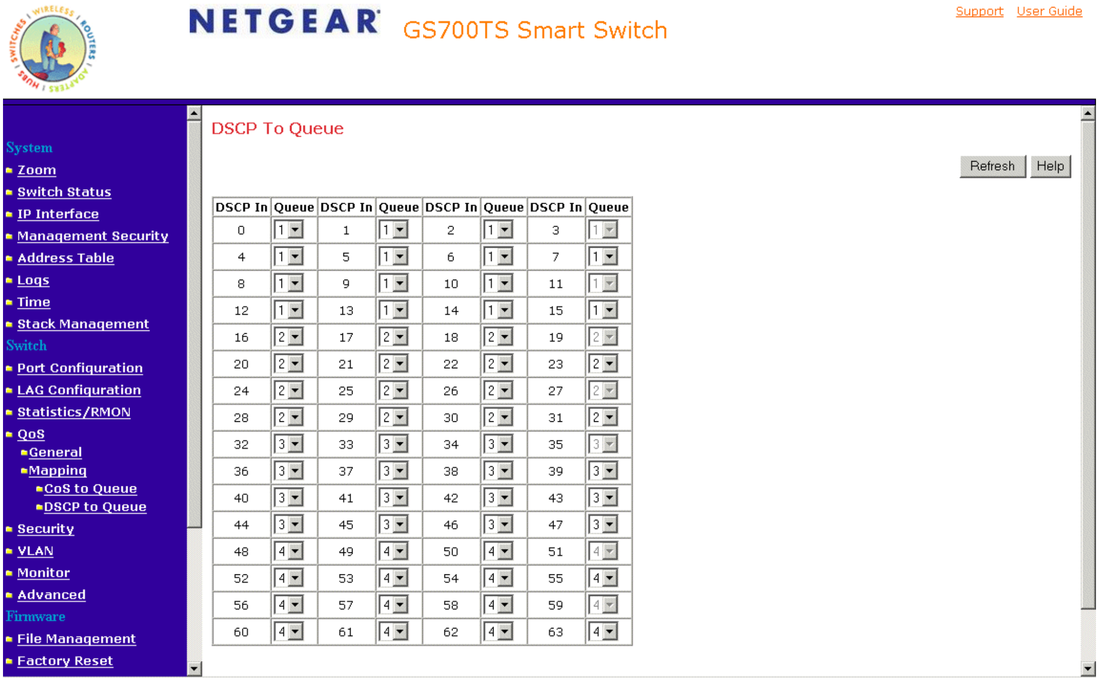
3. Click Apply. The CoS value is mapped to a queue and the device is updated.

Mapping DSCP Values to Queues

The *DSCP to Queue Page* contains fields for mapping DSCP settings to traffic queues. For example, a packet with a DSCP tag value of 3 can be assigned to queue 2.

To map CoS values to queues:

1. Click **QoS > Mapping > DSCP to Queue**. The *DSCP to Queue Page* opens:



DSCP To Queue

DSCP In	Queue	DSCP In	Queue	DSCP In	Queue	DSCP In	Queue
0	1	1	1	2	1	3	1
4	1	5	1	6	1	7	1
8	1	9	1	10	1	11	1
12	1	13	1	14	1	15	1
16	2	17	2	18	2	19	2
20	2	21	2	22	2	23	2
24	2	25	2	26	2	27	2
28	2	29	2	30	2	31	2
32	3	33	3	34	3	35	3
36	3	37	3	38	3	39	3
40	3	41	3	42	3	43	3
44	3	45	3	46	3	47	3
48	4	49	4	50	4	51	4
52	4	53	4	54	4	55	4
56	4	57	4	58	4	59	4
60	4	61	4	62	4	63	4

Figure 5-68

The *DSCP to Queue Page* contains the following fields:

- **DSCP In** – Displays the incoming packet's DSCP value.
- **Queue** – Specifies the traffic-forwarding queue to which the DSCP priority is mapped. Four traffic priority queues are supported.

2. Define the relevant fields.
3. Click Apply. The DSCP value is mapped to a queue and the device is updated.

Configuring SNMP Security

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports the following SNMP versions:

- SNMP v1, v2c.

- SNMP v3.

The SNMP agents maintain a list of variables that 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 strings control access rights to the SNMP agents.

SNMP v3 applies access control and a new traps mechanism. In addition, User Security Model (USM) parameters are defined for SNMPv3, including:

- **Authentication** – Provides data integrity and data origin authentication.
- **Privacy** – Protects against the disclosure of message content. Cipher Block-Chaining (CBC) is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However, privacy cannot be enabled without authentication.
- **Timeliness** – Protects against message delay or message redundancy. The SNMP agent compares the incoming message to the message time information.
- **Key Management** – Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on Object IDs (OIDs).

OIDs are used by the system to manage device features.

SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

The device generates copy traps.

This section contains the following topics:

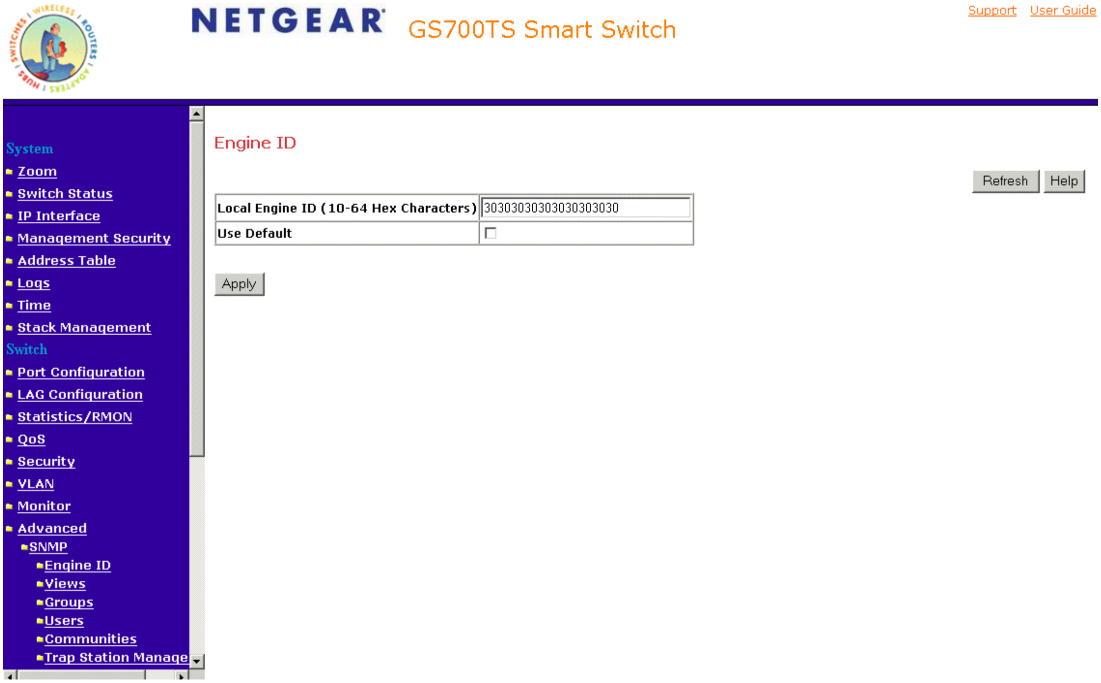
- Defining the Engine ID
- Defining SNMP Users
- Defining SNMP Views
- Defining SNMP Communities
- Trap Station Management
- Trap Filter Settings

Defining the Engine ID

The *Engine ID Page* allows network managers to define the SNMP Engine ID and allows network managers to assign the default parameters to SNMP.

To define the Local Engine ID:

1. Click **Advanced** > **SNMP** > **Engine ID**. The *Engine ID Page* opens:



Engine ID

Local Engine ID (10-64 Hex Characters)	30303030303030303030
Use Default	□

Figure 5-69

The *Engine ID Page* contains the following fields:

- **Local Engine ID (10-64 Hex Characters)** – Displays the local device Engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte digit can be separated by a period or a colon. The Engine ID must be defined before SNMPv3 is enabled.
- **Use Default** – Uses the device-generated Engine ID. The default Engine ID is based on the device MAC address and is defined per standard as:
  - *First 4 octets* – first bit = 1, the rest is IANA Enterprise number.
  - *Fifth octet* – Set to 3 to indicate the MAC address that follows.

– *Last 6 octets* – MAC address of the device.

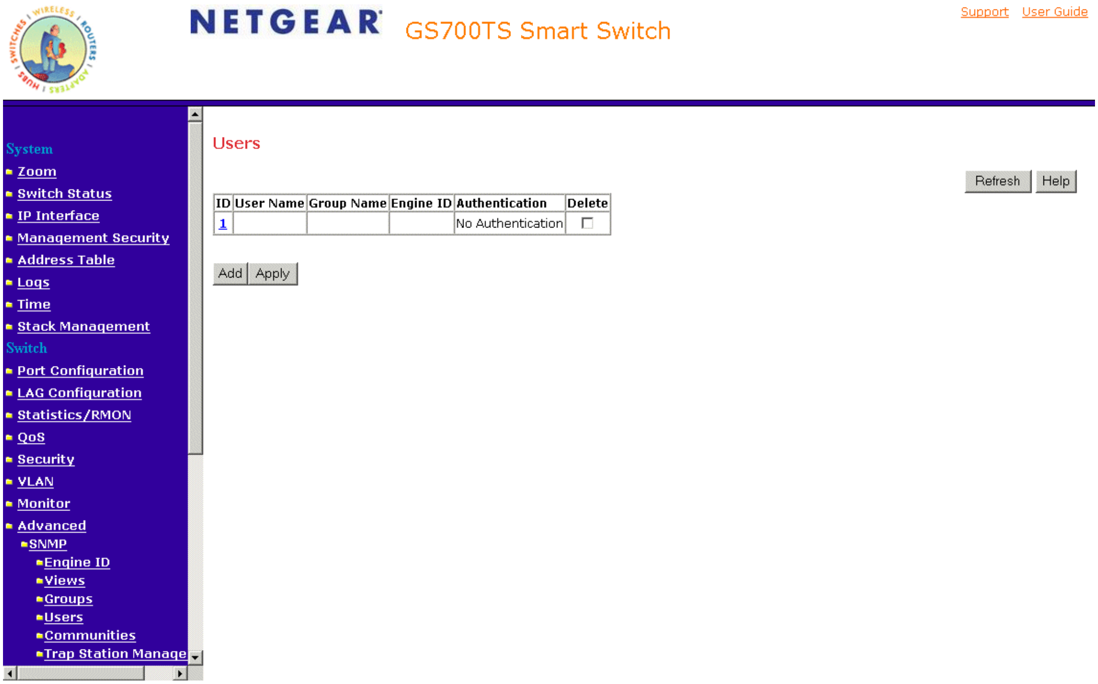
2. Define the relevant fields.
3. Click Apply. The SNMP global security parameters are set and the device is updated.

Defining SNMP Users

The *SNMP Users 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 SNMP group:

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



ID	User Name	Group Name	Engine ID	Authentication	Delete
1				No Authentication	□

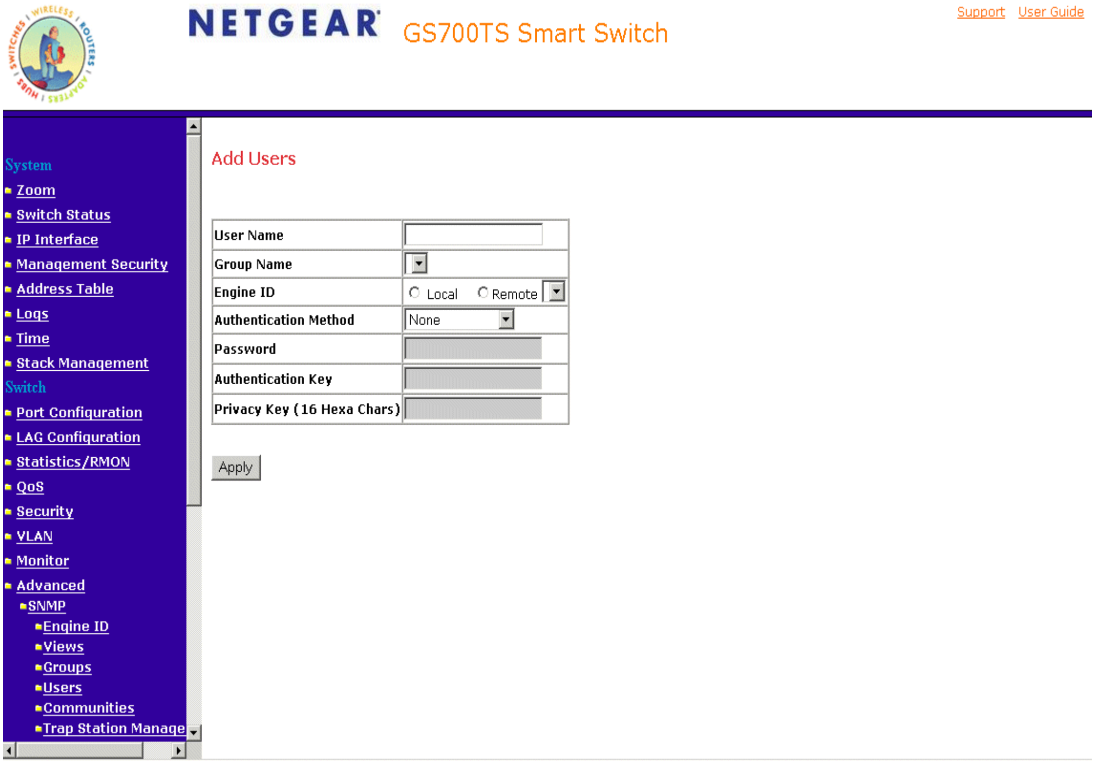
Figure 5-70

The *SNMP Users Page* contains the following fields:

- **ID** – Indicates the stacking number.
- **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. The possible field values are:
  - *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.
  - *No Authentication* – No user authentication is used.
- **Delete** – Removes users from a specified group. The possible field values are:
  - *Checked* – Removes the selected user.
  - *Unchecked* – Maintains the list of users.

2. Click Add. The Add SNMP Users Page opens:



Add Users

User Name	
Group Name	▼
Engine ID	○ Local ○ Remote ▼
Authentication Method	None ▼
Password	
Authentication Key	
Privacy Key (16 Hexa Chars)	

Figure 5-71

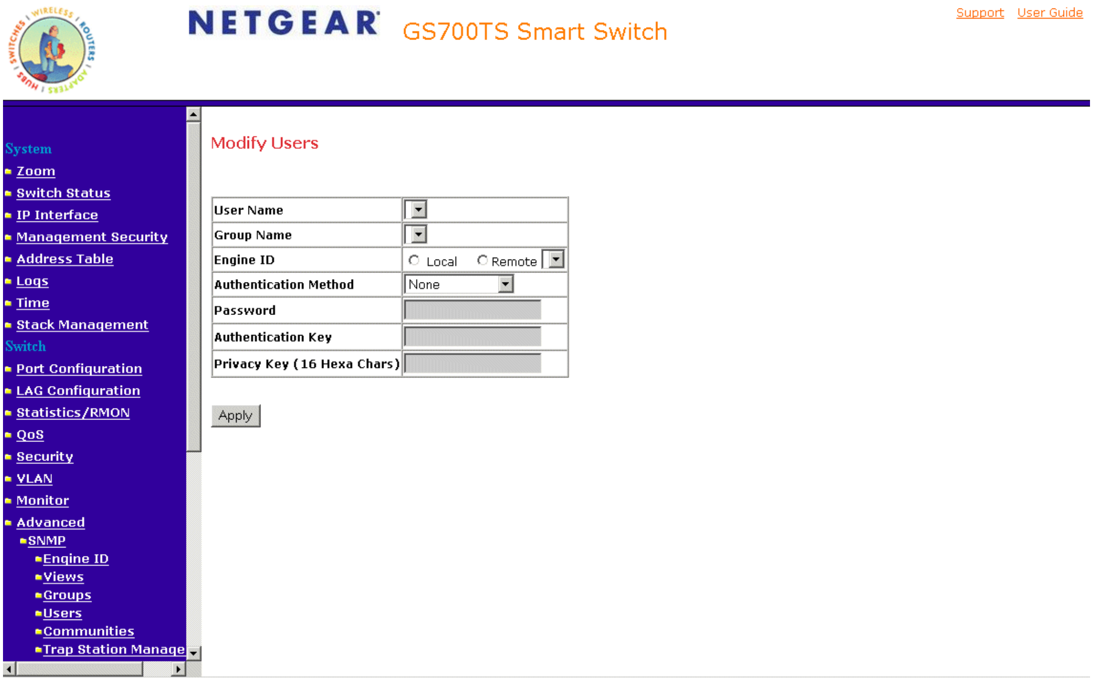
In addition to the fields in the *SNMP Users Page*, the *Modify Users Page* contains the following additional fields:

- **Password** – Defines the password for the group member.
- **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 (16 Hexa Chars)** – Defines the privacy key (LSB). If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 36 bytes redefined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.

3. Define the relevant fields.
4. Click Apply. The SNMP user is defined and the device is updated.

To modify a SNMP group:

1. Click **Advanced** > **SNMP** > **Users**. The *SNMP Users Page* opens.
2. Select a SNMP group. The *Modify Users Page* opens:



Modify Users

User Name	
Group Name	
Engine ID	○ Local ○ Remote
Authentication Method	None
Password	
Authentication Key	
Privacy Key (16 Hexa Chars)	

Apply

Figure 5-72

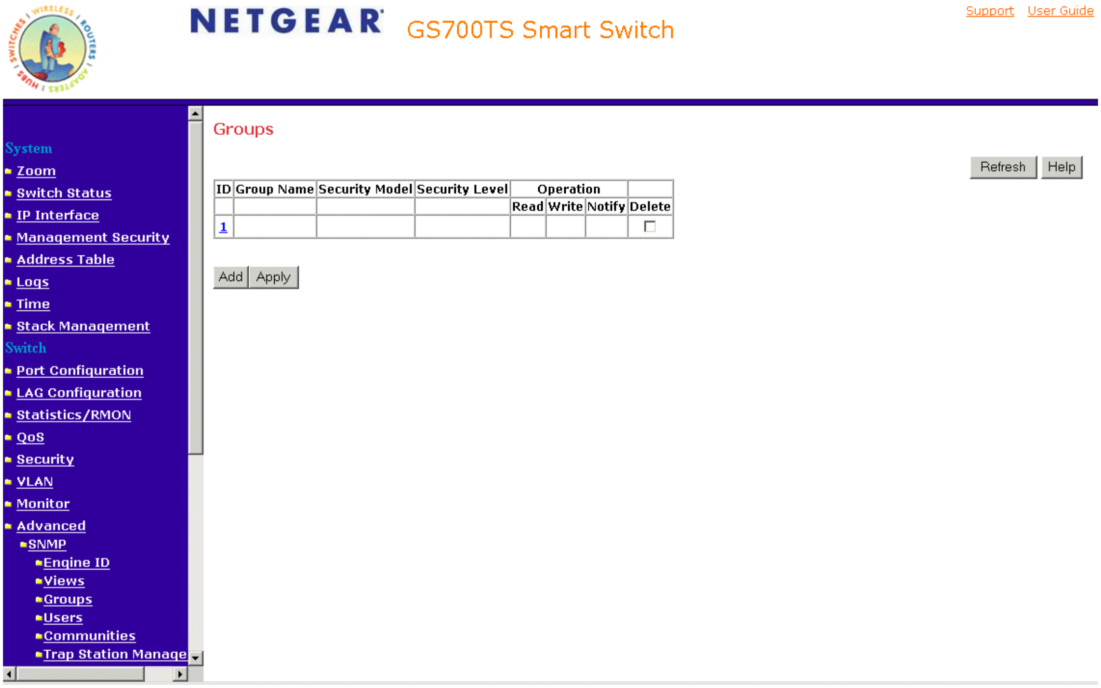
3. Modify the relevant fields.
4. Click Apply. The SNMP user is defined and the device is updated.

Defining SNMP Groups

The *Groups 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 **Advanced** > **SNMP** > **Groups**. The *Groups Page* opens:



ID	Group Name	Security Model	Security Level	Operation			
				Read	Write	Notify	Delete
1							☐

Figure 5-73

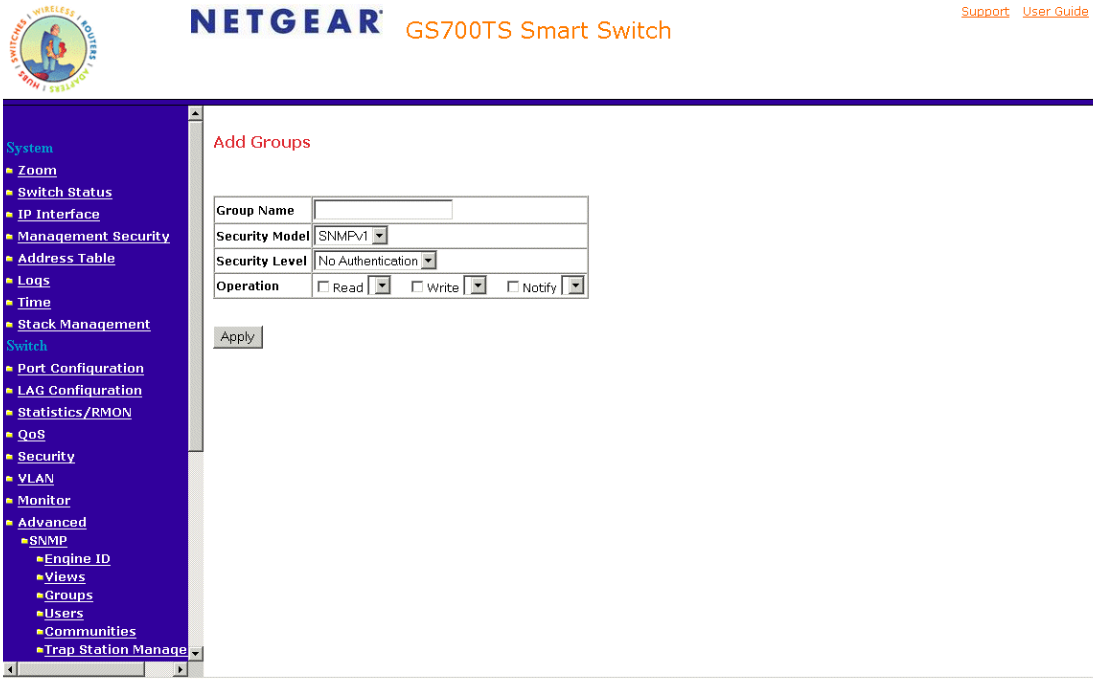
The *Groups Page* contains the following fields:

- **ID** – Indicates the stacking number.
- **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.
  - *SNMPv2c* – SNMPv2c 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. Changes cannot be made to the assigned SNMP view.
  - *Write* – Management access is read-write. Changes can be made to the assigned SNMP view.
  - *Notify* – Sends traps for the assigned SNMP view.
  - *Delete* – Deletes the SNMP group.

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



Add Groups

Group Name	
Security Model	SNMPv1
Security Level	No Authentication
Operation	□ Read □ Write □ Notify

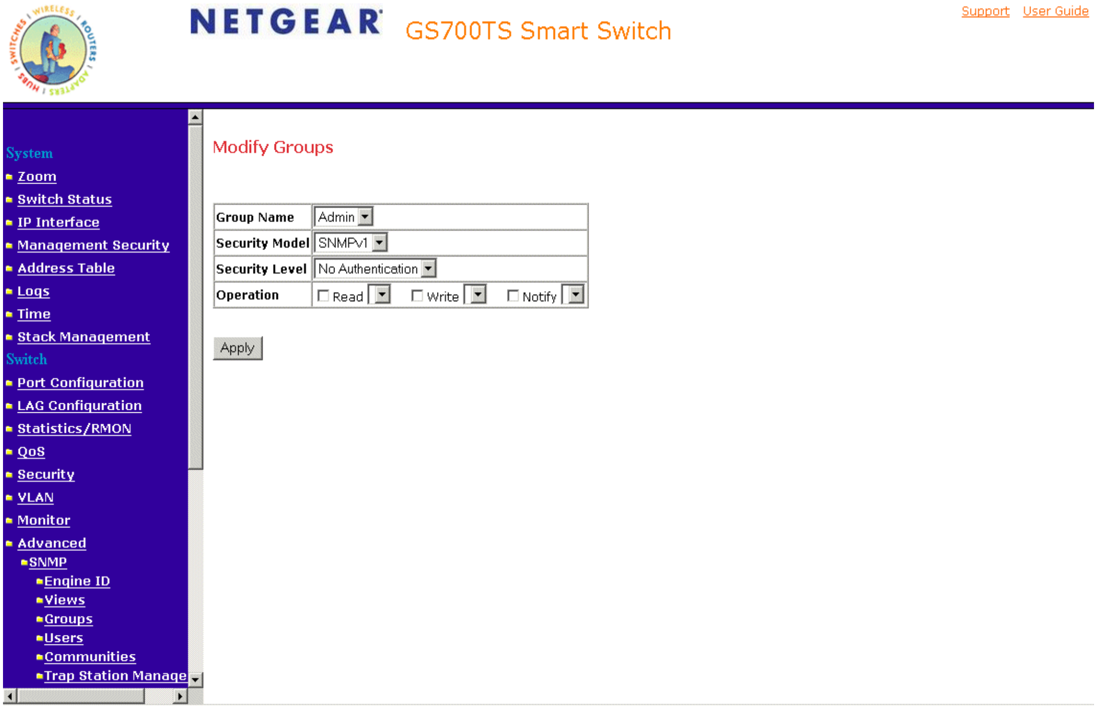
Figure 5-74

3. Define the relevant fields.

4. Click Apply. The SNMP group profile is added and the device is updated.

To modify SNMP Group settings:

1. Click **Advanced** > **SNMP** > **Groups**. The *Modify Groups Page* opens.
2. Click the ID of the group you want to modify. The *Modify Groups Page* opens:



Modify Groups

Group Name	Admin
Security Model	SNMPv1
Security Level	No Authentication
Operation	□ Read □ Write □ Notify

Apply

Figure 5-75

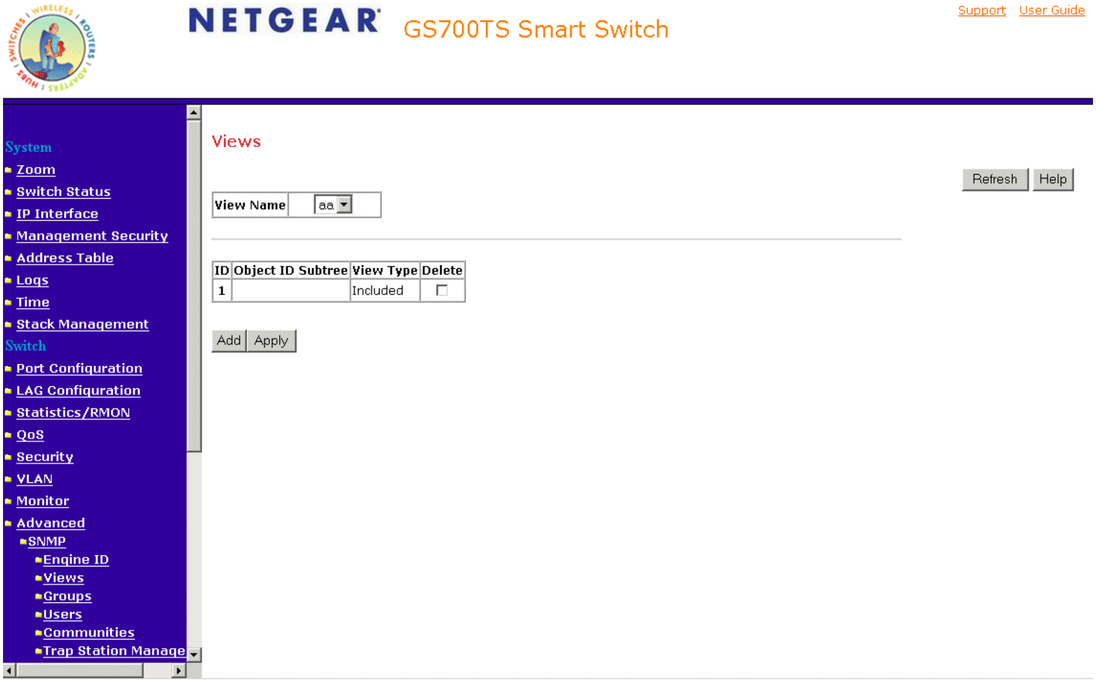
3. Modify the relevant fields.
4. Click Apply. The SNMP group profile is modified and the device is updated.

Defining SNMP Views

SNMP Insert space views provide or block access to device features or portions of features. For example, a view can be defined which provides that SNMP group A has Read Only (R/O) access to multicast groups, while SNMP group B has Read-Write (R/W) access to multicast groups. Feature access is granted via the MIB name or MIB Object ID.

To define SNMP views:

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



View Name: aa

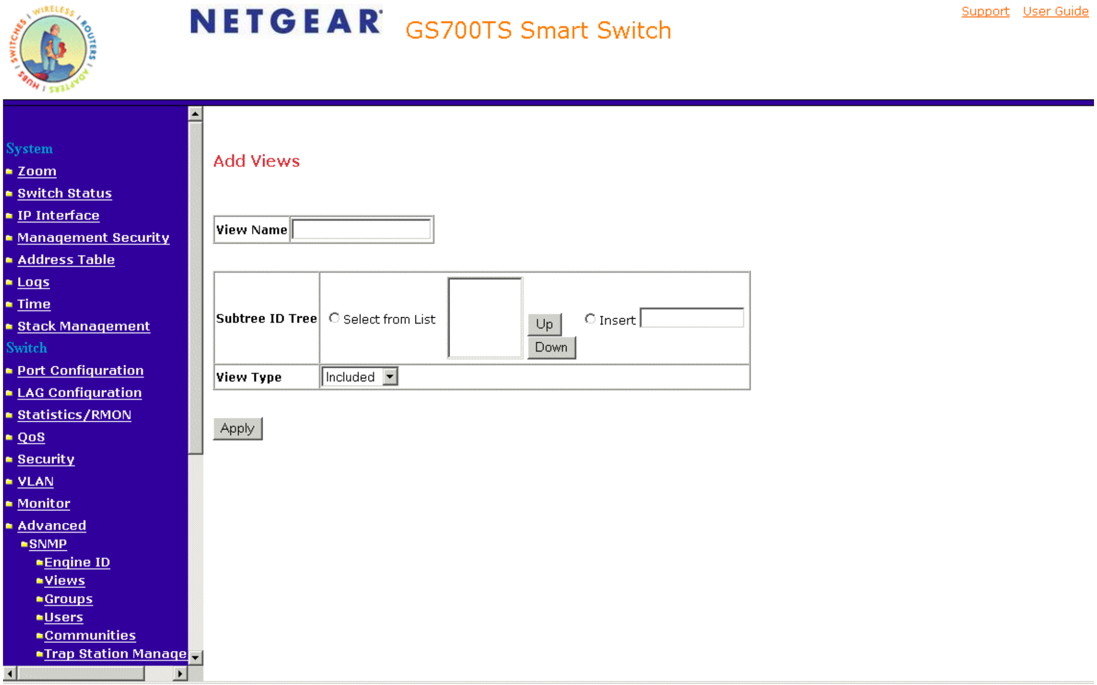
ID	Object ID Subtree	View Type	Delete
1		Included	☐

Figure 5-76

The *Views Page* contains the following fields:

- **View Name** – Displays the user-defined views. The view name can contain a maximum of 30 alphanumeric characters.
- **ID** – Indicates the stacking number.
- **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 will be included in or excluded from the selected SNMP view.
- **Delete** – Deletes the currently selected view. The possible field values are:
  - *Checked* – Removes the selected view.
  - *Unchecked* – Maintains the list of views.

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



View Type: Included

Figure 5-77

3. Define the relevant fields.

4. Click Apply. The view is defined and the device is updated.

Defining SNMP Communities

Access rights are managed by defining communities in the SNMP Communities Page. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c.

The *Communities Page* is divided into the following tables:

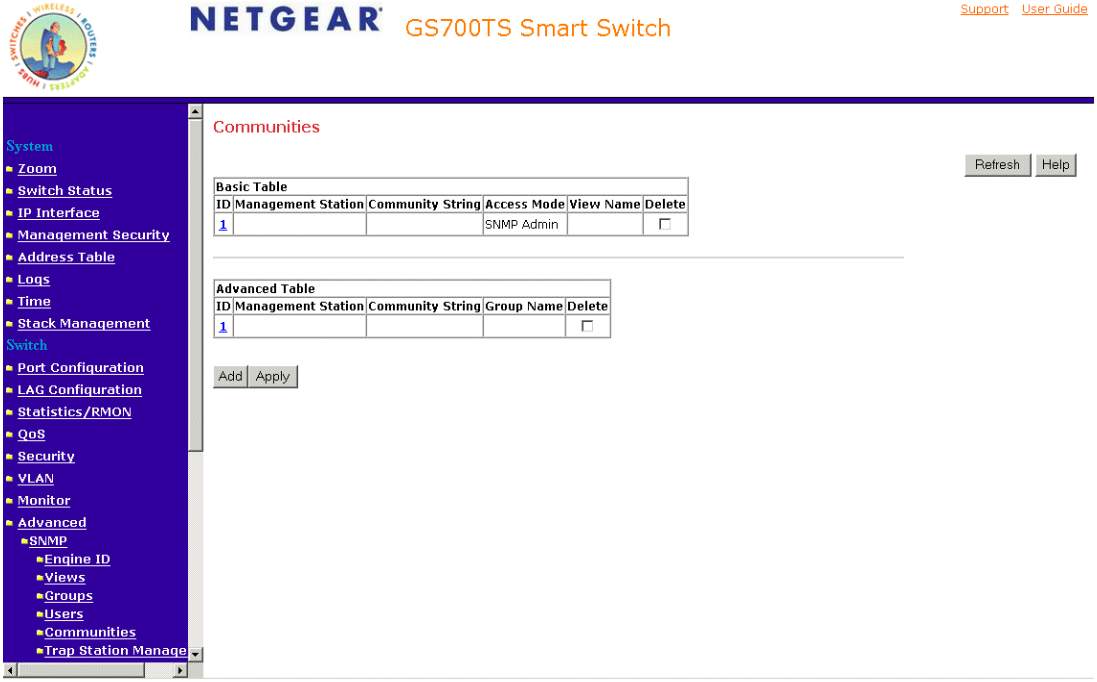
- **SNMP Communities Basic Table**. The SNMP Communities Basic Table contains the following fields when using SNMPv1 and SNMPv3:
  - **ID** – Indicates the table entry number.
  - **Management Station** – Displays the management station IP address for which the basic SNMP community is defined.

- **Community String** – Defines the password 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. Changes cannot be made to the community.
  - *Read Write* – Management access is read-write. 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.
- **Delete** – Removes a community. The possible field values are:
  - *Checked* – Removes the selected SNMP community.
  - *Unchecked* – Maintains the SNMP communities.

- **SNMP Communities Advanced Table.** The SNMP Communities Advanced Table contains the following fields:
  - **ID** – Indicates the table entry number.
  - **Management Station** – Displays the management station IP address for which the advanced SNMP community is defined.
  - **Community String** – Defines the password used to authenticate the management station to the device.
  - **Group Name** – Defines advanced SNMP community group names.
  - **Delete** – Removes a community. The possible field values are:
    - *Checked* – Removes the selected SNMP communities.
    - *Unchecked* – Maintains the SNMP communities.

To define SNMP communities:

1. Click **Advanced** > **SNMP** > **Communities**. The *Communities Page* opens:



Communities

Basic Table

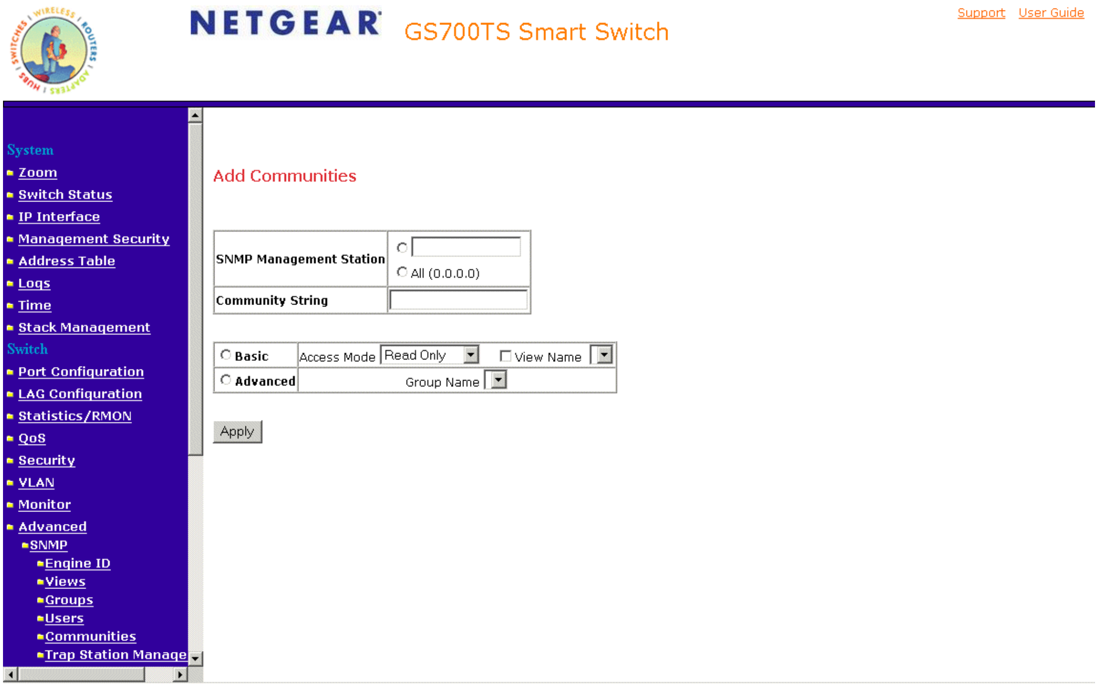
ID	Management Station	Community String	Access Mode	View Name	Delete
1			SNMP Admin		□

Advanced Table

ID	Management Station	Community String	Group Name	Delete
1				□

Figure 5-78

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



Add Communities

SNMP Management Station	○ ○ All (0.0.0.0)
Community String	

○ Basic	Access Mode Read Only ▾	□ View Name ▾
○ Advanced	Group Name ▾	

Apply

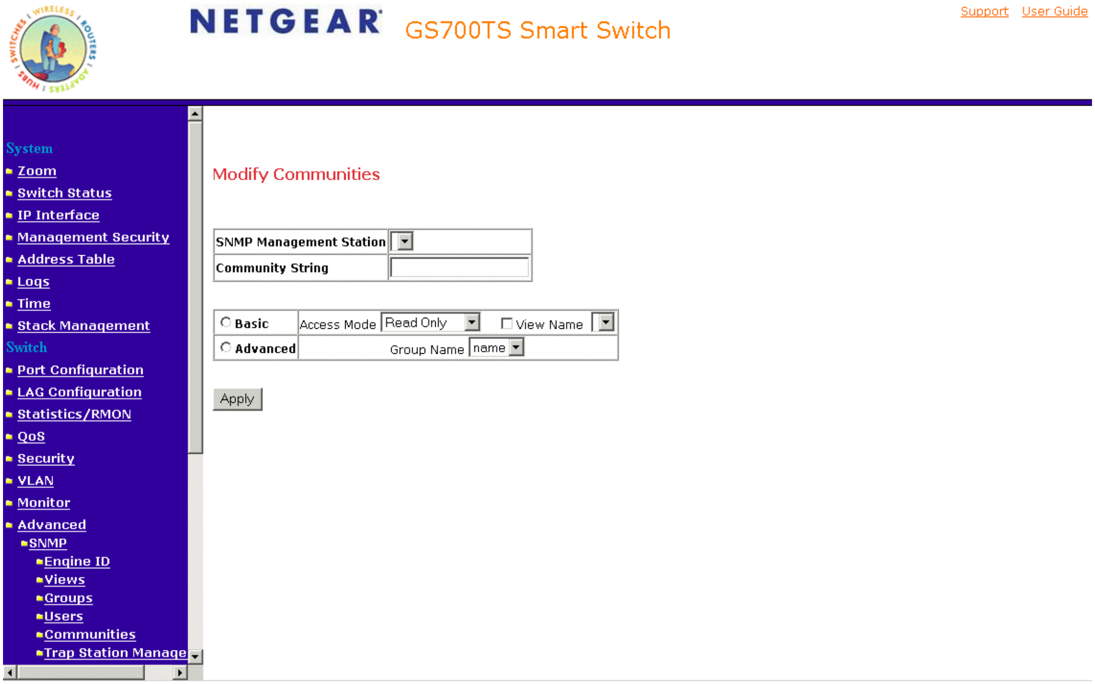
Figure 5-79

3. Define the relevant fields.

4. Click Apply. The SNMP community is added and the device is updated.

To modify SNMP community settings:

1. Click **Advanced** > **SNMP** > **Communities**. The *Communities Page* opens.
2. Click an interface in the field. The *Modify Communities Page* opens:



Modify Communities

SNMP Management Station	
Community String	

○ Basic	Access Mode Read Only	□ View Name
○ Advanced	Group Name name	

Figure 5-80

3. Modify the relevant fields.
4. Click Apply. The SNMP community is modified and the device is updated.

Trap Station Management

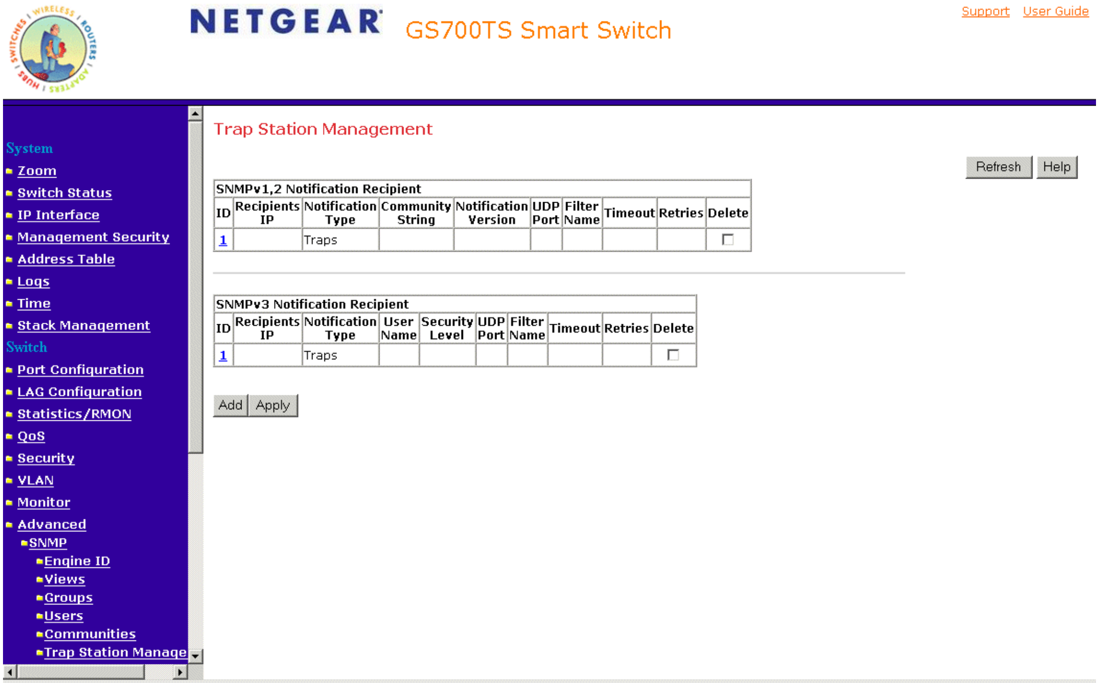
The Trap Station Management Page contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters

- Providing Access Control Checks

To define trap station management:

1. Click **Advanced > SNMP > Trap Station Management.** The *Trap Station Management Page* opens:



Trap Station Management

SNMPv1,2 Notification Recipient

ID	Recipients IP	Notification Type	Community String	Notification Version	UDP Port	Filter Name	Timeout	Retries	Delete
1		Traps							☐

SNMPv3 Notification Recipient

ID	Recipients IP	Notification Type	User Name	Security Level	UDP Port	Filter Name	Timeout	Retries	Delete
1		Traps							☐

Figure 5-81

The *Trap Station Management Page* is divided into the following tables:

- *SNMPv1, 2c Notification Recipient*
- *SNMPv3 Notification Recipient*

SNMPv1, 2c Notification Recipient

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

- **ID** – Indicates the stacking number.
- **Recipients IP** – Displays the IP address to which the traps are sent.
- **Notification Type** – Displays the notification sent. The possible field values are:

  - *Traps* – Indicates traps are sent.
  - *Inform* – Indicates informs are sent.
- **Community String** – Displays the community string of the trap manager.
- **Notification Version** – Displays the trap type. The possible field values are:
  - *SNMP V1* – Indicates that SNMP Version 1 traps are sent.
  - *SNMP V2c* – Indicates that SNMP Version 2 traps are sent.
- **UDP Port** – Displays the UDP port used to send notifications. 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 re-sending informs. The default is 15 seconds.
- **Retries** – Indicates the amount of times the device re-sends an inform request. The default is 3 seconds.
- **Delete** – Removes the currently selected recipient. The possible field values are:
  - *Checked* – Removes the selected recipient from the list of recipients.
  - *Unchecked* – Maintains the list of recipients.

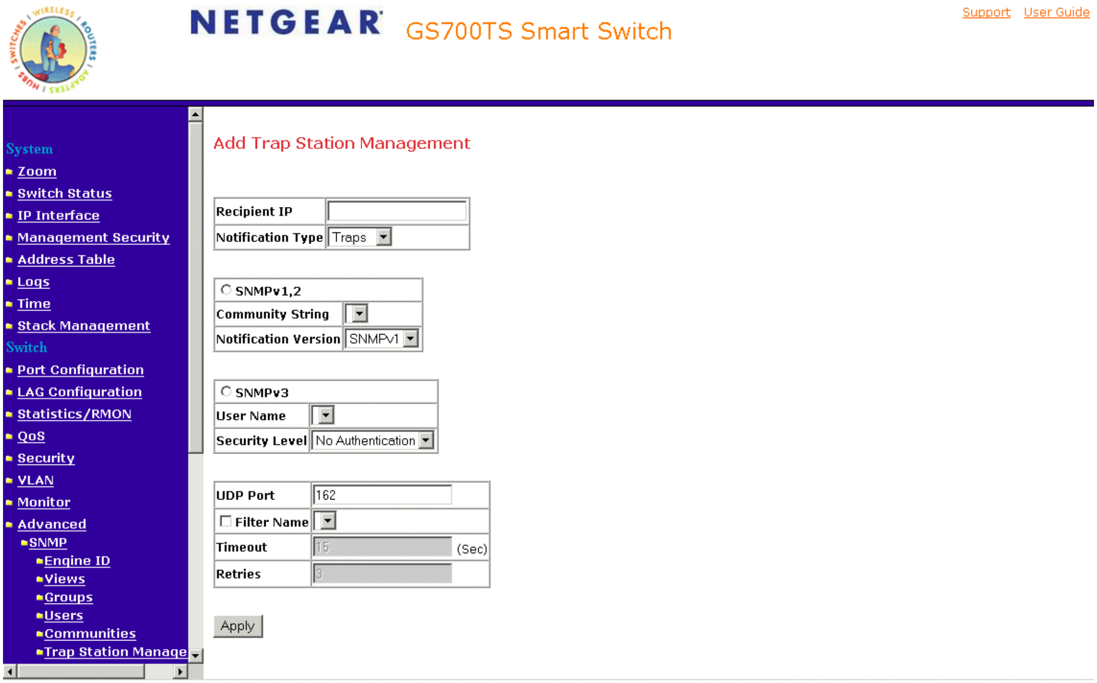
SNMPv3 Notification Recipient

The SNMPv3 Notification Recipient table contains the following fields:

- **ID** – Indicates the stacking number.
- **Recipient IP** – Displays the IP address to which the traps are sent.
- **Notification Type** – Displays the type of notification sent. The possible field values are:
  - *Traps* – 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** – 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 (seconds) the device waits before resending informs. The field range is 1-300. The default is 10 seconds.
- **Retries** – The amount of times the device resends an inform request. The field range is 1-255. The default is 3.
- **Delete** – Removes the currently selected recipient. The possible field values are:
  - *Checked* – Removes the selected recipient from the list of recipients.
  - *Unchecked* – Maintains the list of recipients.

2. Click Add. The *Add Trap Station Management Page* opens:



Add Trap Station Management

Recipient IP	
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	

Apply

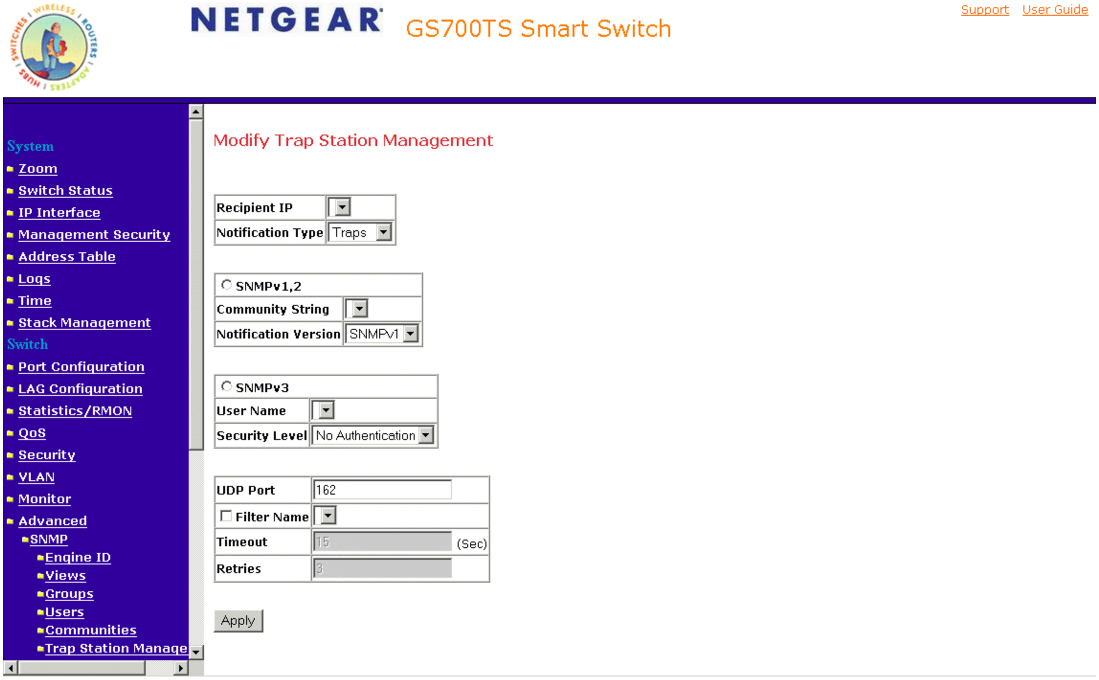
Figure 5-82

3. Define the relevant fields.

4. Click Apply. The SNMP Notification recipients are defined and the device is updated.

To modify trap station management:

1. Click **Advanced > SNMP > Trap Station Management.** The *Trap Station Management Page* opens.
2. Click an ID. The *Modify Trap Station Management Page* opens:



Modify Trap Station Management

Recipient IP	
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

Figure 5-83

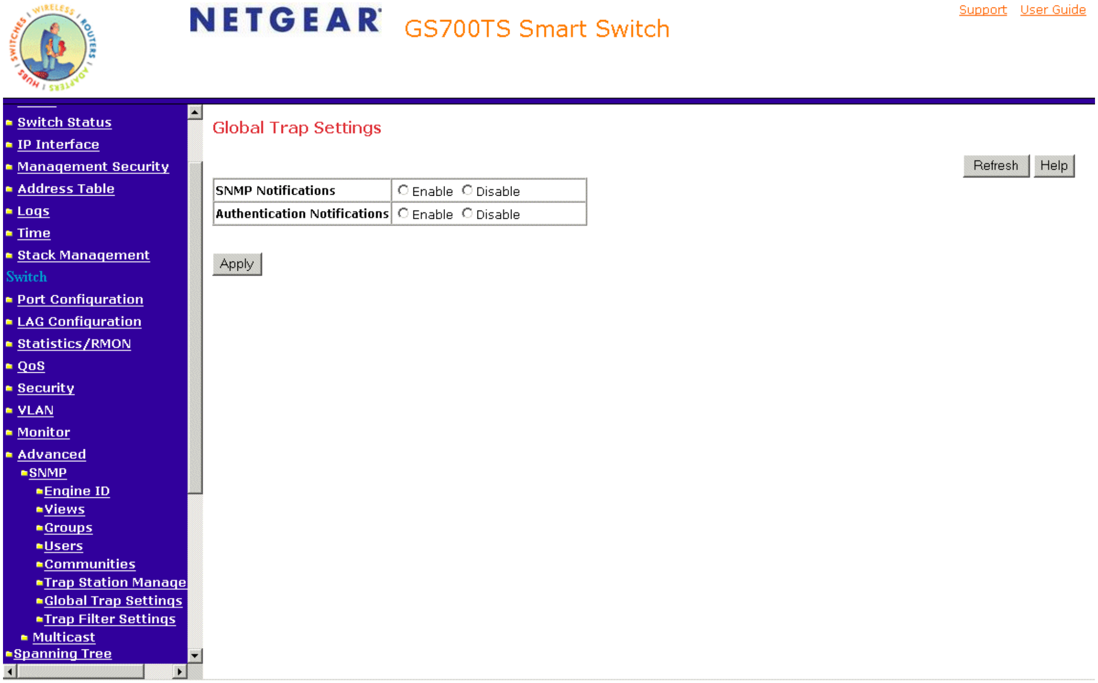
3. Modify the relevant fields.
4. Click Apply. The SNMP Notification recipients are defined and the device is updated.

Global Trap Settings

The *Global Trap Settings Page* contains parameters for defining SNMP notification parameters.

To define SNMP notification global parameters:

1. Click **Advanced > SNMP > Global Trap Settings**. The *Global Trap Settings Page* opens:



Global Trap Settings

SNMP Notifications	○ Enable ○ Disable
Authentication Notifications	○ Enable ○ Disable

Figure 5-84

The *Global Trap Settings Page* contains the following fields:

- **SNMP Notifications** – Specifies whether the device can send SNMP notifications. The possible field values are:
  - *Enable* – Enables SNMP notifications.
  - *Disable* – Disables SNMP notifications.
- **Authentication Notifications** – Specifies whether SNMP authentication failure notification is enabled on the device. The possible field values are:
  - *Enable* – Enables the device to send authentication failure notifications.
  - *Disable* – Disables the device from sending authentication failure notifications.

2. Define the relevant fields.

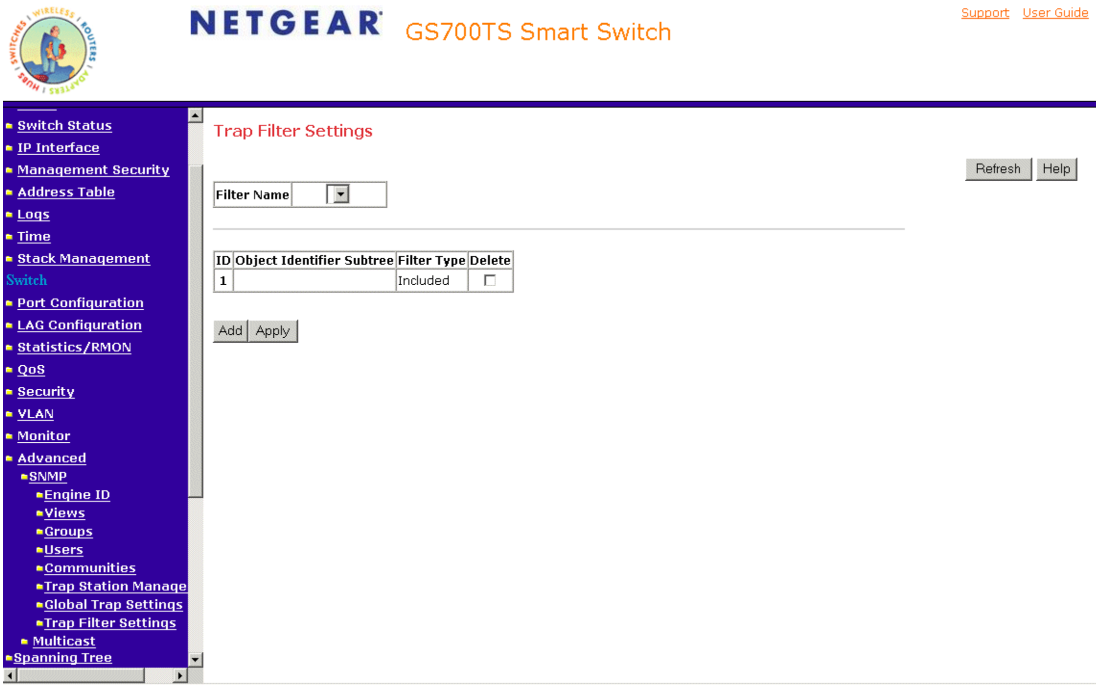
3. Click Apply. The SNMP notification properties are defined and the device is updated.

Trap Filter Settings

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

To define SNMP Trap Filter settings:

1. Click **Advanced > SNMP > Trap Filter Settings**. The *Trap Filter Settings Page* opens:



Trap Filter Settings

Filter Name

ID	Object Identifier Subtree	Filter Type	Delete
1		Included	☐

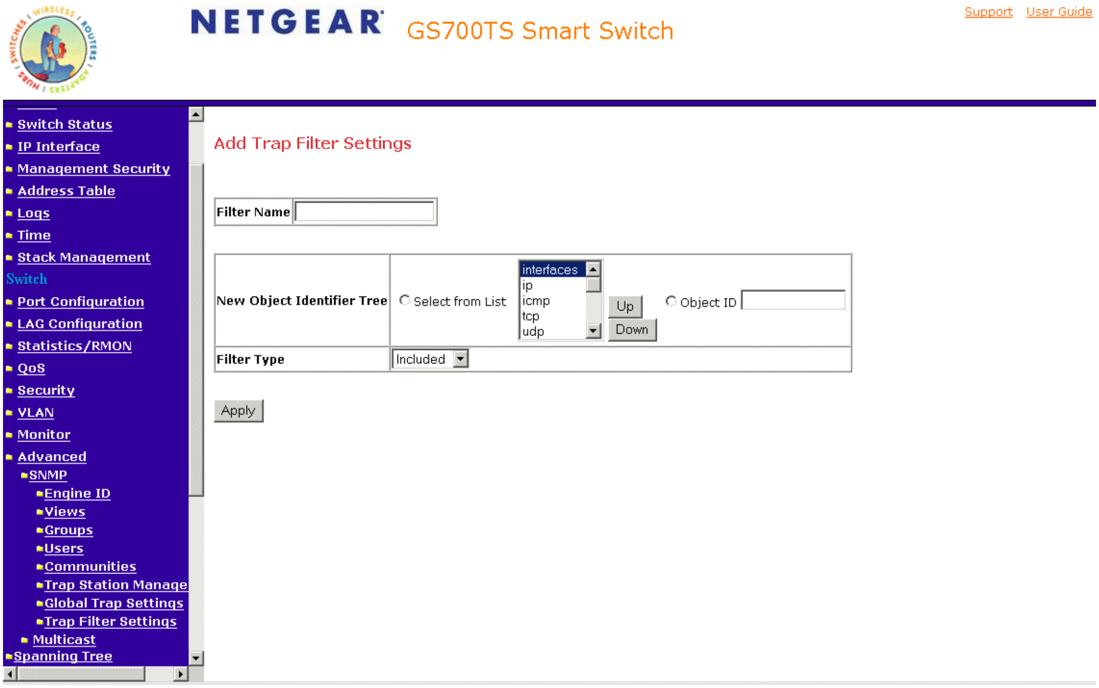
Figure 5-85

The *Trap Filter Settings Page* contains the following fields:

- **Filter Name** – Contains a list of user-defined notification filters.
- **ID** – Indicates the Trap Filter Settings Table entry number.
- **Object Identifier Subtree** – 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. OIDs are selected from either the Select from field or the Object ID field.
- **Filter Type** – Indicates whether to send traps or informs relating to the selected OID.
  – *Excluded* – Does not send traps or informs.

  - *Included* – Sends traps or informs.
- **Delete** – The possible field values are:
  - *Checked* – Deletes the selected filter.
  - *Unchecked* – Maintains the list of filters.

2. Click Add. The *Add Trap Filter Settings Page* opens:



Add Trap Filter Settings

Filter Name			
New Object Identifier Tree	○ Select from List	interfaces ip icmp tcp udp	○ Object ID
Filter Type	Included		

Figure 5-86

3. Define the relevant fields.
4. Click Apply. The SNMP Trap filter is defined and the device is updated.

Configuring Multicast Forwarding

Multicast forwarding allows a single packet to be forwarded to multiple destinations. L2 Multicast service is based on L2 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.

- **Registered Multicast traffic** – If traffic addressed to a registered multicast group is seen it is handled by an entry in the Multicast Filtering Database and forwarded only to the registered ports.
- **Unregistered Multicast traffic** – If traffic addressed to an unregistered multicast group is seen it is handled by a special entry in the Multicast Filtering Database. The default setting of this is to flood all such traffic (traffic in unregistered multicast groups).

Layer 2 switching forwards multicast packets to all relevant VLAN ports by default, treating the packet as a multicast transmission. Multicast traffic forwarding is functional. However, irrelevant ports also receive the multicast, causing increased network traffic. Multicast forwarding filters enable forwarding of Layer 2 packets to port subsets, defined in the multicast filter database.

The device supports forwarding L2 Multicast Packets. Multicast forwarding is enabled by default, and not configurable by user.

This section contains the following topics:

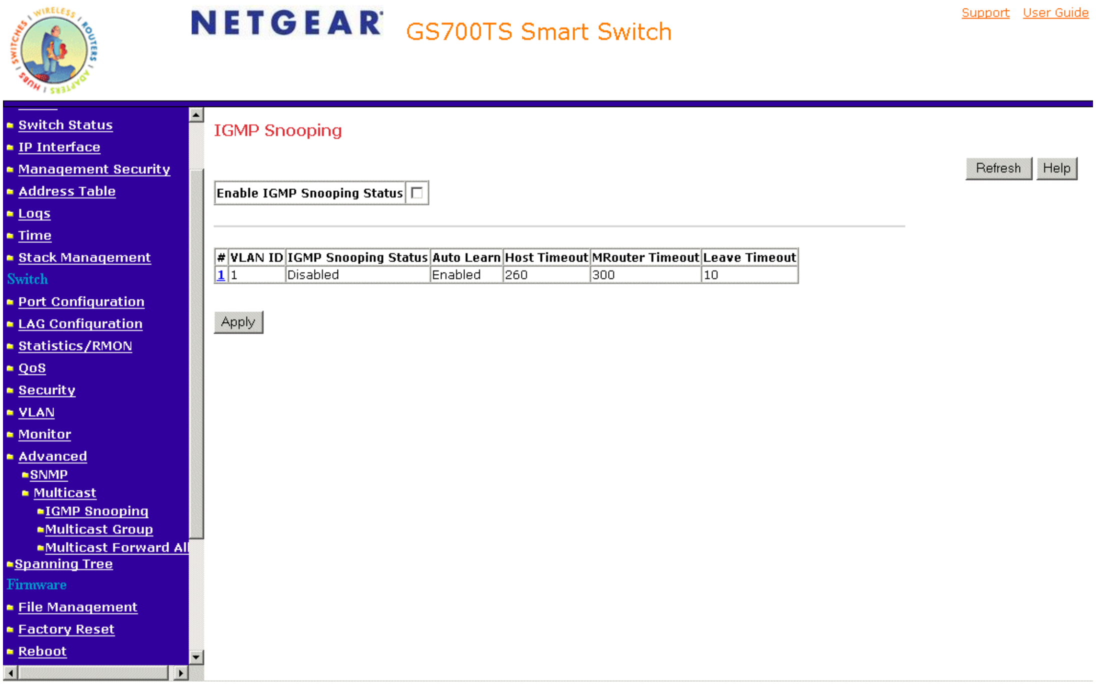
- Configuring IGMP Snooping
- Defining Multicast Groups
- Configuring Multicast Forward All

Configuring IGMP Snooping

When IGMP snooping is enabled, 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, and what routing protocols are forwarding packets and multicast traffic. Ports requesting to join a specific multicast group issues an IGMP report specifying that multicast group.

To enable IGMP Snooping:

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



IGMP Snooping

Enable IGMP Snooping Status □

#	VLAN ID	IGMP Snooping Status	Auto Learn	Host Timeout	MRouter Timeout	Leave Timeout
1	1	Disabled	Enabled	260	300	10

Figure 5-87

The *IGMP Snooping Page* contains the following fields:

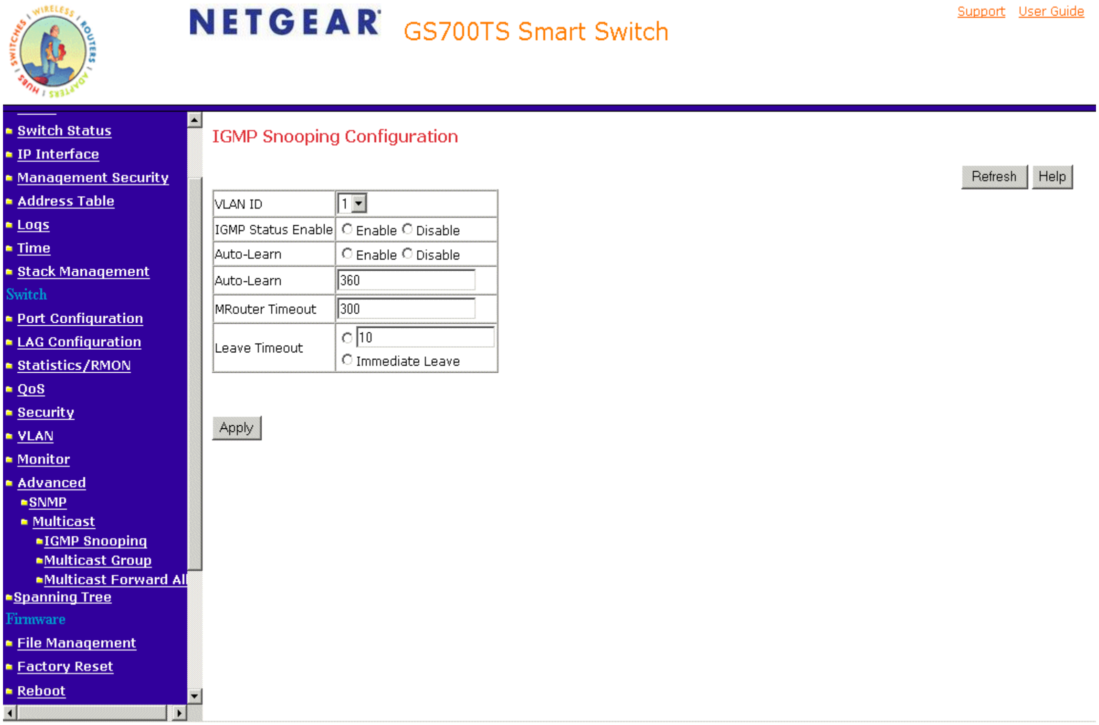
- **Enable IGMP Snooping Status** – Indicates if IGMP Snooping is enabled on the device. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled. The possible field values are:
  - *Checked* – Enables IGMP Snooping on the device.
  - *Unchecked* – Disables IGMP Snooping on the device.
- **VLAN ID** – Specifies the VLAN ID.
- **IGMP Snooping Status** – Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:
  - *Enabled* – Enables IGMP Snooping on the VLAN.
  - *Disabled* – Disables IGMP Snooping 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:
  - *Enabled* – Enables auto learn.
  - *Disabled* – 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. Define the relevant fields.
3. Click Apply. The *IGMP Snooping Page* is defined and the device is updated.

To modify IGMP Snooping:

1. Click **Advanced** > **Multicast** > **IGMP Snooping**. The *IGMP Snooping Configuration Page* opens.
2. Select a VLAN. The *IGMP Snooping Configuration Page* opens:



IGMP Snooping Configuration

VLAN ID	1
IGMP Status Enable	○ Enable ○ Disable
Auto-Learn	○ Enable ○ Disable
Auto-Learn	360
MRouter Timeout	300
Leave Timeout	○ 10 ○ Immediate Leave

Figure 5-88

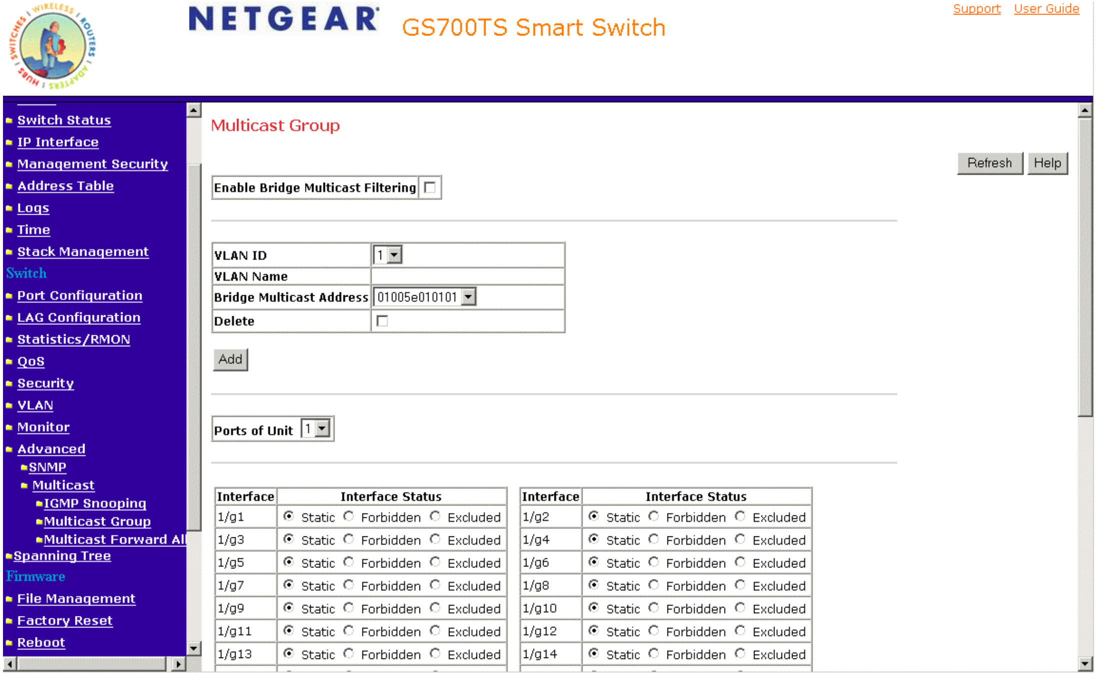
3. Modify the relevant fields.
4. Click Apply. The IGMP Snooping is defined and the device is updated.

Defining Multicast Groups

The *Multicast Group Page* displays the ports and LAGs attached to the multicast service group in the Ports and LAGs tables. The Port and LAG tables also reflect the manner in which the port or LAGs joined the multicast group. Ports can be added either to existing groups or to new multicast service groups. The *Multicast Group Page* permits new multicast service groups to be created. The *Multicast Group Page* also assigns ports to a specific multicast service address group.

To define multicast groups:

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



Multicast Group

Enable Bridge Multicast Filtering □

VLAN ID	1
VLAN Name	
Bridge Multicast Address	01005e010101
Delete	□

Ports of Unit 1

Interface	Interface Status	Interface	Interface Status
1/g1	● Static ○ Forbidden ○ Excluded	1/g2	● Static ○ Forbidden ○ Excluded
1/g3	● Static ○ Forbidden ○ Excluded	1/g4	● Static ○ Forbidden ○ Excluded
1/g5	● Static ○ Forbidden ○ Excluded	1/g6	● Static ○ Forbidden ○ Excluded
1/g7	● Static ○ Forbidden ○ Excluded	1/g8	● Static ○ Forbidden ○ Excluded
1/g9	● Static ○ Forbidden ○ Excluded	1/g10	● Static ○ Forbidden ○ Excluded
1/g11	● Static ○ Forbidden ○ Excluded	1/g12	● Static ○ Forbidden ○ Excluded
1/g13	● Static ○ Forbidden ○ Excluded	1/g14	● Static ○ Forbidden ○ Excluded

Figure 5-89

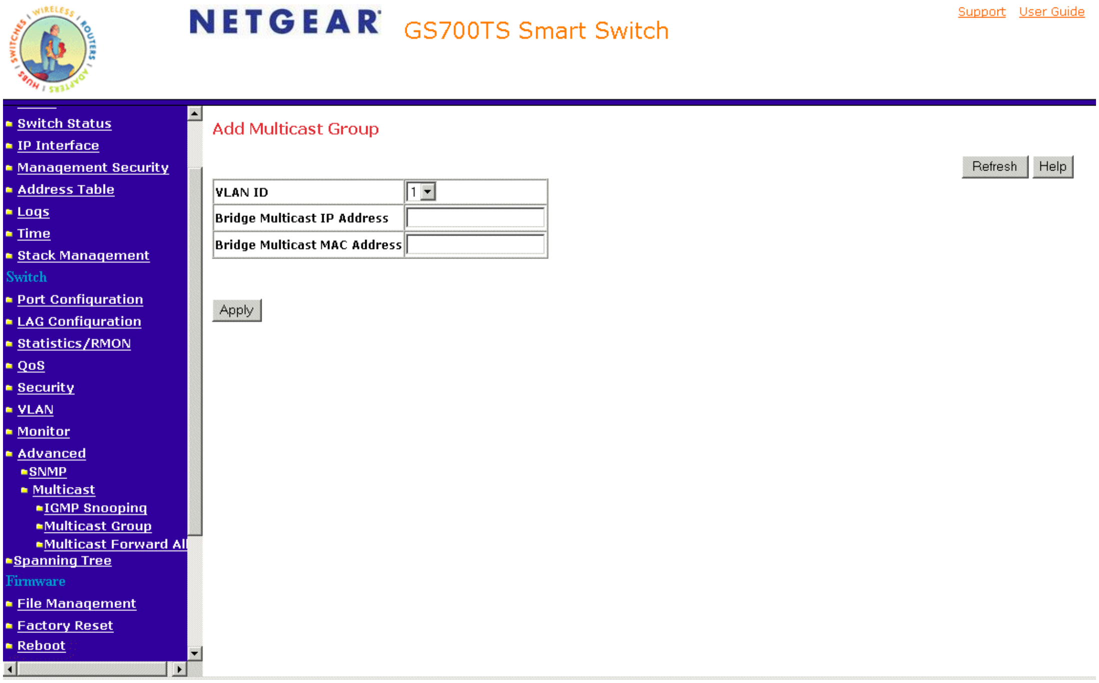
The *Multicast Group Page* contains the following information:

- **Enable Bridge Multicast Filtering** – Indicate 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** – Identifies a VLAN and contains information about the multicast group address.
- **VLAN Name** – Displays the user defined VLAN name.
- **Bridge Multicast Address** – Identifies the multicast group MAC address/IP address.
- **Delete** – The possible field values are:

- *Checked* – Deletes the Vlan ID from the multicast group.
- *Unchecked* – Maintains the list of Vlan IDS.

- **Ports of Unit** – The unit for which the ports are displayed.
- **Interface** – Ports that can be added to a multicast service.
- **Interface Status** – Indicates the interface status. The possible field values are:
  - *Static* – The interface is statistically configured to the multicast group.
  - *Forbidden* – The interface is forbidden from joining the multicast group.
  - *Excluded* – The port is not a member of the multicast group.

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



Add Multicast Group

VLAN ID	1
Bridge Multicast IP Address	
Bridge Multicast MAC Address	

Figure 5-90

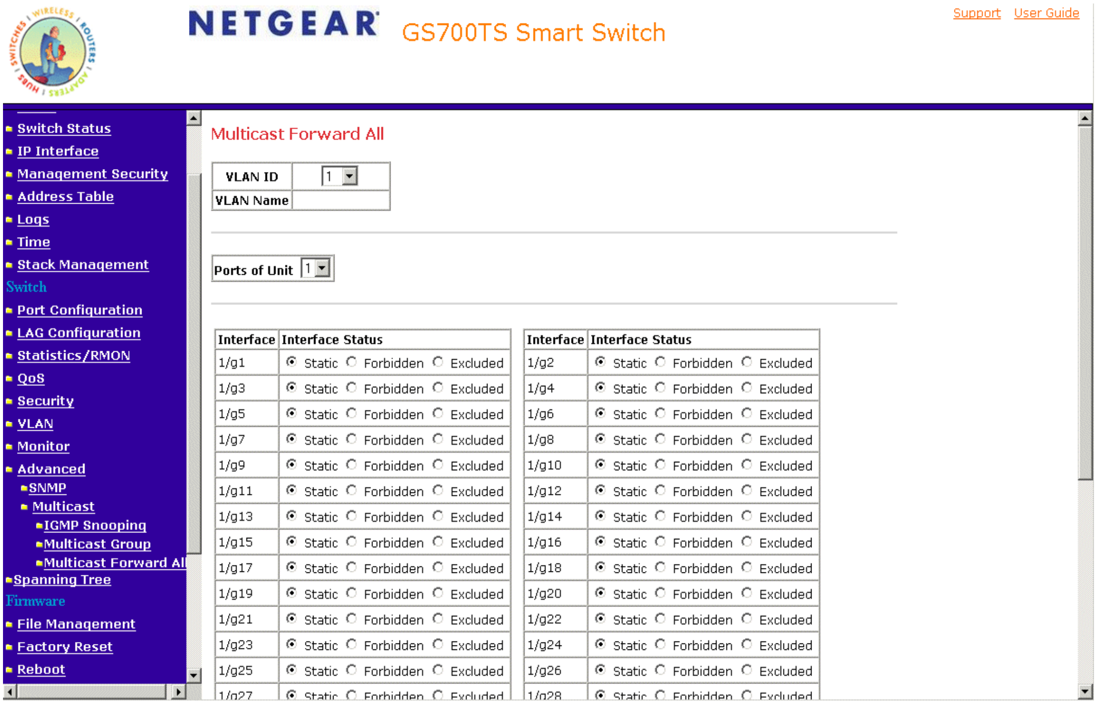
3. Define the relevant fields.
4. Click Apply. The multicast group is defined, and the device is updated.

Configuring Multicast Forward All

The Bridge Multicast Forward All page contains fields for attaching ports or LAGs 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 LAGs are defined, only a Multicast Forward All table displays.

To define Multicast forward all settings:

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



Multicast Forward All

VLAN ID	1
VLAN Name	

Ports of Unit 1

Interface	Interface Status	Interface	Interface Status
1/g1	● Static ○ Forbidden ○ Excluded	1/g2	● Static ○ Forbidden ○ Excluded
1/g3	● Static ○ Forbidden ○ Excluded	1/g4	● Static ○ Forbidden ○ Excluded
1/g5	● Static ○ Forbidden ○ Excluded	1/g6	● Static ○ Forbidden ○ Excluded
1/g7	● Static ○ Forbidden ○ Excluded	1/g8	● Static ○ Forbidden ○ Excluded
1/g9	● Static ○ Forbidden ○ Excluded	1/g10	● Static ○ Forbidden ○ Excluded
1/g11	● Static ○ Forbidden ○ Excluded	1/g12	● Static ○ Forbidden ○ Excluded
1/g13	● Static ○ Forbidden ○ Excluded	1/g14	● Static ○ Forbidden ○ Excluded
1/g15	● Static ○ Forbidden ○ Excluded	1/g16	● Static ○ Forbidden ○ Excluded
1/g17	● Static ○ Forbidden ○ Excluded	1/g18	● Static ○ Forbidden ○ Excluded
1/g19	● Static ○ Forbidden ○ Excluded	1/g20	● Static ○ Forbidden ○ Excluded
1/g21	● Static ○ Forbidden ○ Excluded	1/g22	● Static ○ Forbidden ○ Excluded
1/g23	● Static ○ Forbidden ○ Excluded	1/g24	● Static ○ Forbidden ○ Excluded
1/g25	● Static ○ Forbidden ○ Excluded	1/g26	● Static ○ Forbidden ○ Excluded
1/g27	● Static ○ Forbidden ○ Excluded	1/g28	● Static ○ Forbidden ○ Excluded

Figure 5-91

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

- **VLAN ID** – Displays the VLAN for which multicast parameters are displayed.
- **VLAN Name** – Displays the user defined VLAN name.
- **Ports of Unit** – Displays ports that can be added to a multicast service.

- **Interface** – Displays the interface for which the multicast parameters on the device is defined.
- **Interface Status** – Indicates the interface status. The possible field values are:
  - *Static* – Attaches the port to the multicast router or switch as a static port.
  - *Forbidden* – Forbidden. The port cannot be attached.
  - *Excluded* – Excluded. The port is not attached.

2. Define the relevant fields.

3. Click Apply. The Multicast Forward All settings are defined, and the device is updated.

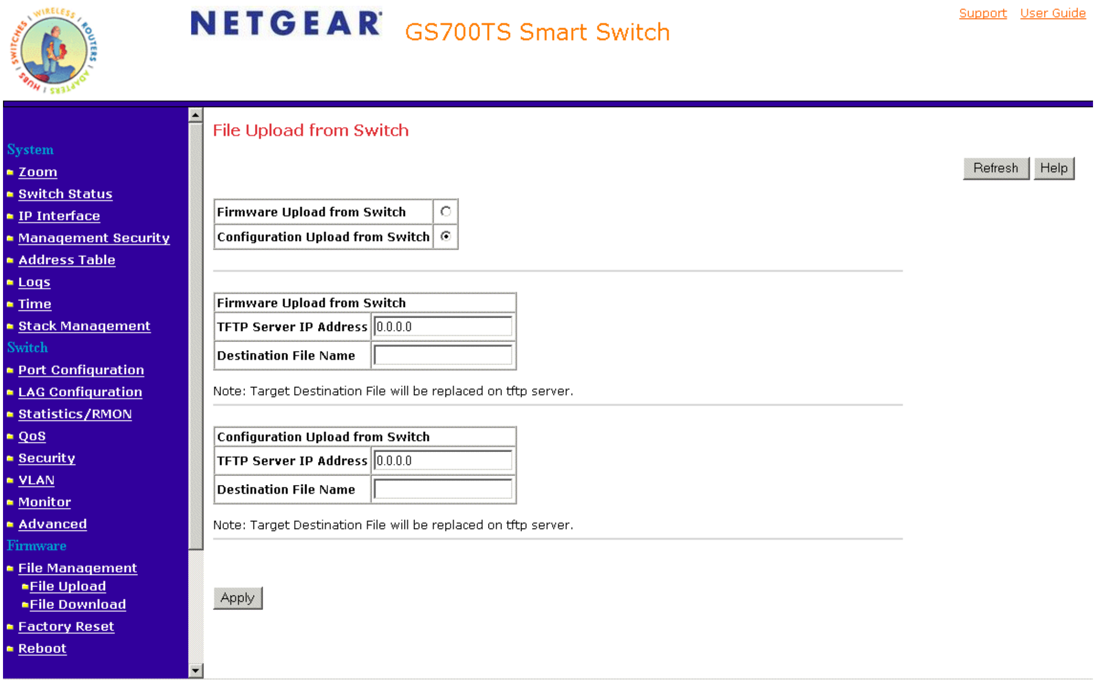
Managing System Files

System Files can be backed up and restored using file management section.

- Upload backs up the firmware and configuration from the switch.
- Download restores a previously saved firmware or configuration onto the switch.

To back up files:

1. Click **File Management > File Upload from Switch**. The *File Upload from Switch Page* opens:



File Upload from Switch

Firmware Upload from Switch	○
Configuration Upload from Switch	●

Firmware Upload from Switch	
TFTP Server IP Address	0.0.0.0
Destination File Name	

Note: Target Destination File will be replaced on tftp server.

Configuration Upload from Switch	
TFTP Server IP Address	0.0.0.0
Destination File Name	

Note: Target Destination File will be replaced on tftp server.

Figure 5-92

The *Configuration Upload from Switch* contains the following fields:

- *Firmware Upload from Switch*
- *Configuration Upload from Switch*

Firmware Upload from Switch

The Firmware section contains the following fields:

- **TFTP Server IP Address** – Specifies the TFTP Server IP Address to which the firmware upload file is uploaded.
- **Destination File Name**– Specifies the source file name to be uploaded.

Configuration Upload from Switch

The Configuration Upload from Switch section contains the following fields:

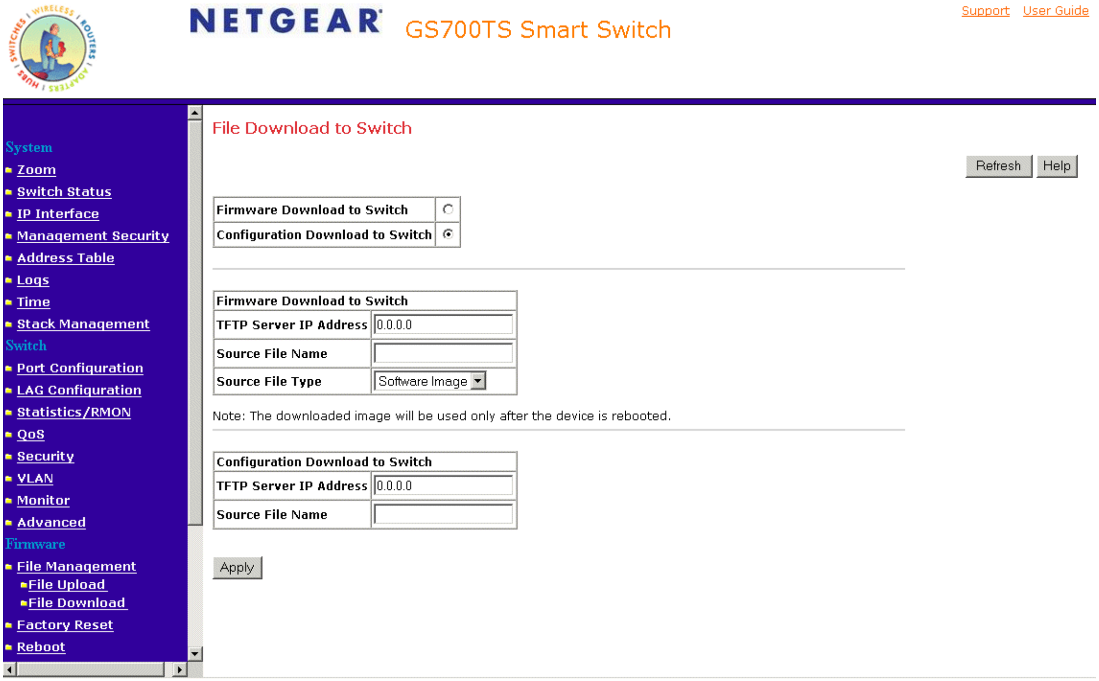
- **TFTP Server IP Address** – Specifies the TFTP Server IP Address to which the configuration file is uploaded.
- **Destination File Name**– Specifies the source file name to be uploaded.

> **Note:** Target Destination File will be replaced on the tftp server.

2. Click Browse to search for the system file.
3. Click Apply to upload the selected file.

To restore saved settings:

1. Click **File Management > File Download to Switch**. The *File Download to Switch Page* opens:



File Download to Switch

Firmware Download to Switch	○
Configuration Download to Switch	●

Firmware Download to Switch	
TFTP Server IP Address	0.0.0.0
Source File Name	
Source File Type	Software Image

Note: The downloaded image will be used only after the device is rebooted.

Configuration Download to Switch	
TFTP Server IP Address	0.0.0.0
Source File Name	

Figure 5-93

The *File Download to Switch Page* contains the following fields:

- *Firmware Download to Switch*
- *Configuration Download to Switch*

Firmware Download to Switch

The Firmware section contains the following fields:

- **TFTP Server IP Address** – Specifies the TFTP Server IP Address from which files are downloaded from the switch.
- **Source File Name**– Specifies the source file name to be downloaded from the switch.
- **Source File Type** – Specifies the destination file type to which to the file is downloaded from the switch. The possible field values are:

  - *Software Image* – Downloads the Image file.
  - *Boot Code* – Downloads the Boot file.

> **Note:** The downloaded image will be used only after the device is rebooted.

Configuration Download to Switch

The Configuration Download section contains the following fields:

- **TFTP Server IP Address** – Specifies the TFTP Server IP Address from which the configuration files are downloaded.
- **Source File Name** – Specifies the configuration files to be downloaded.

2. Click Browse to search for the system file.
3. Click Apply to download the selected file.

Monitoring the Device

This section contains the following topics:

- Configuring Port Mirroring
- Performing Copper Cable Tests

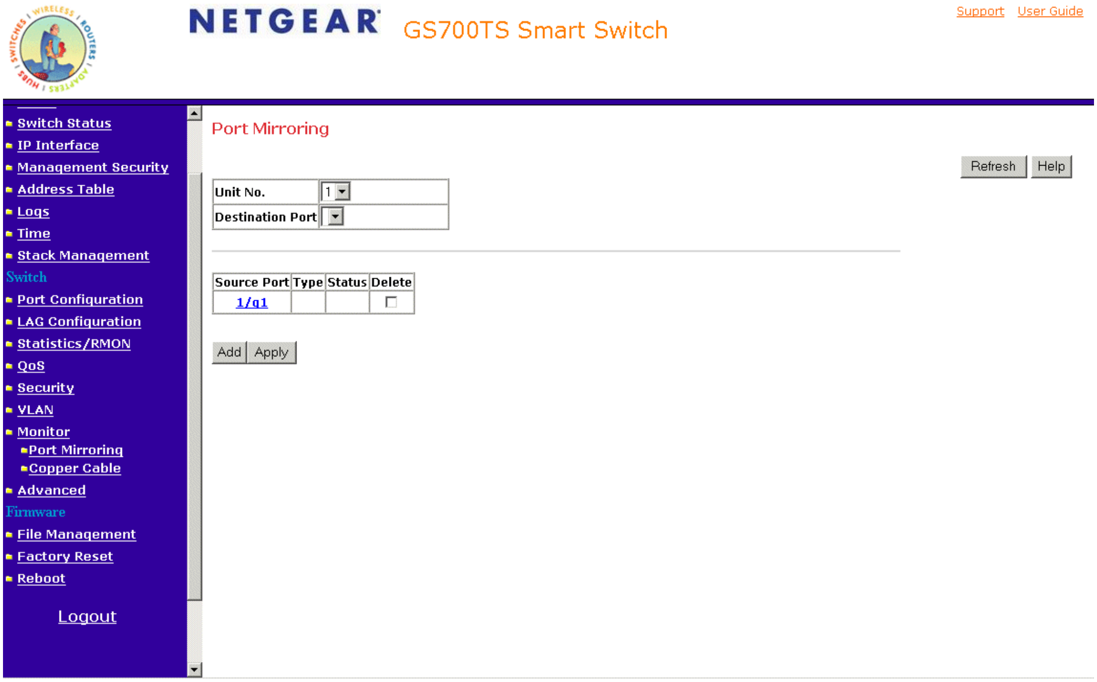
Configuring Port Mirroring

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 switch performance monitoring. Network administrators can configure up to eight ports for port mirroring. The switch is capable of mirroring all transmitted packets; all received packets; or all packets, both transmitted and received.

Network administrators can configure port mirroring by selecting specific ports from which to copy packets, and other ports to which the packets are copied.

To enable port mirroring:

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



Port Mirroring

Unit No.	1
Destination Port	

Source Port	Type	Status	Delete
1/g1			□

Figure 5-94

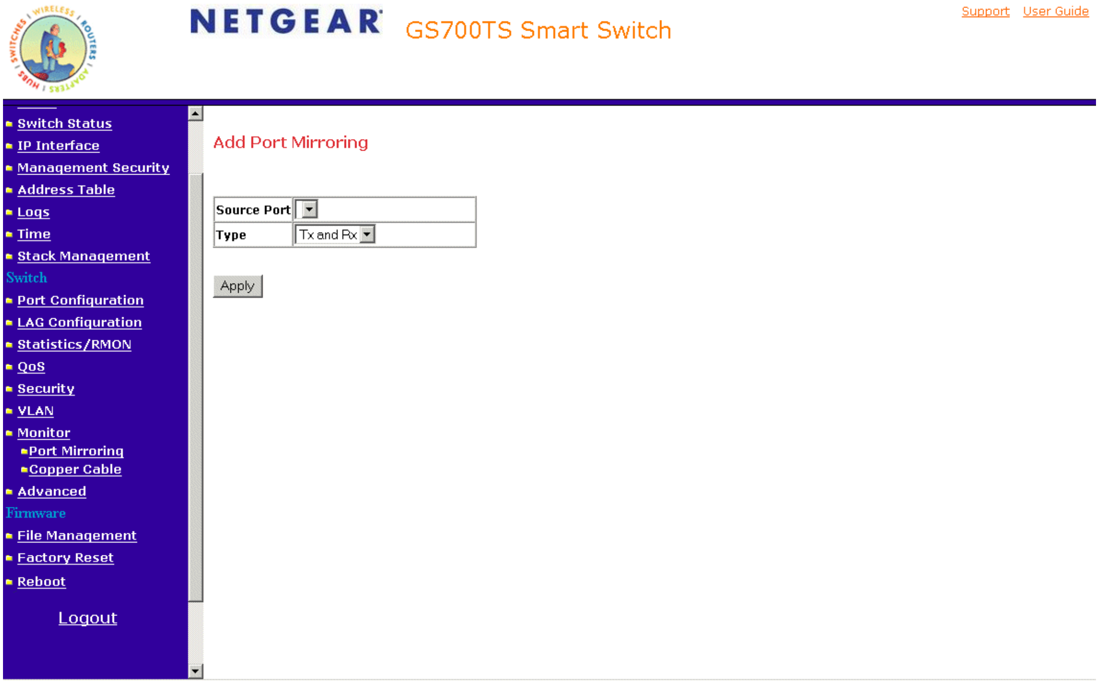
The *Port Mirroring Page* contains the following fields:

- **Unit No.** – Indicates the stacking number.
- **Destination Port** – Defines the port number to which port traffic is copied.
- **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* – Copies traffic received by the port.
  - *Tx* – Copies traffic transmitted by the port.
  - *Tx and Rx* – Copies traffic both transmitted and received by the port. This is the default value.
- **Status** – Indicates if the port is currently monitored. The possible field values are:

- *Active* – Indicates the port is currently monitored.
- *Ready* – Indicates the port is not currently monitored.

- **Delete** – Removes the port mirroring session. The possible field values are:
  - *Checked* – Removes the selected port mirroring sessions.
  - *Unchecked* – Maintains the port mirroring session.

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



Add Port Mirroring

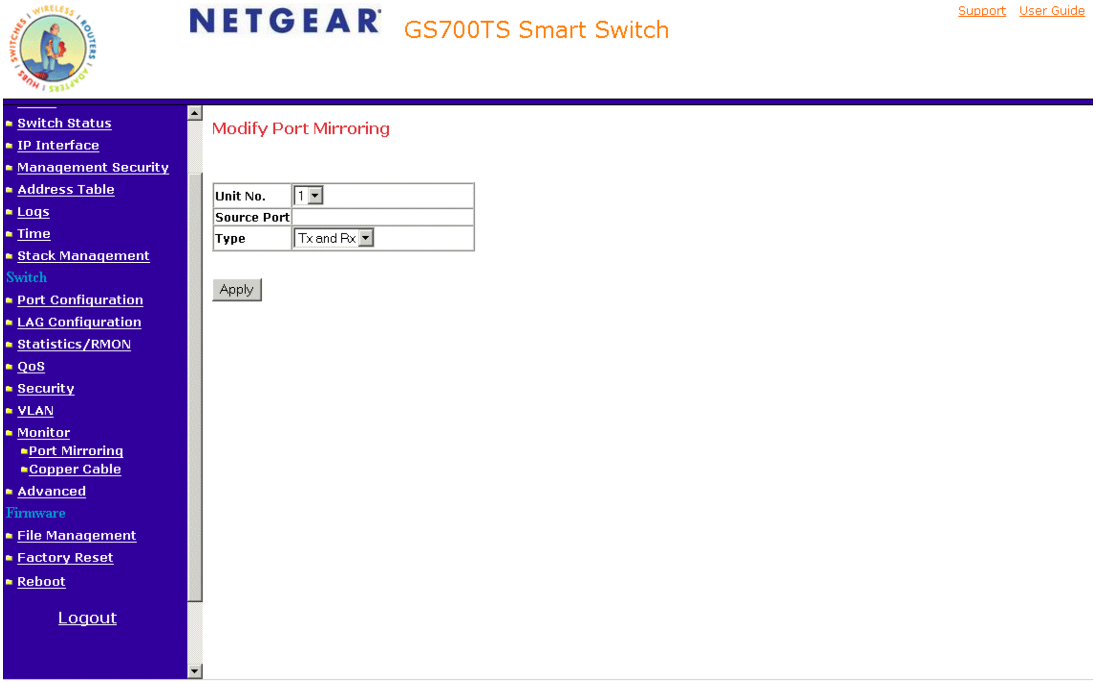
Source Port	
Type	Tx and Rx

Figure 5-95

3. Define the relevant fields.
4. Click Apply. The port mirroring session is defined and the device is updated.

To modify the port mirroring settings:

1. Click **Monitor** > **Port Mirroring**.
2. Click an interface. The *Modify Port Mirroring Page* opens:



Modify Port Mirroring

Unit No.	1
Source Port	
Type	Tx and Rx

Figure 5-96

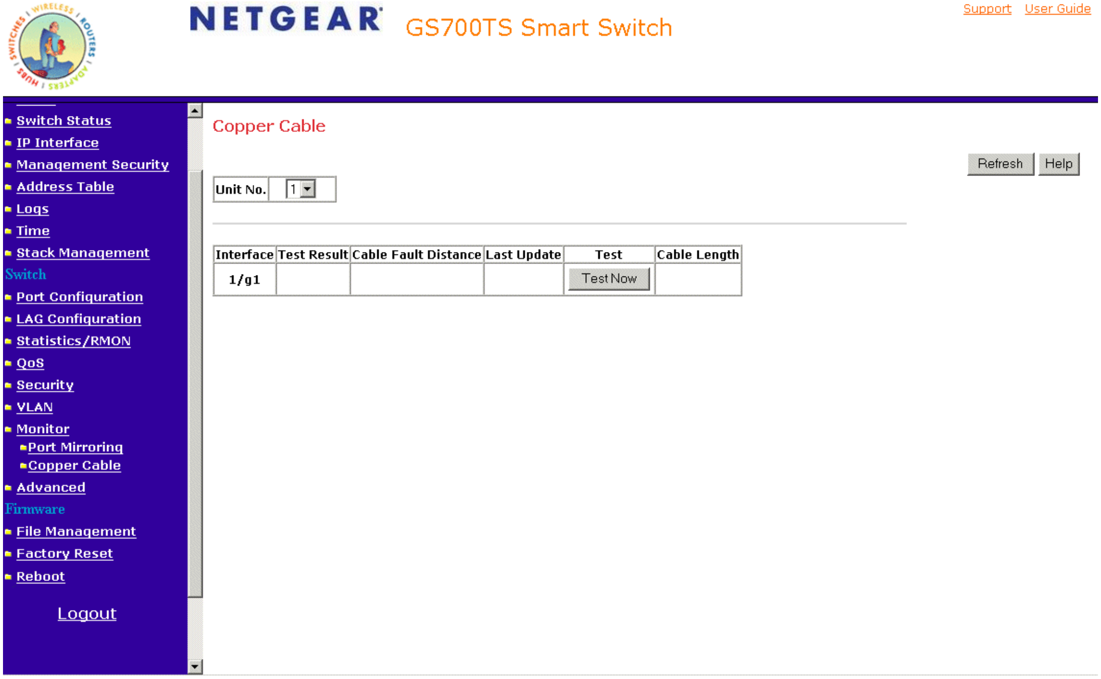
3. Modify the relevant fields.
4. Click Apply. The port mirroring settings are modified and the device is updated.

Performing Copper Cable Tests

The Performing Copper Cable Tests contains fields for performing tests on copper cables. Cable testing provides 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 test cables:

1. Click **Monitor > Copper Cable.** The *Copper Cable Page* opens:



Copper Cable

Unit No. 1

Interface	Test Result	Cable Fault Distance	Last Update	Test	Cable Length
1/g1				Test Now	

Figure 5-97

The *Copper Cable Page* contains the following fields:

- **Unit No.** – Indicates the stacking member for which the copper cable test results are displayed.
- **Interface** – 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.
- **Test** – Click Test Now . The test results are displayed.
- **Cable Length** – Indicates the approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.

Managing RMON Statistics

This section contains information for viewing the Remote Monitoring Statistics. RMON Statistics allow network managers to view network traffic information from a single workstation.

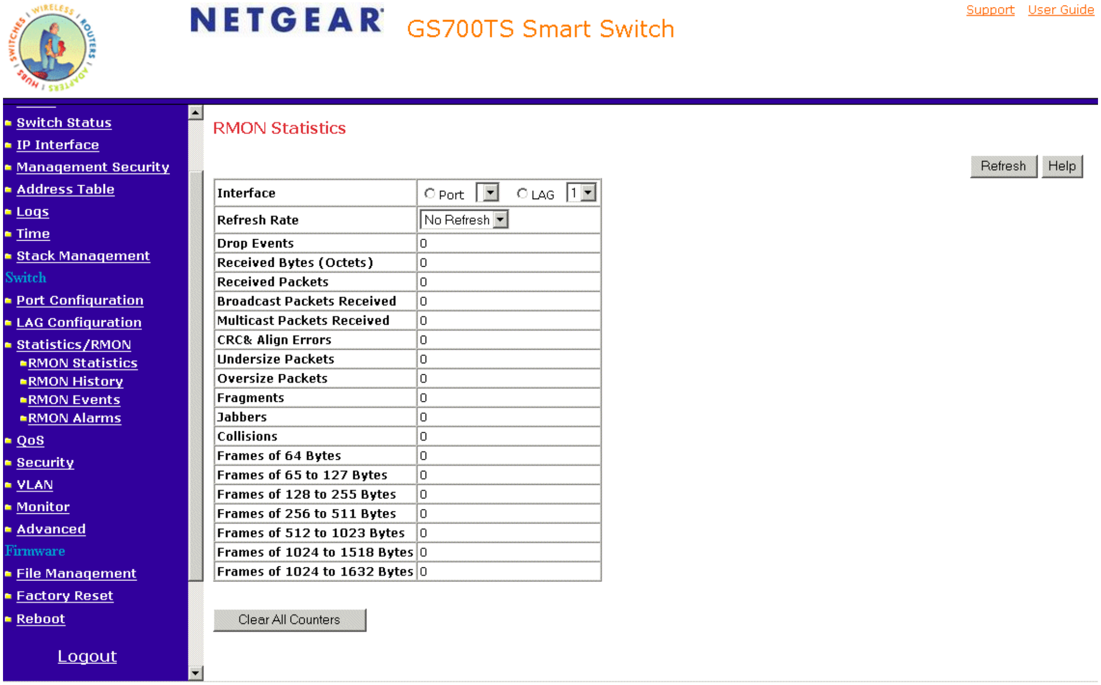
- Viewing RMON Statistics
- Configuring RMON History
- Defining RMON Events

Viewing RMON Statistics

The *RMON Statistics Page* contains fields for viewing information about device utilization and errors that occurred on the device.

To view RMON statistics:

1. Click **Statistics/RMON** > **RMON Statistics**. The *RMON Statistics Page* opens:



RMON Statistics

Interface	○ Port ▾ ○ LAG 1 ▾
Refresh Rate	No Refresh ▾
Drop Events	0
Received Bytes (Octets)	0
Received Packets	0
Broadcast Packets Received	0
Multicast Packets Received	0
CRC& Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	0
Frames of 65 to 127 Bytes	0
Frames of 128 to 255 Bytes	0
Frames of 256 to 511 Bytes	0
Frames of 512 to 1023 Bytes	0
Frames of 1024 to 1518 Bytes	0
Frames of 1024 to 1632 Bytes	0

Figure 5-98

The *RMON Statistics Page* contains the following fields:

- **Interface** – Indicates the device for which statistics are displayed. The possible field values are:
  - *Port* – Defines the specific port for which RMON statistics are displayed.
  - *LAG* – Defines the specific LAG for which RMON statistics are displayed.
- **Refresh Rate** – Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - *No Refresh* – Indicates that the RMON statistics are not refreshed.
  - *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.

- **Drop Events** – Displays the number of dropped events that have occurred on the interface since the device was last 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** – Number of xx-byte frames received on the interface since the device was last refreshed.

2. Select an interface in the Interface field. The RMON statistics are displayed.

Resetting RMON Statistics Counters

1. Open the Viewing RMON Statistics.

2. Click Clear All Counters. The RMON statistics counters are cleared.

Configuring RMON History

This section contains the following topics:

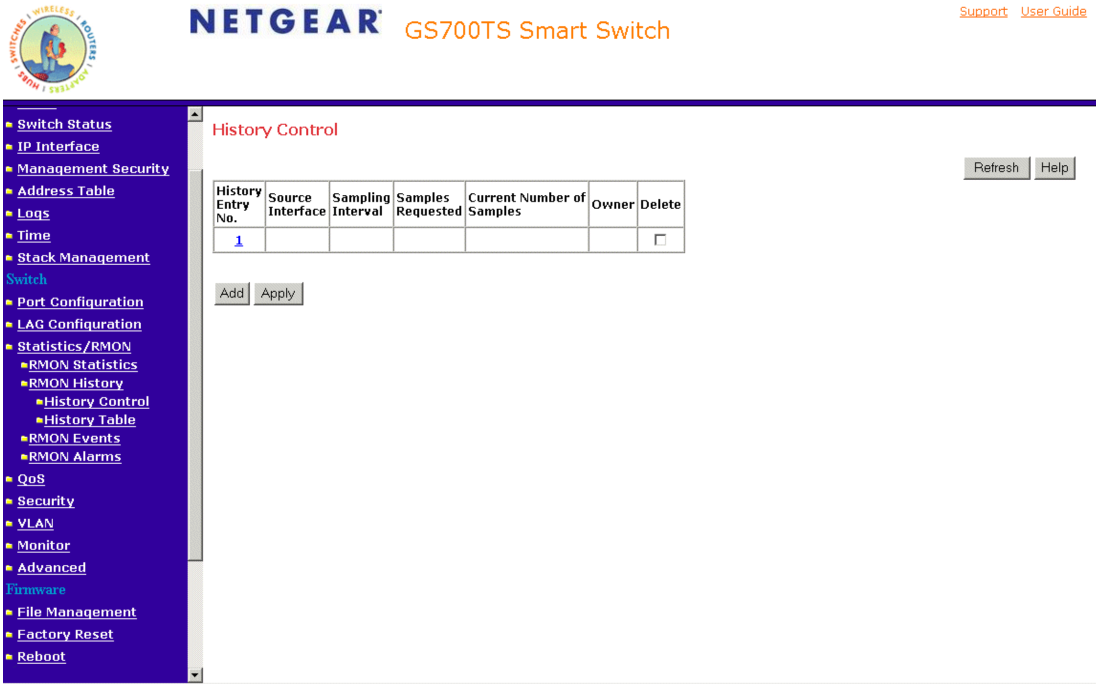
- Defining RMON History Control
- Viewing the RMON History Table

Defining RMON History Control

The *History Control 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 > RMON History > History Control.** The *History Control Page* opens:



History Control

History Entry No.	Source Interface	Sampling Interval	Samples Requested	Current Number of Samples	Owner	Delete
1						□

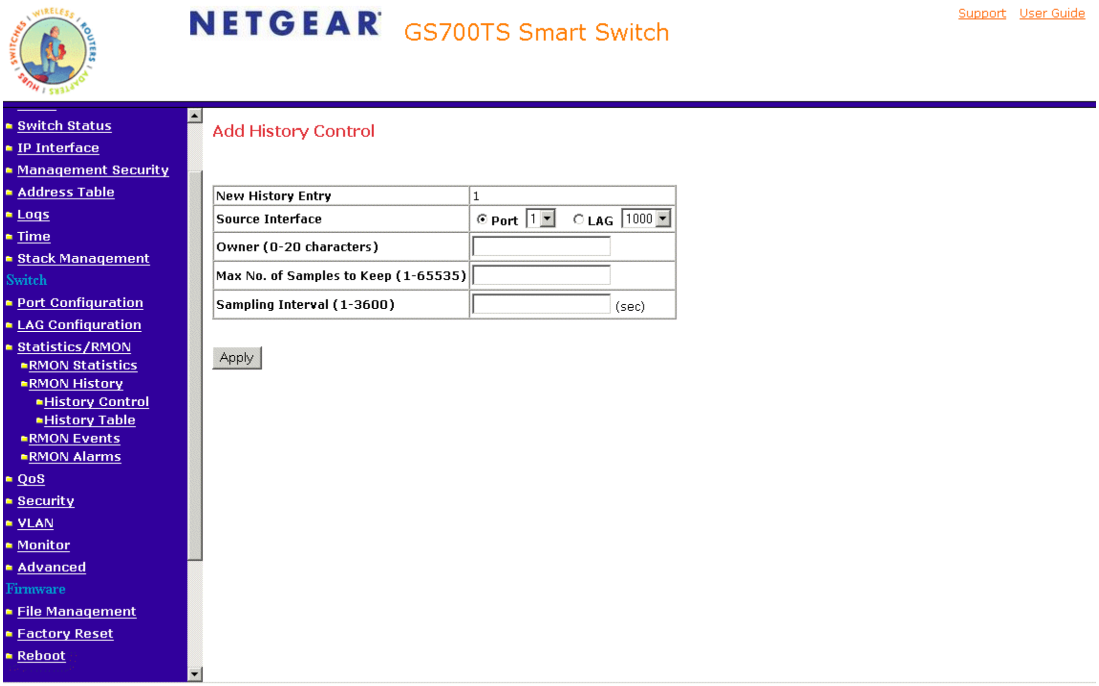
Figure 5-99

The *History Control Page* contains the following fields:

- **History Entry No.** – Displays the entry number for the History Control Table page.
- **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.
  - *LAG* – Specifies the LAG from which the RMON information was taken.
- **Sampling Interval** – Indicates in seconds the time that samples are taken from the ports. The field range is 1-3600. The default is **1800 seconds (equal to 30 minutes).**
- **Samples Requested** – Displays the number of samples to be saved. The field range is 1-65535. The default value is 50.
- **Current Number of Samples in List–** Displays the current number of samples taken.

- **Owner** – Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Delete** – Removes History Control entries. The possible field values are:
  - *Checked* – Removes the selected History Control entry.
  - *Unchecked* – Maintains the current History Control entries.

2. Click Add. The *Add History Control Page* opens:



Add History Control

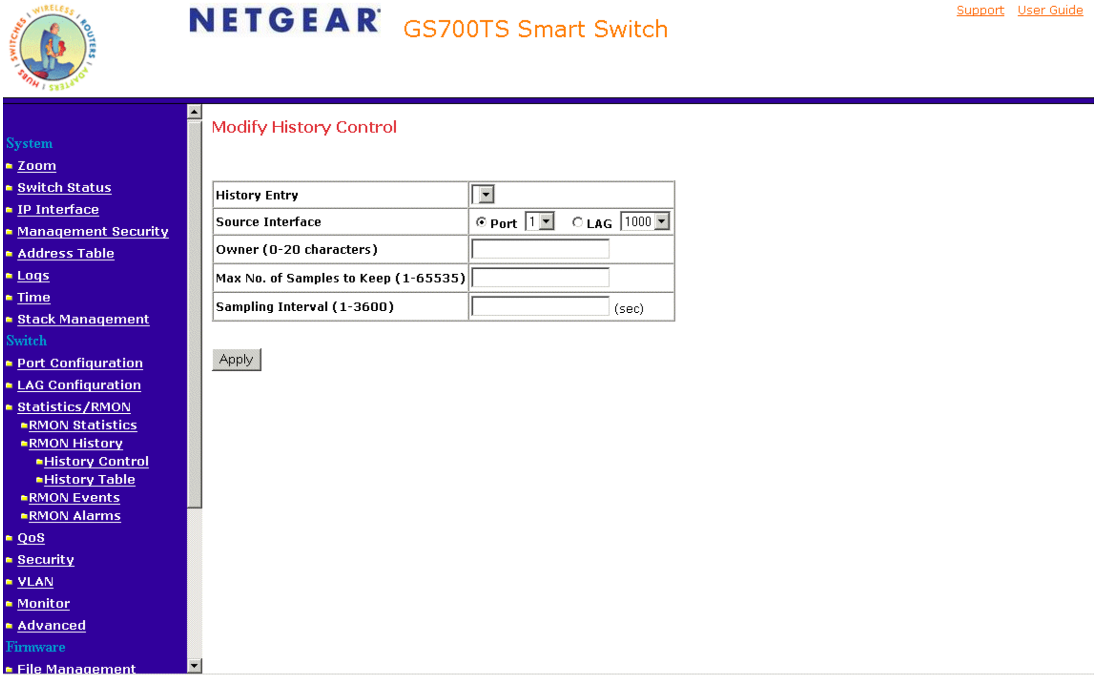
New History Entry	1
Source Interface	● Port 1 ○ LAG 1000
Owner (0-20 characters)	
Max No. of Samples to Keep (1-65535)	
Sampling Interval (1-3600)	(sec)

Figure 5-100

3. Define the relevant fields.
4. Click Apply. The entry is added to the History Control Page and the device is updated.

To modify RMON history information:

1. Click **Statistics/RMON** > **RMON History** > **History Control.** The *History Control Page* opens.
2. Click a history entry number. The *Modify History Control Page* opens:



Modify History Control

History Entry	
Source Interface	● Port 1 ○ LAG 1000
Owner (0-20 characters)	
Max No. of Samples to Keep (1-65535)	
Sampling Interval (1-3600)	(sec)

Apply

Figure 5-101

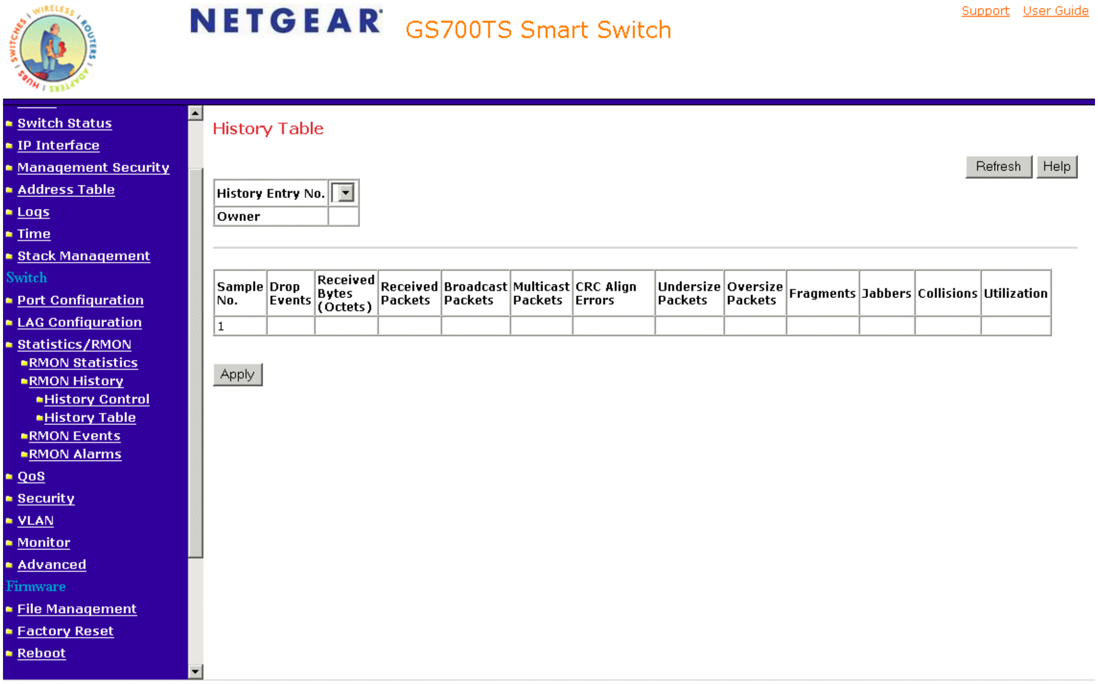
3. Modify the relevant fields.
4. Click Apply. The entry is modified and the device is updated.

Viewing the RMON History Table

The *History Table Page* contains interface specific statistical network samples. Each table entry represents all counter values compiled during a single sample.

To view the RMON History Table:

1. Click **Statistics/RMON** > **RMON History** > **History Table**. The *History Table Page* opens:



History Table

History Entry No.	
Owner	

Sample No.	Drop Events	Received Bytes (Octets)	Received Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization
1												

Figure 5-102

The *History Table Page* contains the following fields:

- **History Entry No.** – Displays the entry number for the History Control Table page.
- **Owner** – Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Sample No.** – Indicates the sample number from which the statistics were taken.
- **Drop Events** – Displays the number of dropped events that have occurred on the interface since the device was last 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 since the device was last refreshed, including bad packets, multicast packets, 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 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.

2. Select a history entry number.

3. Click Apply. The RMON history table is displayed.

Defining RMON Events

This section includes the following topics:

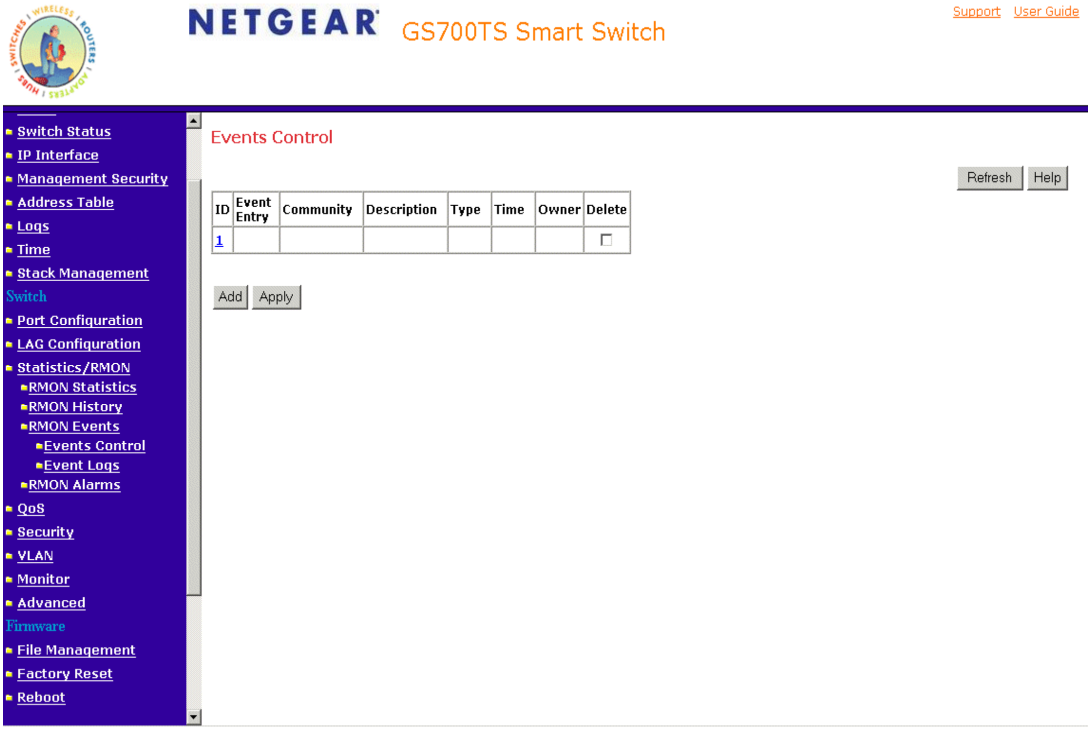
- Defining RMON Events Controll
- Viewing the RMON Events Logs

Defining RMON Events Control

The *Events Control Page* contains fields for defining RMON events.

To view RMON events:

1. Click **Statistics/RMON > RMON Events > Events Control**. The *Events Control Page* opens:



ID	Event Entry	Community	Description	Type	Time	Owner	Delete
1							☐

Figure 5-103

The *Events Control Page* contains the following fields:

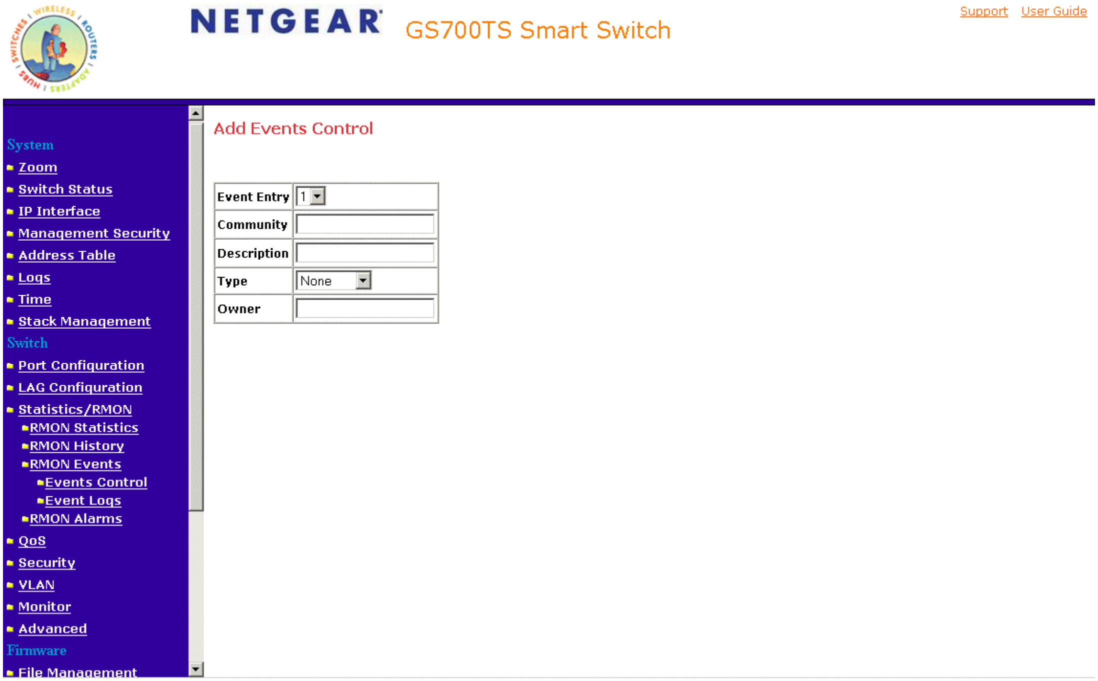
- **ID** – Indicates the stacking number.
- **Event Entry** – Displays the event.
- **Community** – Displays the community to which the event belongs.
- **Description** – Displays the user-defined event description.
- **Type** – Describes the event type. Possible values are:
  - *Log* – Indicates that 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.
- **Delete** – Removes a RMON event. The possible field values are:
  - *Checked* – Removes a selected RMON event.
  - *Unchecked* – Maintains RMON events.

2. Click Apply. The RMON events table is displayed.

To add an RMON event:

1. Click **Statistics/RMON > RMON Events > Events Control**. The *Events Control Page* opens.
2. Click Add. The *Add Events Control Page* is opens:



Add Events Control

Event Entry	1
Community	
Description	
Type	None
Owner	

Figure 5-104

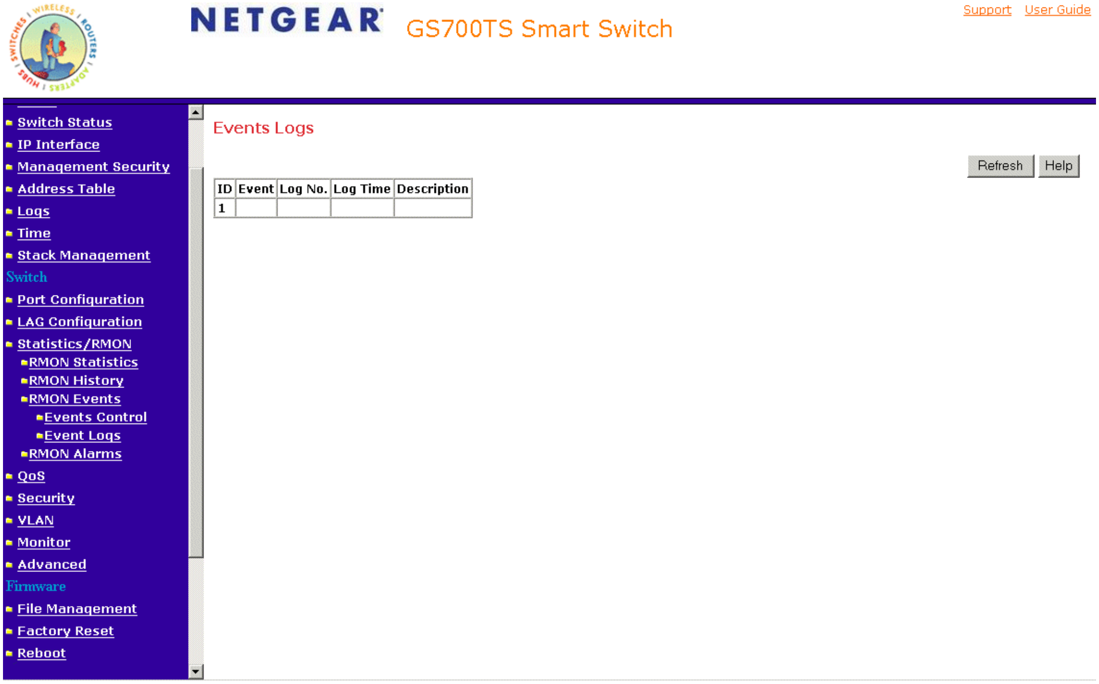
3. Define the relevant fields.
4. Click Apply. The port mirroring session is defined and the device is updated.

Viewing the RMON Events Logs

The *Events Logs Page* contains a list of RMON events.

To view RMON event logs:

1. Click **Statistics/RMON** > **RMON Events** > **Event Logs**. The *Events Logs Page* opens:



Events Logs

ID	Event	Log No.	Log Time	Description
1				

Figure 5-105

The *Events Logs Page* contains the following fields:

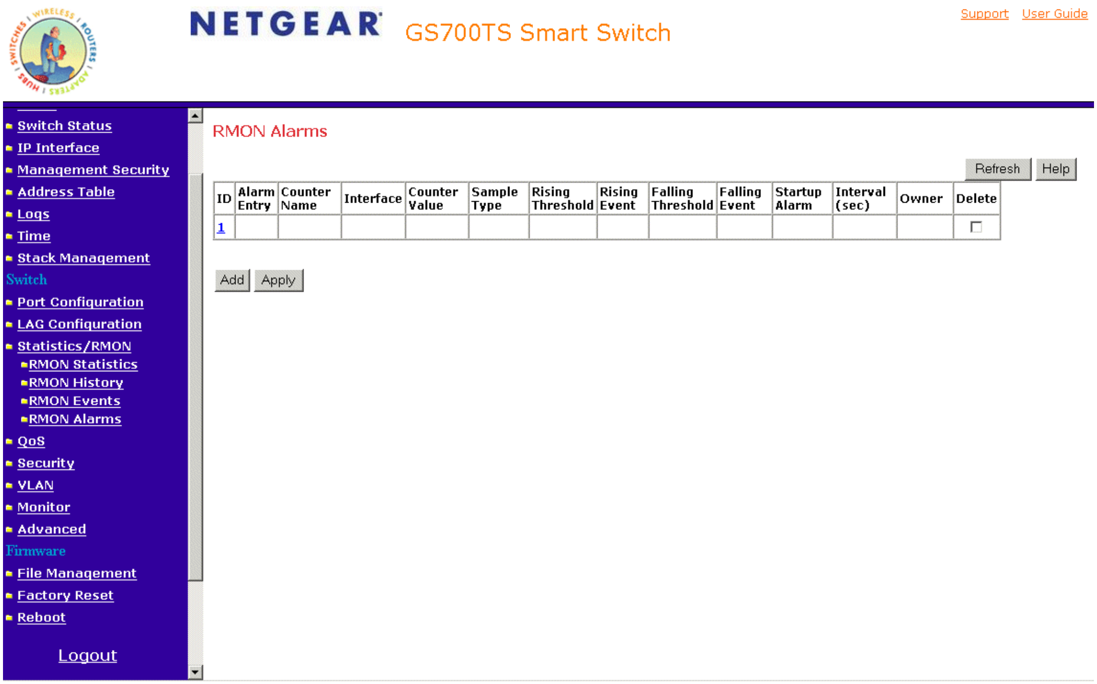
- **ID** – Indicates the Events Logs Page table entry.
- **Event** – Displays the RMON Events.
- **Log No.**– Displays the log number.
- **Log Time** – Displays the time when the log entry was entered.
- **Description** – Displays the log entry description.

Defining RMON Alarms

The RMON Alarms 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** > **RMON Alarms**. The *RMON Alarms Page* opens:



ID	Alarm Entry	Counter Name	Interface	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Startup Alarm	Interval (sec)	Owner	Delete
1													□

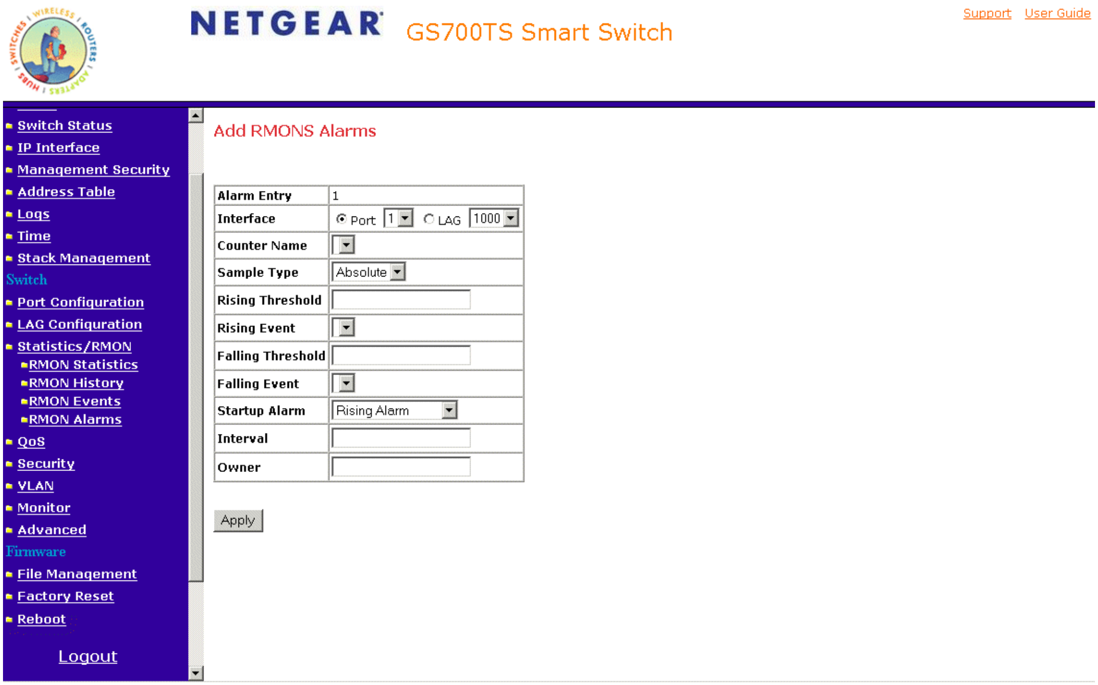
Figure 5-106

The *RMON Alarms Page* contains the following fields:

- **ID** – The row number of the alarm entry.
- **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.
  - *LAG* – Displays the RMON statistics for the selected LAG.
- **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. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising Event** – Displays the mechanism in which the alarms are reported. The possible field values are:
  - *LOG* – Indicates there is not a saving mechanism for either the device or in the management system. If the device is not reset, the entry remains in the Log Table.
  - *TRAP* – Indicates that an SNMP trap is generated and sent via the Trap mechanism. The Trap can also be saved using the Trap mechanism.
  - *Both* – Indicates that both the Log and Trap mechanism are used to report alarms.
- **Falling Threshold** – Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event –** Displays the mechanism in which the alarms are reported.
- **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.
- **Delete** – Removes the RMON Alarms Table entry.

2. Click Add. The *Add RMON Alarms Page* opens:



Add RMONS Alarms

Alarm Entry	1
Interface	● Port 1 ○ LAG 1000
Counter Name	
Sample Type	Absolute
Rising Threshold	
Rising Event	
Falling Threshold	
Falling Event	
Startup Alarm	Rising Alarm
Interval	
Owner	

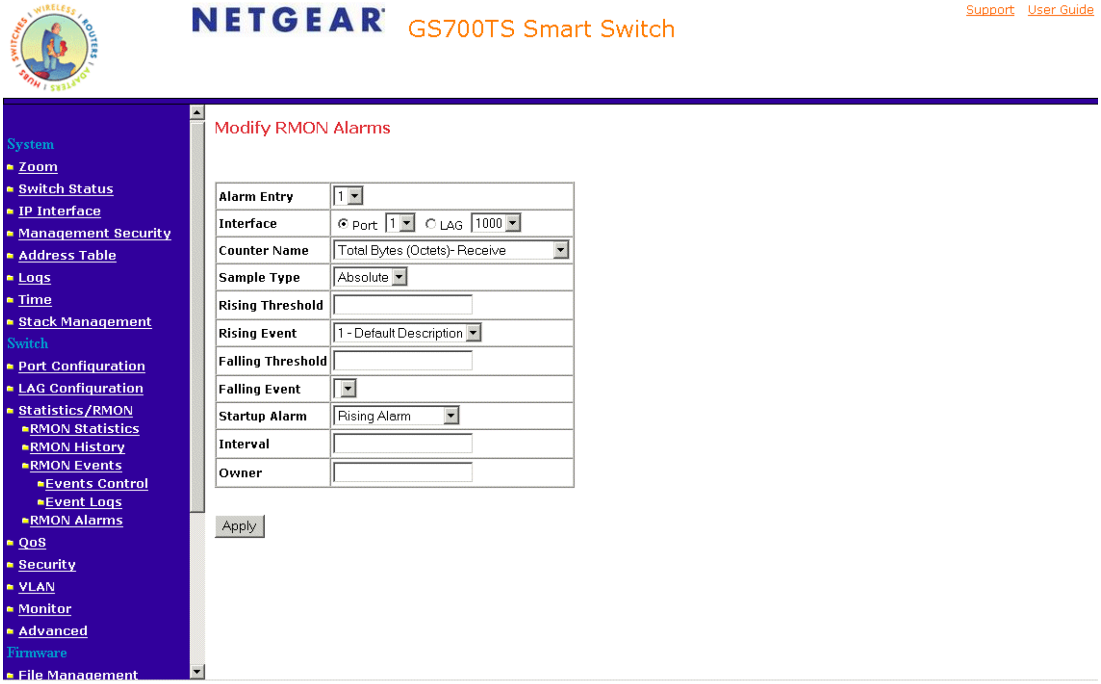
Figure 5-107

3. Define the relevant fields.

4. Click Apply. The RMON alarm is added and the device is updated.

To modify RMON alarms:

1. Click **Statistics/RMON > RMON Alarms**. The *RMON Alarms Page* opens.
2. Select an ID. The *Modify RMONS Alarms Page* opens:



Modify RMON Alarms

Alarm Entry	1
Interface	● Port 1 ○ LAG 1000
Counter Name	Total Bytes (Octets)- Receive
Sample Type	Absolute
Rising Threshold	
Rising Event	1 - Default Description
Falling Threshold	
Falling Event	
Startup Alarm	Rising Alarm
Interval	
Owner	

Apply

Figure 5-108

3. Modify the relevant fields.
4. Click Apply. The RMON alarm is modified and the device is updated.

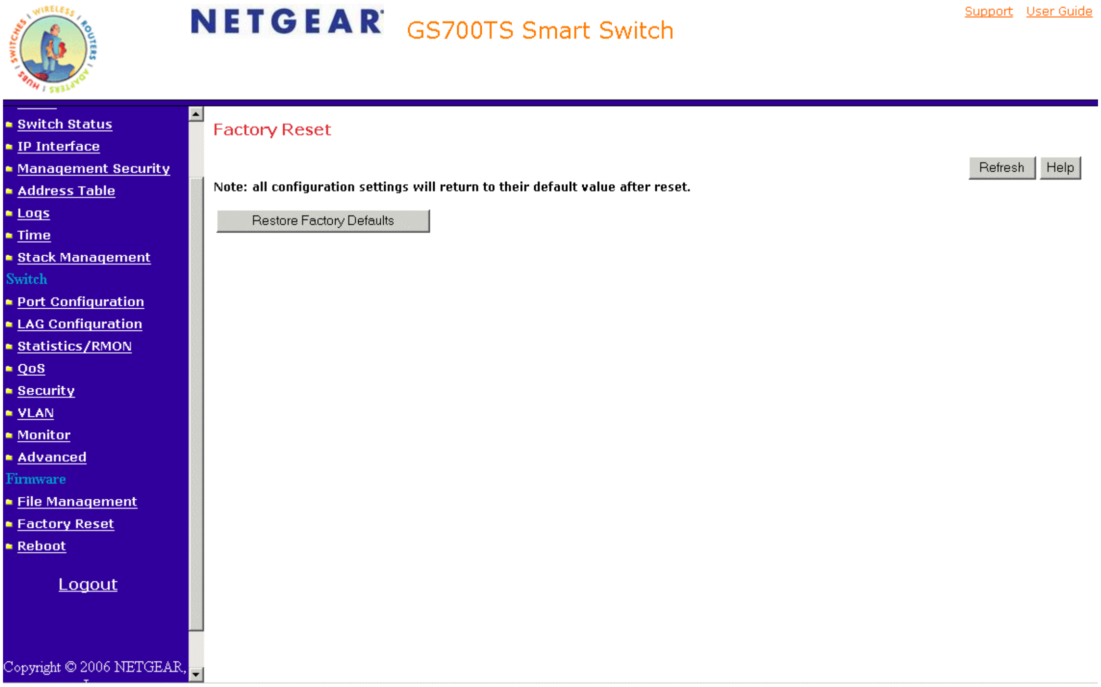
Resetting the Factory Default Values

The Factory Reset Page allows network managers to reset the device to the factory defaults shipped with the switch. Restoring factory defaults results in erasing the configuration file. The stacking defaults are not restored from this page, including:

- The stacking mode
- The stacking cables
- The Unit ID numbering

To restore stacking defaults, press the Factory Default button on the front panel of your device. To reset the factory defaults:

1. Click **Factory Reset**. The *Factory Reset Page* opens:



Note: all configuration settings will return to their default value after reset.

Figure 5-109

2. Click Restore Factory Defaults. The device reboots and the original default values are set.

Appendix A
Default Settings

This appendix provides default settings for the NETGEAR Model GS700TS Smart Gigabit Ethernet Switch. You can always configure the switch to default settings by using the Factory Reset function from a web browser.

Table 1: Default Settings

Feature	GS700TS Default Setting
Port Speed	Auto-negotiation
Port Duplex	Auto-negotiation
Flow Control (half duplex)	Enabled
Flow Control (full duplex)	Enabled
IP Configuration	DHCP enabled
Password	password
VLAN	802.1q based VLAN
Link Aggregation (Trunk)	Disabled
Traffic Prioritization (QoS)	Optimized for flow control, all ports set normal priority

Index