GS108T Smart Switch Software Administration Manual

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

202-10249-01
May 2007

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks of NETGEAR, Inc. in the United States and/or other countries. Microsoft, Windows, and Windows NT are registered trademarks and Vista is a trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders.

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. Information is subject to change without notice.

Certificate of the Manufacturer/Importer

It is hereby certified that the GS108T Gigabit Smart Switch 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.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the first category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines that are aimed at preventing radio interference in commercial and/or industrial areas.

Consequently, when this equipment is used in a residential area or in an adjacent area thereto, radio interference may be caused to equipment such as radios and TV receivers.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

EU Statement of Compliance

The NETGEAR GS108T Gigabit Smart Switch is compliant with the following EU Council Directives: 89/336/EEC and LVD 73/23/EEC. Compliance is verified by testing to the following standards: EN55022 Class A, EN55024 and EN60950-1.

⚠	**Warning:** This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take appropriate measures.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (NETGEAR GS108T Gigabit Smart Switch) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (NETGEAR GS108T Gigabit Smart Switch) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Customer Support

For assistance with installing and configuring your NETGEAR system or for questions or problems following installation:

- Check the NETGEAR Web page at http://www.NETGEAR.com/support
- Call Technical Support in North America at 1-888-NETGEAR. If you are outside North America, please refer to the phone numbers listed on the Support Information Card that was included with your switch.
- Email Technical Support at support@NETGEAR.com.
- Defective or damaged merchandise can be returned to your point-of-purchase representative.

Internet/World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the uniform resource locator (URL) http://www.NETGEAR.com. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

FCC Requirements for Operation in the United States

FCC Information to User: This product does not contain any user-serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

FCC Guidelines for Human Exposure: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm

between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity: We, NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model GS108T: ProSafe™ 8 Port 10/100/1000 smart switch complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: a) This device may not cause harmful interference and b) This device must accept any interference received, including interference that may cause undesired operation."

Product and Publication Details

Model Number:	GS108T
Publication Date:	May 2007
Product Family:	Smart Switch
Product Name:	GS108T Gigabit Smart Switch
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10249-01
Publication Version Number:	1.0

Contents

About This Manual

The *NETGEAR® GS108T Smart Switch Software Administration Manual* describes how to install, configure, operate, and troubleshoot the GS108T Gigabit Smart Switch using, its included software. This book describes the software configuration procedures and explains the options available within those procedures.

Who Should Use this Book

The information in this manual is intended for readers with intermediate to advanced system management skills.

This document was created primarily for the system administrator who wishes to install and configure the GS108T Smart Switch in a network. It assumes that the reader has a general understanding of switch platforms and a basic knowledge of Ethernet and networking concepts. To install this switch, it is not necessary to understand and use all of its capabilities. Once basic configuration is performed, it will function in a network using its remaining factory default parameters. However, a greater level of configuration—anywhere from the basic up to the maximum possible—will allow your network the full benefit of the switch's features. The web interface simplifies this configuration at all levels.

How to Use This Book

This document describes configuration commands for the GS108T Smart Switch software. The commands can all be accessed from the Web interface.

- Chapter 1, "Getting Started with Switch Management" describes how to use the SmartWizard Discovery utility to set up your switch so that you can communicate with it.
- Chapter 2, "Introduction to the Web Browser Interface" introduces the Web browser interface.
- Chapter 3, "Managing System Settings" describes how to configure the System functions.
- Chapter 4, "Configuring the Switch" describes how to configure the Switch functions.
- Chapter 5, "Managing Firmware and Reset Options" describes the firmware upgrade procedure and reset functions.

- Appendix A, “Specifications and Default Values” gives GS108T Smart Switch specifications and lists default feature values.
- Appendix B, “Virtual Local Area Networks (VLANs)” describes some concepts of VLANs.
- Appendix C, “Network Cabling” gives cabling requirements and describes some details of port cabling connections.

Note: Refer to the product release notes for the GS108T Smart Switch Software application level code. The release notes detail the platform specific functionality of the Switching, SNMP, Config, and Management packages.

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, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
Fixed	Command prompt, CLI text, code
italics	URL links

- **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 GS108T Smart Switch according to these specifications:

Product Version	GS108T Gigabit Smart Switch
Manual Publication Date	May 2007

	Note: Product updates are available on the NETGEAR, Inc. website at *http://www.netgear.com/support*.

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 a 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, choose one of the following options:

- **Printing a Page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.
- **Printing from PDF**. 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*.

– Printing a PDF Chapter.
  - Click the *PDF of This Chapter* link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
  - Click the print icon in the upper left of your browser window.

– Printing a PDF version of the Complete Manual.
  - 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 your browser 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.

Revision History

Part Number	Version Number	Date	Description
202-10249-01	1.0	May 2007	Product created

Chapter 1
Getting Started with Switch Management

This section provides an overview of switch management, including the methods you can choose to start managing your NETGEAR GS108T Gigabit Smart Switch. It also leads you through the steps necessary to get started, using the SmartWizard Discovery utility. The section includes this information under the following headings:

- "System Requirements"
- "Switch Management Interface"
- "Network with a DHCP Server"
- "Network without a DHCP Server"
- "Web Access"
- "Additional Utilities"

System Requirements

The following hardware and software facilities are required to run the applications described in this manual:

- Network facilities:
  - Ethernet network with or without DHCP server as appropriate
  - Ethernet cable to connect the switch to a PC
- For running the SmartWizard Discovery utility and local or remote Web Management:
  - IBM-type PC with CD drive: RAM size and disk specification are not critical
  - OS software: Microsoft Windows Vista, Windows XP, or Windows 2000
  - Desktop computer running Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later, or equivalent

Note: For complete hardware installation instructions, refer to the *GS108T Smart Switch Hardware Installation Guide* included on your *Resource CD*, or go to *http://www.netgear.com/support*.

Switch Management Interface

Your NETGEAR GS108T Gigabit Smart Switch contains an embedded web server and management software for managing and monitoring switch functions. This switch will function as a simple switch without using the management software but its use enables you to configure more advanced features and consequently improve switch efficiency and the overall performance of your network.

Web-Based Management enables you to monitor, configure, and control your switch remotely using a common web browser, instead of having to use expensive and complicated SNMP software products. Simply by using your web browser, you can monitor the performance of your switch and optimize its configuration for your network. Using your browser, for example, you can set up VLANs, traffic priority, and configure port trunking.

In addition, NETGEAR provides the SmartWizard Discovery utility with this product. This program runs under Microsoft Windows XP or Windows 2000 and provides a “front end” that discovers the switches on your network segment. When you power up your switch for the first time, the SmartWizard Discovery utility enables you to configure its basic network parameters without prior knowledge of IP address or subnet mask. Following such configuration, this program leads you into the Web Management interface.

Table 1-1 shows some features of the SmartWizard Discovery utility and Web Management.

Table 1-1. Switch Management Methods

Management Method	Features
SmartWizard Discovery utility	No IP address or subnet mask setup needed Discover all switches on the network User-friendly interface under Microsoft Windows Firmware upgrade capability Password change feature Provides entry to web configuration of switch
Web browser	Password protection Ideal for configuring the switch remotely Compatible with Internet Explorer and Netscape Navigator on any platform Extensive switch configuration possible Configuration backup and restore

For a more detailed discussion of the SmartWizard Discovery utility, continue with this section: “Network with a DHCP Server” or “Network without a DHCP Server” on page 1-4. For a detailed discussion of the Web Browser Interface, see Chapter 2, “Introduction to the Web Browser Interface”.

Network with a DHCP Server

To install the switch in a network with a DHCP server, proceed as follows:

1. Connect the GS108T Smart Switch to a DHCP network.
2. Power on the switch by connecting its AC-DC power adapter.
3. Install the SmartWizard Discovery utility on your computer.
4. Start the SmartWizard Discovery utility.
5. Click **Discover** for the SmartWizard Discovery utility to find your GS108T Gigabit Smart Switch. You should see a screen similar to that shown below.

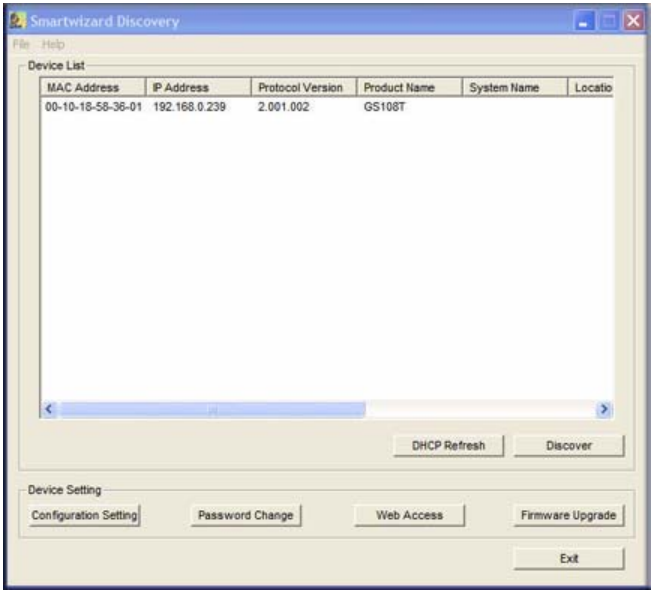


Figure 1-1

6. Make a note of the displayed IP address assigned by the DHCP server. You will need this value to access the switch directly from a web browser (without using the SmartWizard Discovery utility).
7. Select your switch by clicking on the line that shows it. Then click the Web Access button. The discovery utility displays a login window similar to the following:

Figure 1-2

Use your web browser to manage your switch. The default password is ‘password’. Then use this page to proceed to management of the switch covered in Chapter 2, “Introduction to the Web Browser Interface”.

Network without a DHCP Server

This section describes how to set up your switch in a network without a DHCP server, and is divided into the following tasks:

- Manually assign network parameters for your switch
- Configure the NIC settings on the host PC
- Log in to the web-based switch management utility

Manually Assigning Network Parameters

If your network has no DHCP service, you must assign a static IP address to your switch. If you choose, you can assign it a static IP address even if your network has DHCP service. Proceed as follows:

1. Connect the GS108T Gigabit Smart Switch to your existing network.
2. Power on the switch by plugging in the AC-DC power adapter (Default IP is 192.168.0.239).
3. Install the SmartWizard Discovery utility on your computer.
4. Start the SmartWizard Discovery utility.
5. Click **Discover** for the SmartWizard Discovery utility to find your GS108T Gigabit Smart Switch. You should see a screen similar to that shown in Figure 1-1 on page 1-3.
6. Click **Configuration Setting**. A screen similar to that shown below appears.

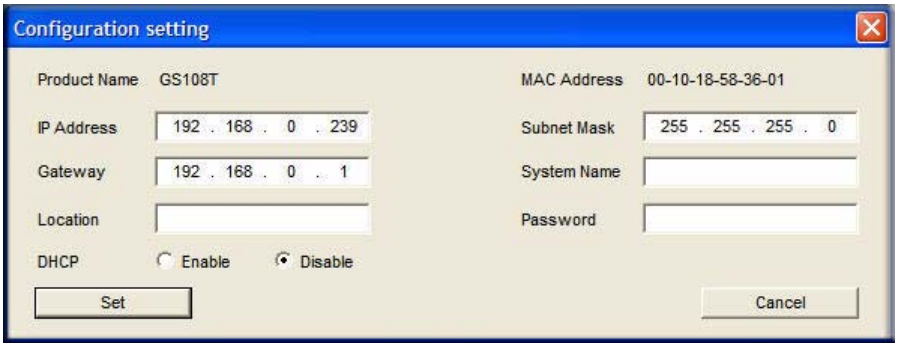


Figure 1-3

7. Choose the **Disable** radio box to disable DHCP.
8. Enter your chosen switch IP address, gateway IP address and subnet mask, and then type your password and click **Set**. Please ensure that your PC and the GS108T Gigabit Smart Switch are in the same subnet. Make a note of these settings for later use.

NIC Setting on the Host that Accesses the GS108T Gigabit Smart Switch

The settings of your network interface card (NIC) under MS Windows OS are made with entries into Windows screen pages similar to the ones shown below. For comparison, the settings pages of the switch are also shown although they do not appear in the Windows view.

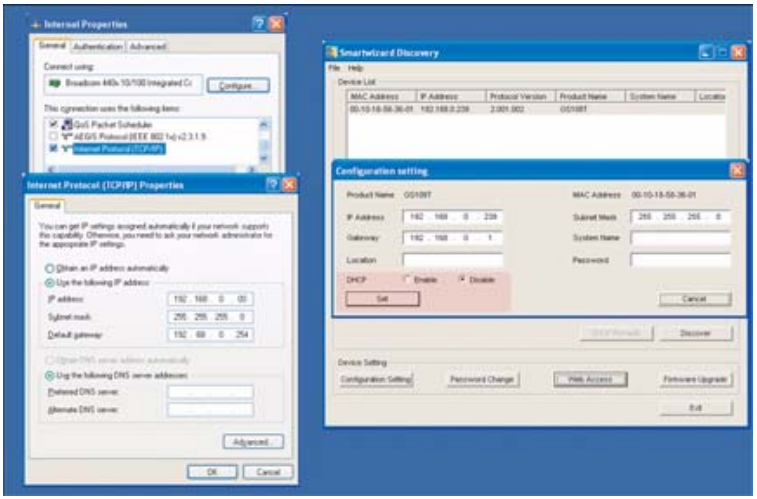


Figure 1-4

You need Windows Administrator privileges to change these settings.

1. On your PC, access the MS Windows operating system TCP/IP Properties.
2. Set IP address and subnet mask appropriately. The subnet mask value should be identical to that set in the switch. The PC IP address must be different from that of the switch but lie in the same subnet.
3. Click **Web Access** in the SmartWizard Discovery utility to enable the management screens as described in the following section.

Web Access

For Web access, you can either:

- Select “Web Access” using the SmartWizard Discovery utility (see “Network with a DHCP Server” or “Network without a DHCP Server”).
- Access the switch directly, without using the SmartWizard Discovery utility.

You must work from the same network segment that contains the switch (i.e., the subnet mask values of switch and PC host must be the same) and you must point your browser using the switch IP address. If you used the SmartWizard Discovery utility to set up IP address and subnet mask, either with or without DHCP server, use that IP address in your browser window.

If you are starting with an “out of the box” switch and are not using the SmartWizard Discovery utility, you must initially configure your host PC to be on a network segment to match the default parameters of the switch, which are:

- IP address: 192.168.0.239
- Subnet Mask: 255.255.255.0

Later, you may want to change the network parameters to match those of your network (this procedure is described in Chapter 3, “Managing System Settings” in “Setup” on page 3-6). Your host PC network parameters must then also be set back to match your network.

Clicking **Web Access** on the SmartWizard Discovery utility or accessing the switch directly displays the page shown below.

Figure 1-5

Use this page to proceed to management of the switch covered in Chapter 2, “Introduction to the Web Browser Interface”.

Additional Utilities

Alternatively, from the main page shown on Figure 1-1 on page 1-3 you can access these additional functions:

- “Password Change”

- “Firmware Upgrade”

Password Change

You can set a new password of up to 20 ASCII characters.

1. Click **Password Change** from the Switch Setting section. The Password Change screen appears. You can set a new password. In this process, you are required to enter the old password and to confirm the new one.
2. Click **Set** to enable the new password.

Firmware Upgrade

	Note: You can also upgrade the firmware using the File Download menu of the switch (see “File Download” on page 5-3).

If you click **Firmware Upgrade** from the main screen (see Figure 1-1 on page 1-3), after you have selected the switch to upgrade, the following screen appears:

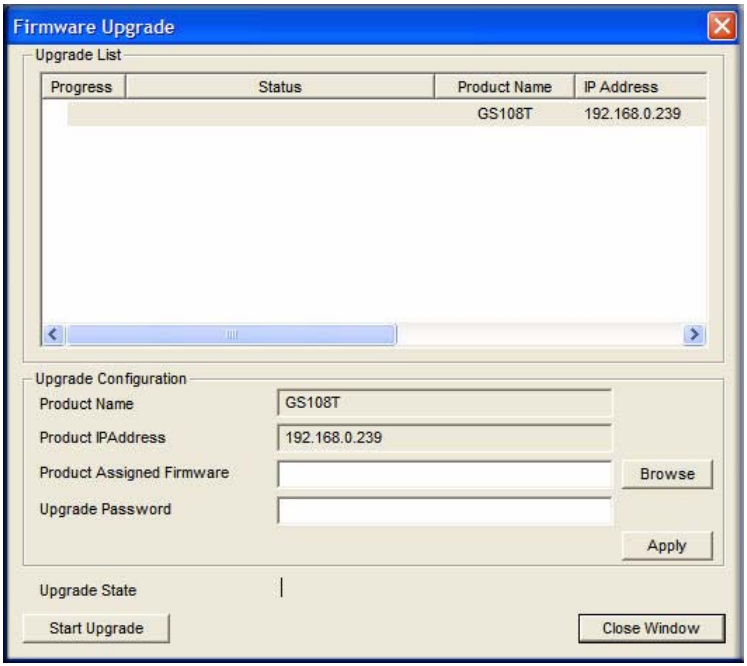


Figure 1-6

The application software for the GS108T Smart Switch is upgradeable, enabling your switch to take advantage of improvements and additional features as they become available. The upgrade procedure and the required equipment are described as follows. This procedure assumes that you have downloaded or otherwise obtained the firmware upgrade and that you have it available as a binary file on your computer. This procedure uses the TFTP protocol to implement the transfer from computer to switch.

1. Enter the following values into the appropriate places in the form:
   - **Firmware Path**: The location of the new firmware. If you do not know the location, you can click Browse to locate the file.
   - **Password**: Enter your password; the default password is ‘password’.
   - **Upgrade State**: Shows upgrading in progress.
2. Click **Start** to begin loading the upgrade. The system software is automatically loaded to all stacking members. When the process is complete, the switch automatically reboots.

Exit

Click **Exit** from the Switch Setting section to close the SmartWizard Discovery utility.

Chapter 2
Introduction to the Web Browser Interface

This section introduces the browser interface that enables you to configure and manage your NETGEAR GS108T Gigabit Smart Switch. Your GS108T Smart Switch provides a built-in browser interface that enables you to configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer or Netscape Navigator. Online Help is also provided for many of the basic functions and features of the switch.

This section introduces the areas of the browser interface and includes the following headings:

- "Logging Into the NETGEAR Home Page"
- "Other Features of the Browser Interface"

Logging Into the NETGEAR Home Page

Begin your overview of the GS108T Smart Switch browser interface by logging in:

1. Start the application, either through the SmartWizard Discovery utility or directly by entering the switch's IP address, as described in Chapter 1, "Getting Started with Switch Management".
2. Press **Enter**. The Login page appears as shown below.

Figure 2-1

3. Enter the password (the factory default is *password*) and click **Login**. The first page of the GS108T Smart Switch browser interface is displayed.

The Navigation Menu

As shown below, logging in brings you to the view of the browser interface.

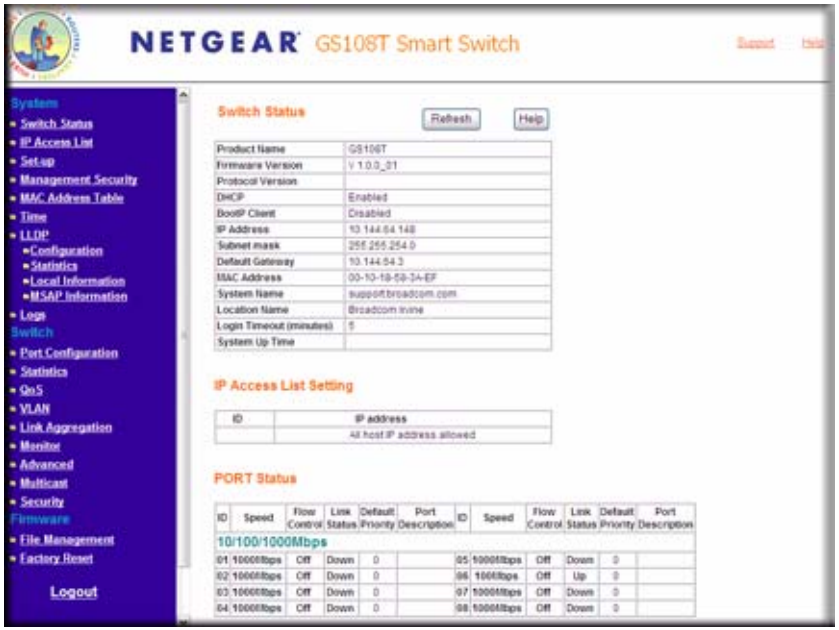


Figure 2-2

The blue navigation menu on the left provides access to all the configuration functions of the switch, and remains constant.

For further description of the functions, refer to the appropriate section of this manual:

- Chapter 3, “Managing System Settings”, which describes how to configure the System functions
- Chapter 4, “Configuring the Switch”, which describes how to configure the Switch functions
- Chapter 5, “Managing Firmware and Reset Options”, which describes the firmware upgrade procedure and reset functions

Other Features of the Browser Interface

The header of the page also includes the following links:

- **Support**: brings up the NETGEAR web site
- **Help**: accesses the Help menu

The blue navigation menu also includes the Logout selection, which logs you out of the browser interface.

Within the various browser interface pages, there are several other buttons that you can use. Their names and functions are listed below:

- **Browse**: Locates a certain path for a desired file
- **Refresh**: Pulls that screen's data from current values on the system
- **Apply**: Submits change request to system and refreshes screen data
- **Add**: Add new entries to table information and refreshes screen data
- **Delete**: Deletes selected entries from table and refreshes screen data
- **Factory Reset**: Restores the system factory default value
- **Help**: Goes to relevant section of the Help menu

Chapter 3
Managing System Settings

Using the System Settings Utility

The Navigation Pane on the left hand side of the home page contains a System Menu that enables you to manage your GS108T Gigabit Smart Switch with features under the following main headings:

- "Switch Status"
- "IP Access List"
- "Setup"
- "Management Security"
- "MAC Address Table"
- "Time"
- "LLDP"
- "Logs"

The description that follows in this chapter covers these features and tells you how to set them in the GS108T Smart Switch.

Switch Status

The Switch Status page reports the settings of the configurable parameters of the switch.

1. Click **System Status** in the blue navigation panel. A screen similar to that shown below appears.

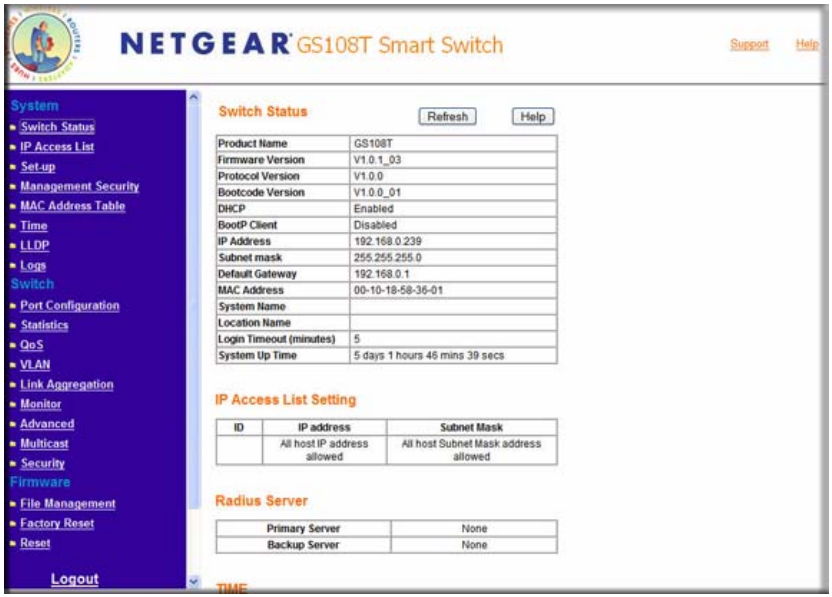


Figure 3-3

2. View the basic system information:
   - **Product name** shows the switch model name.
   - **Firmware Version** displays the software version of the switch.
   - **Protocol Version** is the discovery version of the switch.
   - **DHCP** indicates the enabled/disabled state of DHCP client functionality.
   - **BootP Client** indicates the enabled/disabled state of BootP client functionality.
   - **IP Address** indicates the IP address of the switch.
   - **Subnet Mask** is the subnet mask of the IP address.
   - **Default Gateway** is the IP address of the gateway for the remote manager.
   - **MAC Address** indicates the MAC address of the switch.
   - **System Name** shows the switch name set by user.
   - **Location Name** shows where the switch located.
   - **Login Timeout (minutes)** defines the web login timeout time of the switch.
   - **System Up time** defines the switch up time after boot up.
3. Scroll down to view additional status information:
   - IP Access List Setting

- Radius Server
- TIME
- LLDP Settings
- Logs Configuration
- PORT Status
- IEEE 802.1P QOS Status
- Port Based VLAN Settings
- IEEE 802.1Q PVID
- Link Aggregation
- Monitor
- Jumbo Frame Setting
- Jumbo Frame Disabled
- Rate Limiting
- Storm Control
- IEEE802.1W RSTP Setting
- RSTP Function Disabled
- SNMP Setting
- IGMP Snooping Settings
- Dynamic Multicast Entry Table
- Unknown Multicast Settings
- IEEE 802.1x Port Based Authentication State Settings
- Port Security Settings
- Trusted MAC Settings

IP Access List

The IP Access List page allows you to limit the IP addresses that can access the management portion of the switch. The switch will only respond to requests from computers with an IP address in the list, so include your IP address with their corresponding subnet mask to set this feature.

1. Click **IP Access List** in the blue navigation panel. A screen similar to that shown below appears.

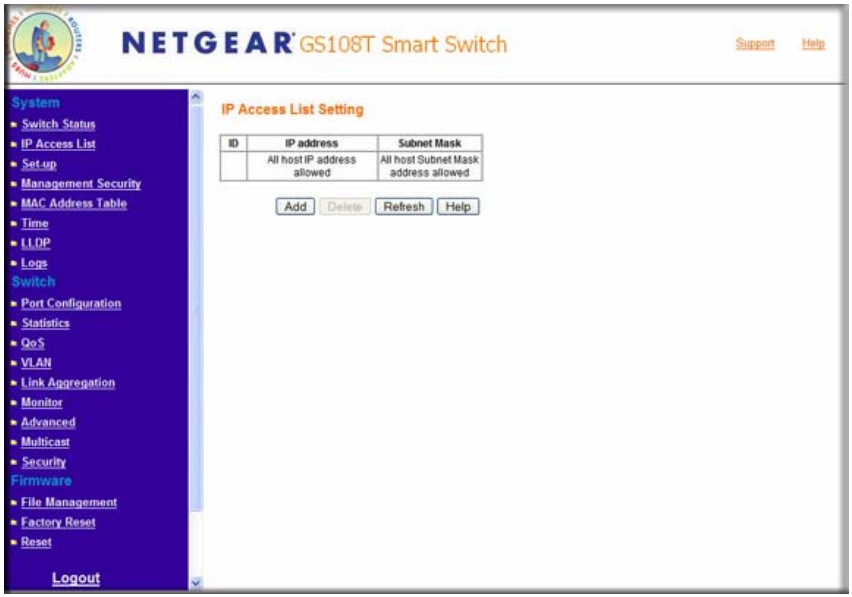


Figure 3-4

2. Add or remove IP addresses on the IP access list.

Adding an IP address to the IP Access List

a. Click **Add** on the IP Access List Setting screen. A screen similar to that shown below appears.

Figure 3-5

b. Input the IP address and subnet mask in the provided field.

c. Click **Apply** to add the IP address and subnet mask.

Removing IP Addresses from the IP Access List

a. Click **Delete** on the IP Access List Setting screen. A screen similar to that shown below appears.

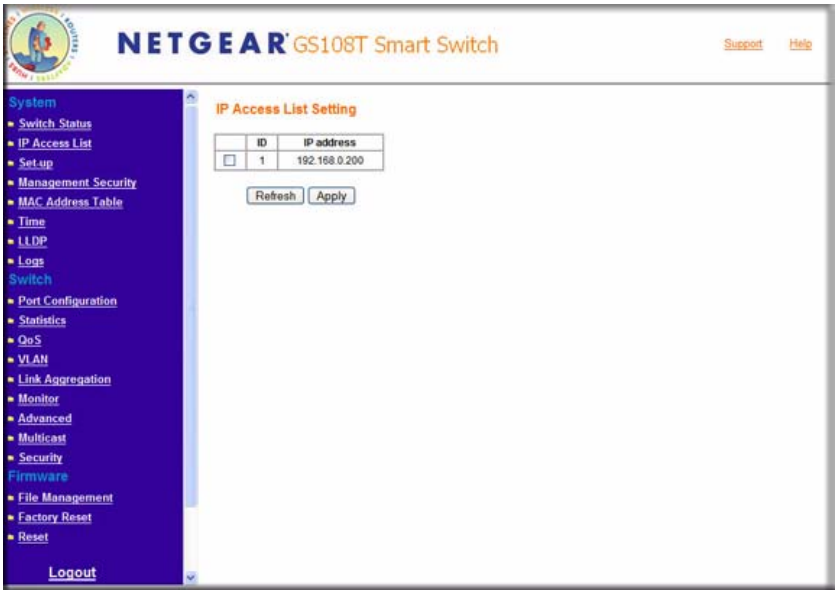


Figure 3-6

b. Check the IP addresses that need to be removed.

c. Click **Apply** to remove the IP addresses.

Setup

The System Setting page lets you give your switch a name and location, as well as other initial configuration settings.

1. Click **Set-up** in the blue navigation panel. A screen similar to that shown below appears.

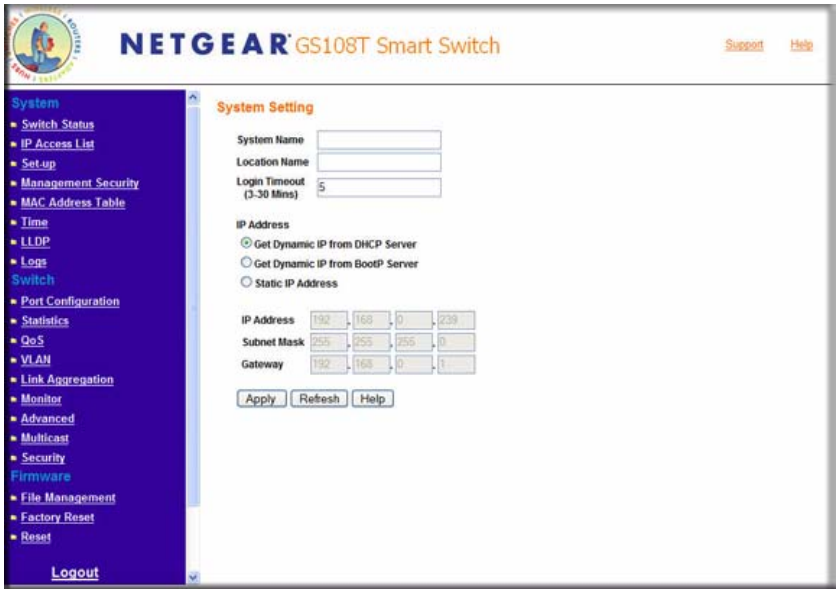


Figure 3-7

2. **System Name:** Assign a system name for the switch. This name is enables you to track your switch.
3. **Location Name:** Assign a location name for the switch. This field assists you in keeping track of which switch you are connected to when you are connected to your switch remotely.
4. **Login Timeout:** Assign a duration for login timeout. User will automatically be logged out if the login session has been idled for the duration. This allows other users to access the switch if one forgets to log out.
5. **IP Address:** Select the system IP address source:
   - **Get Dynamic IP from DHCP Server:** Obtain the IP address via a DHCP server.
   - **Get Dynamic IP from BootP Server:** Obtain the IP address via a BootP server.
   - **Static IP Address:** Manually assign the IP address, subnet mask, and default gateway.
6. Click **Apply** to update the system settings.

Management Security

Click **File Management** in the upper part of the blue navigation panel to expand the item to **Password** and **RADIUS**.

Password

The Password page enables you to change the authentication type and password for the switch.

1. Click **Password** in the blue navigation panel. A screen similar to that shown below appears.

Figure 3-8

2. Specify the authentication procedure:

   a. Select the authentication type from the pulldown menu. The possible field values are:

   - **Local**: Authentication occurs locally.
   - **Radius**: Authentication occurs at the RADIUS server.
   - **None**: No authentication type is applied. A user is allowed to login without any authentication.

   The authentication procedure shows the order by which authentication is performed. If the first authentication type is not available, the second authentication type is used.

Example: If **RADIUS, Local** 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, then authentication is done locally.

b. Click **Apply** to update the authentication procedure.

3. Specify the new password:

a. **Old Password**: Enter the current password to access the switch.

b. **New Password**: Enter the new password to access the switch. The maximum length of password is 15 characters. All printable characters are allowed.

	Note: It is good practice to select a password more than eight characters long and is a combination of numbers and letters. Names and simple words can be easy to guess. If you forget your password, you can always press the **Factory Reset** button on the switch and the password will return to the default value of **password**.

c. **Confirm New Password**: Re-enter the new password.

d. Click **Apply** to update the password.

RADIUS Server

Click **RADIUS Server** in the upper part of the blue navigation panel to expand the item to **Password** and **RADIUS**. Then click **RADIUS** (if necessary) to expand the **Radius** submenu to **Server**.

The RADIUS server is Remote Authentication Dial-In User Service (RADIUS) defined in RFC2865. The server is used by ISPs to authenticate a username and password before authorizing use of the network. You can configure both a primary server and a backup server.

1. Click **Server** in the blue navigation panel. A screen similar to that shown below appears.

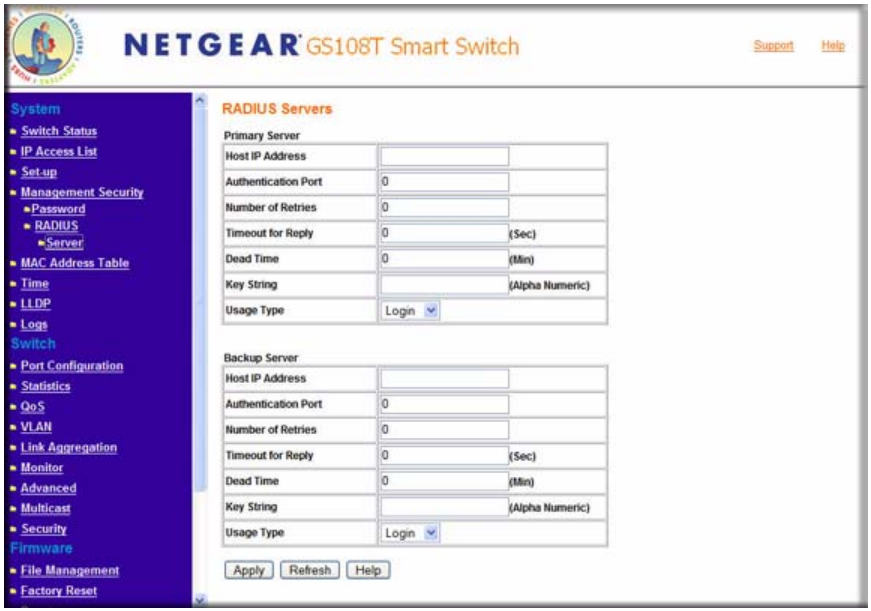


Figure 3-9

2. **Primary Server**: Define the RADIUS Primary Server authentication fields.

   a. **Host IP Addresses**: Specify the IP address of the primary RADIUS server.

   b. **Authentication Port**: Specify the UDP port number of the EAPOL control frame. The default UDP port number is 1812, but other numbers can be used if the RADIUS server can recognize them.

   c. **Number of Retries**: Specify the number of times the switch sends the RADIUS request to the server before giving up.

   d. **Time out for Reply**: Specify the number of seconds the switch waits for the RADIUS server to respond before resending the request.

   e. **Dead Time**: Specify the number of minutes a RADIUS server, that is not responding to authentication requests is to be skipped, thus avoiding the wait for the request to timeout before trying the backup configured server.

   f. **Key String**: Specify the string used by the RADIUS server as a password to identify EAPOL control frames.

   g. **Usage Type**: Select the usage of the radius server. The possible field values are:

      - **Login**: The Radius server is used for logging into switch.

- **802.1x**: The Radius server is used for dot1x authentication.
- **All**: The Radius server is used for both logging in and dot1x authentication.

3. **Backup Server**: Define the RADIUS Backup Server authentication fields in a similar manner.
4. Click **Apply** to update the RADIUS servers.

MAC Address Table

Click **MAC Address Table** in the upper part of the blue navigation panel to expand the item to **Static Address** and **Dynamic Address**.

Static Address

1. Click **Static Address** in the blue navigation panel. A screen similar to that shown below appears.

Figure 3-10

2. Add or remove static addresses on the Static Addresses list.

   Adding a static address to the Static Addresses list

a. Click **Add** on the Static Addresses screen. A screen similar to that shown below appears.

Figure 3-11

b. Input the required information in the provided fields:

- **Interface Port**: Select the interface port to which the entry refers.
- **MAC Address**: Enter the MAC address to which the entry refers.
- **VLAN ID**: Select the VLAN ID number to which the entry refers.

c. Click **Apply** to add the static address.

Removing a static address from the Static Addresses list

a. Check the static addresses on the Static Addresses page that need to be removed.

b. Click **Apply** to remove the static addresses.

Dynamic Address

1. Click **Dynamic Address** in the blue navigation panel. A screen similar to that shown below appears.

Figure 3-12

Querying table entries:

a. Specify how the table is to be queried. The possible field types are as follows:

- **Port**: Specify the interface for which the table is queried.
- **VLAN ID**: Specify the VLAN ID for which the table is queried.
- **MAC Address**: Specify the MAC address for which the table is queried.

b. Click **Query** to query the table entries.

The information returned from the query is display as follows:

- **VLAN ID**: Shows the ID of the current VLAN.
- **MAC Address**: Displays the current MAC address.
- **Interface Port**: Indicates the interface for which the table is currently queried
- **Static/Dynamic**: Indicates whether the entry is static or dynamic

Removing table entries:

a. Enter the VLAN ID and MAC address of the table entry to remove.

b. Click **Remove** to remove the table entries.

Time

SNTP (Simple Network Time Protocol) synchronizes time across the network.

- The time interval at which the switch polls for time is called the *polling time* and is set to 30 minutes. As long as the NTP/SNTP server is reachable, the switch polls for time every 30 minutes and updates the system time.
- The time out period is the time duration for which the switch will wait for a reply from the server. Time out is set to 15 seconds. If two NTP/SNTP servers are specified and neither one is available, then the total time out will be 30 seconds.

You can specify whether to set the system time manually or with an SNTP server.

1. Click **Time** in the blue navigation panel. A screen similar to that shown below appears.

Figure 3-13

2. **Clock Source:** Select the method to set the date and time:
   - Manually: Click **Local Settings**.
   - SNTP Server: click **SNTP**.
3. **Timezone Offset:** Select the local time zone in which the switch is operating.

4. When setting the date and time manually:
   a. **Date:** Specify the date to which the switch is set in DD/MM/YYYY format.
   b. **Local Time:** Specify the switch time in HH:MM:SS format.
5. When setting the date and time with the SNTP server:
   a. **NTP Server IP - 1:** Specify the IP address of the primary NTP/SNTP Server for the switch to use when synchronizing time.
   b. **NTP Server IP - 2:** Specify the IP address of alternate NTP/SNTP Server for the switch to use when synchronizing time.
6. Click **Apply** to update the time settings.

LLDP

Click **LLDP** (Link Layer Discovery Protocol) in the upper part of the blue navigation panel to expand the item to **Configuration**, **Statistics**, **Local Information**, and **MSAP Information**.

LLDP Configuration

LLDP is a one way protocol.

- An LLDP agent can transmit information about the capabilities and current status of the switch associated with its MSAP (MAC Service Access Point) identifier.
- The LLDP agent can also receive information about the capabilities and current status of the switch associated with a remote MSAP identifier.

However, LLDP agents are not provided with any means of soliciting information from other LLDP agents via this protocol.

Switch Settings

1. Click **Configuration** in the blue navigation panel. A screen similar to that shown below appears.

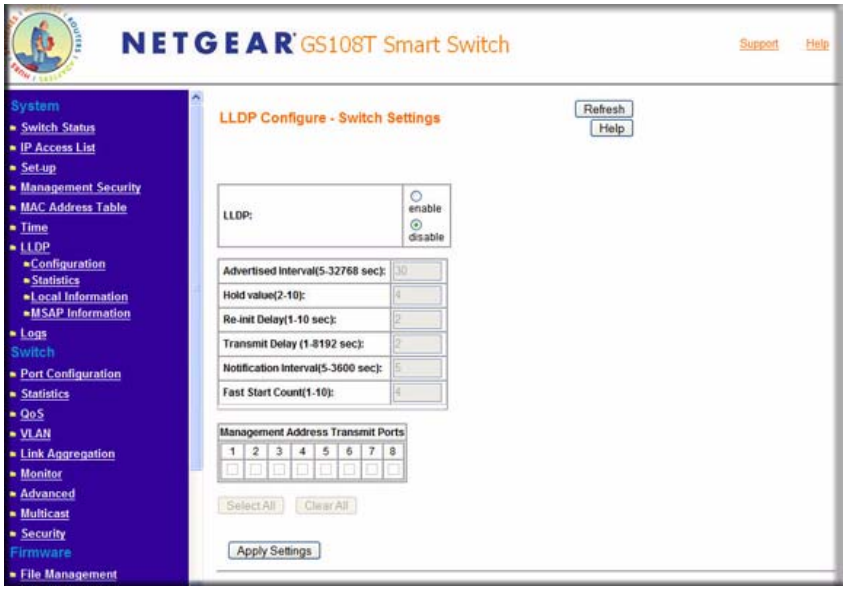


Figure 3-14

The following LLDP configuration information is displayed:

- **Advertised Interval**: The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
- **Hold value**: A multiplier to Advertised interval. The result would be the TTL value for the information advertised.
- **Re-init Delay**: The minimum delay period before from the time a ports becomes disabled until re-initialization.
- **Transmit Delay**: The delay between successive LLDP frame transmissions initiated by value/ status changes in the local system.
- **Notification Interval**: The interval at which notification are generated when remote MSAP information changes.
- **Fast Start Count**: Indicates the number of successive LLDP frame transmissions for one complete Fast Start interval. The default value 4.
- **Management Address Transmit Ports**: Indicates the ports on which the management address will be transmitted.

Port Configuration

A screen similar to that shown below is located near the bottom of the LLDP Configuration Switch Settings screen.

Switch Port Settings

Port	Admin State	SNMP Notification	MED Fast Start Notification	Optional Enabled TLVs			
				Basic	802.1	802.3	MED
1	DISABLED	DISABLED	DISABLED	--	--	--	--
2	DISABLED	DISABLED	DISABLED	--	--	--	--
3	DISABLED	DISABLED	DISABLED	--	--	--	--
4	DISABLED	DISABLED	DISABLED	--	--	--	--
5	DISABLED	DISABLED	DISABLED	--	--	--	--
6	DISABLED	DISABLED	DISABLED	--	--	--	--
7	DISABLED	DISABLED	DISABLED	--	--	--	--
8	DISABLED	DISABLED	DISABLED	--	--	--	--

Figure 3-15

The following information about LLDP configuration for a port is displayed:

- **Admin Status:** The administratively desired status of the local LLDP agent.
- **Notification Enable:** Indicates whether or not notifications from the agent are enabled.
- **MED Notification Enable:** Indicates whether or not MED notifications from the agent are enabled.
- **Optional TLVs Tx Enabled:** Indicates which TLVs are enabled for transmission.

Table 3-1. Legends for Optional Enabled TLVs

Category	*Legend*	*Meaning*
Basic	P	Port Description
	N	System Name
	D	System Description
	C	System Capabilities
802.1	P	Port Vlan ID
802.3	M	MAC/PHY Configuration/Status
	L	Link aggregation
	F	Frame size

Table 3-1. Legends for Optional Enabled TLVs (continued)

Category	*Legend*	*Meaning*
MED	C	Capabilities
	N	Network Policy
	L	Location ID
	M	MDI
	I	Inventory

LLDP Group Port Configuration

The LLDP Group port configuration allows user to configure a group of ports at a time. Configured values will be applied only to selected ports of the switch.

LLDP Statistics

1. Click **Statistics** in the blue navigation panel. A screen similar to that shown below appears.

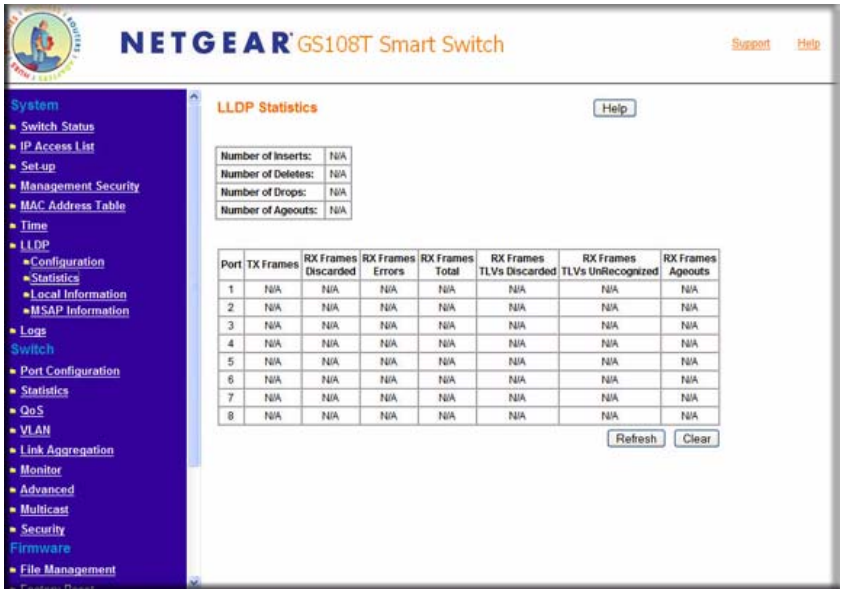


Figure 3-16

The following LLDP statistics are displayed:

- **Number of Inserts**: Total number of Inserts.

- **Number of Deletes**: Total number of deletes.
- **Number of Drops**: Total LLDP frames dropped.
- **Number of Ageouts**: Total LLDP Ageouts occurred.
- **Tx Frames**: Total number of LLDP frames transmitted from a given port.
- **Rx Frames Discarded**: Total number of received and discarded LLDP frames on a given port.
- **Rx Frames Errors**: Total number of error LLDP frames received, on a given port.
- **Rx Frames Total**: Total number of LLDP frames received on a given port.
- **Rx Frames TLVs Discarded**: Total number of TLVs discarded in received LLDP frames on a given port.
- **Rx Frames TLVs Unrecognized**: Total number of TLVs unrecognized in received LLDP frames, on a given port.
- **Rx Frames Ageouts**: Total Ageouts of received LLDP frames on a given port.

Local Information

1. Click **Local Information** in the blue navigation panel. A screen similar to that shown below appears.

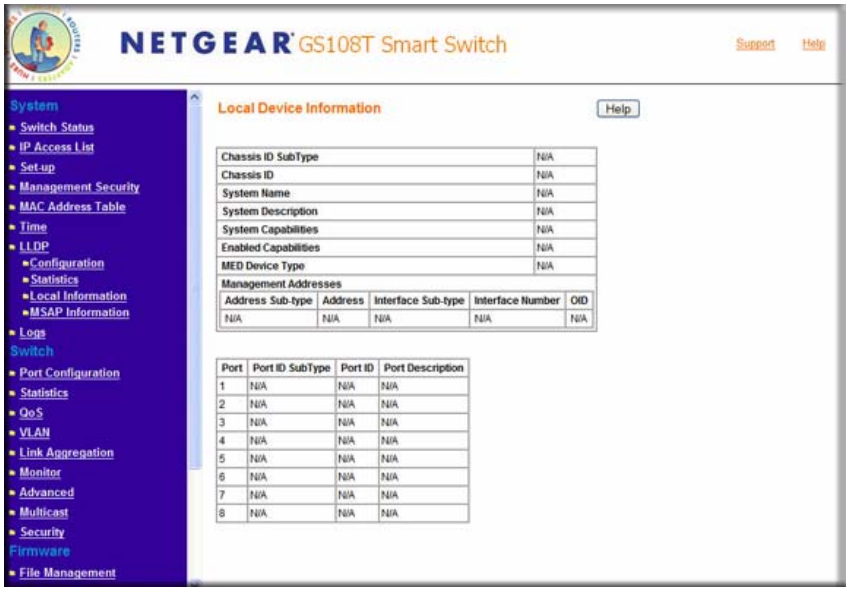


Figure 3-17

The following LLDP local information is displayed:

- **Chassis ID SubType**: Indicates the basis for the Chassis ID entity.
- **Chassis ID**: Identifier for the particular chassis in the System.
- **System Name**: Administratively assigned system name.
- **System Description**: Textual description of the network entity, including the full name and version identification of the system's hardware type.
- **System Capabilities**: Identifies the primary functions of the system.
- **Enabled Capabilities**: Identifies which of the primary functions are enabled.
- **MED Device Type**: Indicates whether the device is a MED device.
- **Management Address**: The address associated with the LLDP agent that may be used to reach higher layer entities to assist discovery by network management.

Table 3-2. Management Address

Item	Description
Address Sub Type	Indicates type of address that is listed in the management address field.
Interface Sub Type	Numbering method used for defining the interface number.
Interface Number	Identifies specific address associated with the management address.
OID	Type of hardware component or protocol entity associated with the given management address.

- **Port**: Local port number.
- **Port ID SubType**: The basis for the identifier that is listed in the Port ID field.
- **Port ID**: Identifier for the port from which LLDPDU was transmitted.
- **Port Description**: Indicates the port’s description.

The following LLDP local port information is displayed:

- **Port ID SubType**: The basis for the identifier that is listed in the Port ID field.
- **Port ID**: Identifier for the port from which LLDPDU was transmitted.
- **PVID**: Port VLAN ID.

Table 3-3. 802.3 Set Details

Item	Description
Auto Negotiation	If auto-negotiation supported and enabled in both the systems, there should be no speed difference.
Aggregator Status	Ports through which LLDPDU is transmitted is aggregated or not.
Aggregator ID	Port ID information for the aggregated port.
Maximum Frame Size	Maximum size of a frame that can be transmitted.

Table 3-4. MED Set Details

Item	Description
Capabilities	LLDP-MED Capabilities are specific to LLDP-MED Devices, advertisement of this TLV by Endpoints enables LLDP-MED capable Network Connectivity Devices to definitively determine support of LLDP-MED by Endpoints they are connecting to.
Device Type	A specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device.
Location Format	Indicates the specific Location ID data format being delivered in the Location ID field.
Location ID	Three Location ID data formats are defined. • Coordinate-based LCI data format • Civic Address LCI data format • ECS ELIN data format
Power Type	The Power Type field represents, whether LLDP-MED device transmitting the LLDPDU is a Power Sourcing Entity (PSE) or Power Device (PD).
Power Source	The Power Source field represents the power source being utilized by a PSE or PD device.
Power Priority	The Power Priority represents the priority of the PD type device to the power being supplied by the PSE type device, or the power priority associated with the PSE type device's port that is sourcing the power via MDI.

Table 3-4. MED Set Details (continued)

Item	Description
Power Value	Indicates the total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
Network Policy	Network policy is associated with multiple sets of application types supported on a given port. • **Application Type**: Integer value indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. • **Unknown Policy Flag**: Indicates that an Endpoint Device wants to explicitly advertise that, this policy is required by the device, but is currently unknown. • **Tagged Flag**: Indicates whether the specified application type is using a tagged or an untagged VLAN. • **Reserved**: Reserved for future standardization. • **VLAN ID**: Contains the VLAN identifier (VID) for the port. • **L2 Priority**: Indicates the Layer 2 priority to be used for the specified application type. • **DSCP Value**: Contains the DSCP value to be used to provide Diffserv node behavior for the specified application type.

MSAP (Remote) Information

1. Click **MSAP Information** in the blue navigation panel. A screen similar to that shown below appears.

Figure 3-18

The following LLDP remote information is displayed:

- **Local Port**: Port on which LLDPDU was received.
- **Chassis ID SubType**: Indicates the basis for the Chassis ID entity.
- **Chassis ID**: Identifier for the particular chassis in the System.
- **Port ID SubType**: The basis for the identifier that is listed in the Port ID field.
- **Port ID**: Identifier for the port from which LLDPDU was transmitted.

The following LLDP Remote Device Information is displayed:

- **Port ID SubType**: The basis for the identifier that is listed in the Port ID field.
- **Port ID**: Identifier for the port from which LLDPDU was transmitted.
- **PVID**: Port VLAN ID.

Table 3-5. 802.3 Set Details

Item	Description
Auto Negotiation	If auto-negotiation supported and enabled in both the systems, there should be no speed difference.
Aggregator Status	Ports through which LLDPDU is transmitted is aggregated or not.

Table 3-5. 802.3 Set Details (continued)

Item	Description
Aggregator ID	Port ID information for the aggregated port.
Maximum Frame Size	Maximum size of a frame that can be transmitted.

Table 3-6. MED Set Details

Item	Description
Capabilities	LLDP-MED Capabilities are specific to LLDP-MED Devices, advertisement of this TLV by Endpoints enables LLDP-MED capable Network Connectivity Devices to definitively determine support of LLDP-MED by Endpoints they are connecting to.
Device Type	A specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device.
Location Format	Indicates the specific Location ID data format being delivered in the Location ID field.
Location ID	Three Location ID data formats are defined. • Coordinate-based LCI data format • Civic Address LCI data format • ECS ELIN data format
Power Type	The Power Type field represents, whether LLDP-MED device transmitting the LLDPDU is a Power Sourcing Entity (PSE) or Power Device (PD).
Power Source	The Power Source field represents the power source being utilized by a PSE or PD device.
Power Priority	The Power Priority represents the priority of the PD type device to the power being supplied by the PSE type device, or the power priority associated with the PSE type device's port that is sourcing the power via MDI.
Power Value	Indicates the total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
Hardware Revision	Alphanumerical string that contains the hardware revision of the endpoint.
Firmware Revision	Alphanumerical string that contains the firmware revision of the endpoint.
Software Revision	Alphanumerical string that contains the software revision of the endpoint.
Serial Number	Alphanumerical string that contains the serial number of the endpoint.

Table 3-6. MED Set Details (continued)

Item	Description
Model Name	Alphanumerical string that contains the model name of the endpoint.
Asset ID	Alphanumerical string that contains the asset identifier of the endpoint.
Network Policy	Network policy is associated with multiple sets of application types supported on a given port. • **Application Type**: Integer value indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. • **Unknown Policy Flag**: Indicates that an Endpoint Device wants to explicitly advertise that, this policy is required by the device, but is currently unknown. • **Tagged Flag**: Indicates whether the specified application type is using a tagged or an untagged VLAN. • **Reserved**: Reserved for future standardization. • **VLAN ID**: Contains the VLAN identifier (VID) for the port. • **L2 Priority**: Indicates the Layer 2 priority to be used for the specified application type. • **DSCP Value**: Contains the DSCP value to be used to provide Diffserv node behavior for the specified application type.

- **Unknown TLVs**: Unrecognized TLVs.

Logs

Click **Logs** in the upper part of the blue navigation panel to expand the item to **Logs Configuration**, **Memory Logs**, **Flash Logs**, and **Server Logs**.

Three types of media are provided for saving the logs:

- The RAM medium uses a fixed block of memory to store logs. It's volatile (i.e., the logs will be cleared after system reboot).
- The flash medium uses one or more sectors of flash memory to store logs. It's non-volatile but considered relatively slow.
- The server medium is a remote host with BSD syslogd compliant daemon running. It uses the UDP protocol to send log messages to the remote server.

Logs Configuration

Logs are used to record various events in the system. By configuring logging system, you can control how many and what log messages are recorded for later reference.

1. Click **Logs Configuration** in the blue navigation panel. A screen similar to that shown below appears.

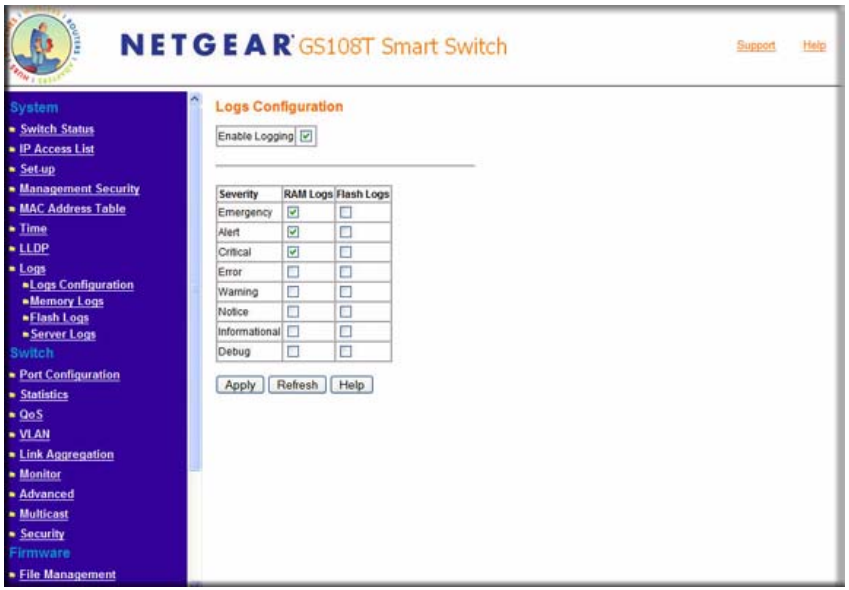


Figure 3-19

2. Click **Enable Logging** to enable logging.
3. Click the desired severity levels for the RAM and flash logs. See "Server Logs" for how to configure the server logs.
4. Click **Apply** to update the logs configuration.

Memory Logs

1. Click **Memory Logs** in the blue navigation panel. A screen similar to that shown below appears.

Figure 3-20

A log consists of the following fields:

- **Index** indicates the global sequence number for the log.
- **Time** indicates the time when the log is recorded.
- **Level** indicates the severity of the log.
- **Message** shows the detailed description of the log.

2. Click **Clear Logs** to clear the memory logs.

Flash Logs

1. Click **Flash Logs** in the blue navigation panel. A screen similar to that shown below appears.

Figure 3-21

A log consists of the following fields:

- **Index** indicates the global sequence number for the log.
- **Time** indicates the time when the log is recorded.
- **Level** indicates the severity of the log.
- **Message** shows the detailed description of the log.

2. Click **Clear Logs** to clear the flash logs.

Server Logs

The Server medium is a remote host with a BSD syslogd compliant daemon running. The switch uses the UDP protocol to send log messages to the remote server.

1. Click **Server Logs** in the blue navigation panel. A screen similar to that shown below appears.

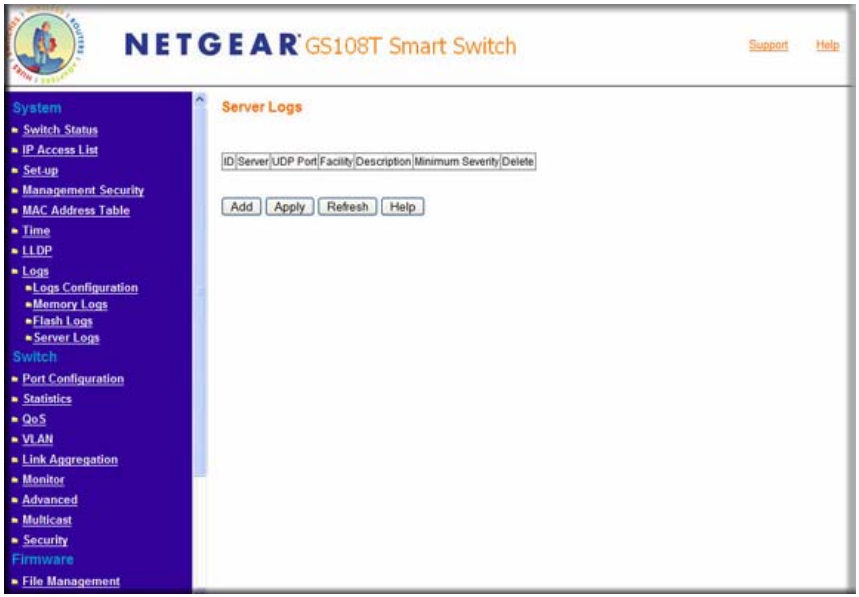


Figure 3-22

The following information is available for each server log:

- **ID**: ID of the server log given by the system.
- **Server**: IP Address of the remote server.
- **UDP Port**: UDP port number to connect with the server.
- **Facility**: Type of facility.
- **Description**: Description of server log.
- **Minimum Severity**: All levels of severity above this minimum severity will be included for logging.

2. Add or remove server logs on the Server Logs list.

Adding a server log to the Server Logs list

a. Click **Add** on the Server Logs screen. A screen similar to that shown below appears.

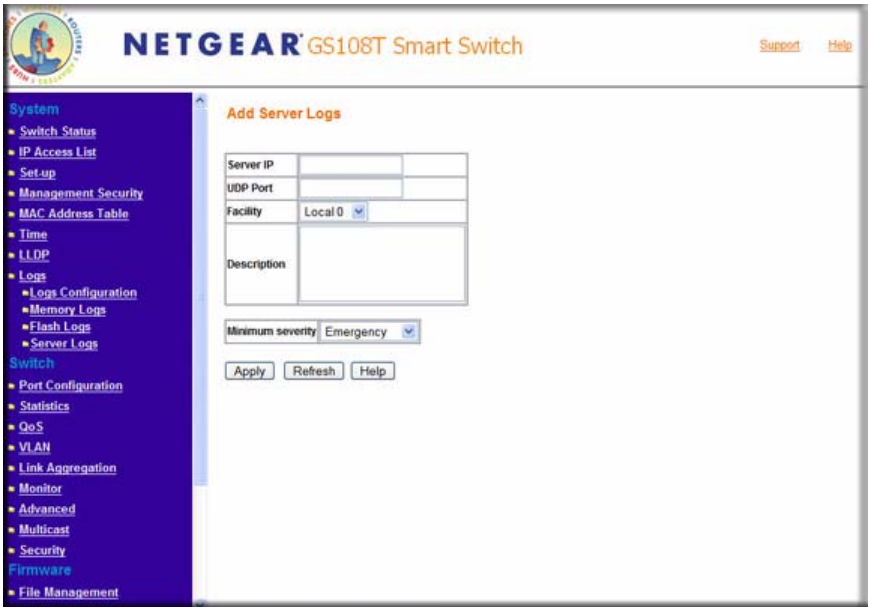


Figure 3-23

b. Input the required information in the provided fields:

- **Server IP**: Input a valid IP Address for the remote server.
- **UDP Port**: Input the UDP port number to connect with the server.
- **Facility**: Input the type of facility. Select any one from the given eight facility types.
- **Description**: Give the description of server log (limit is 256 characters).
- **Minimum Severity**: Select the desired log level from the given eight log levels (e.g., Emergency, Alert, Critical, Error, Warning, Notice, Informational, or Debug).

c. Click **Apply** to add the server log.

Removing a server log from the Server Logs list

a. Check the server logs on the Server Logs page that need to be removed.

b. Click **Apply** to remove the server logs.

Chapter 4
Configuring the Switch

Using the Switch Configuration Utility

The Navigation Pane on the left hand side of the home page contains a Switch Menu that enables you to manage your GS108T Gigabit Smart Switch with features under the following main headings:

- "Port Configuration"
- "Statistics"
- "QoS"
- "VLAN"
- "Link Aggregation"
- "Monitor"
- "Advanced"
- "Multicast"
- "Security"

The description that follows in this chapter covers these features and tells you how to configure them in the GS108T Smart Switch.

Port Configuration

The Port Configuration screen defines speed, duplexing, and flow control operation for a port when auto-negotiation is off. When auto-negotiation is on, those data are negotiated from the link partner. Otherwise, enable or disable ports to control packet forwarding.

1. Click **Port Configuration** in the blue navigation panel. A screen similar to that shown below appears.

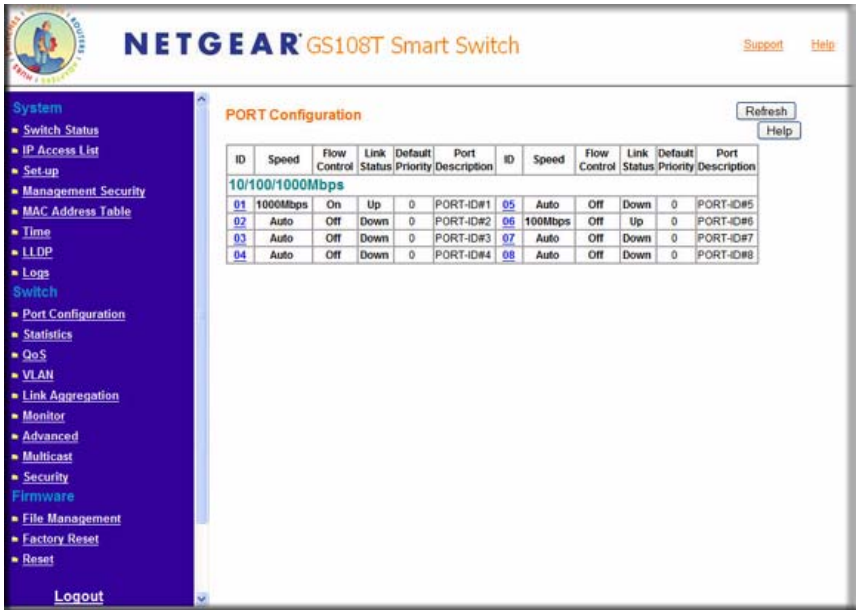


Figure 4-24

The following port configuration settings are displayed for all of the ports:

- **ID** indicates the port number.
- **Speed** indicates duplex speed for the port.
- **Flow Control** indicates whether flow control on or off.
  - When the flow control for a port is enabled, it would send out a pause frame or a jam packet if it is over-subscribed.
  - When this port receives a pause frame, it halts for a certain period before sending out a frame.
- **Link Status**: Indicates whether the link is up/down.
- **Default Priority** indicates the packet priority for packets arriving at the port without tagging.

  If the packet comes in with tag or priority-tag, the priority is retrieved from the priority field of the tag.
- **Port Description**: Provides a description of the port.

2. To change a port, select the port number. A screen similar to that shown below appears.

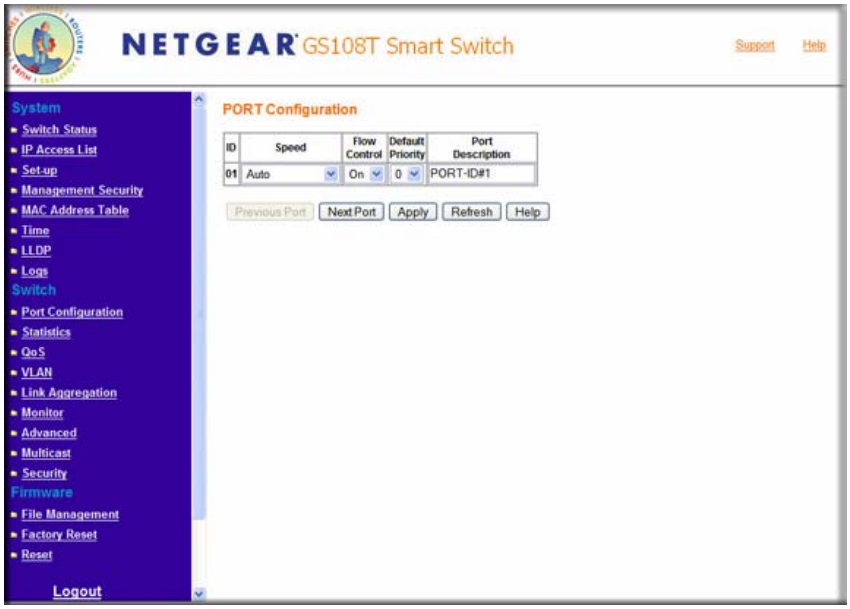


Figure 4-25

ID indicates the port number to control.

3. Specify the new port configuration information:

- **Speed**: Specifies the speed and duplex for the port. The possible entries are:
  - **Auto** (auto-negotiation)
  - **10M Half** (10 Mbps half duplex)
  - **10M Full** (10 Mbps full duplex)
  - **100M Half** (100 Mbps half duplex)
  - **100M Full** (100 Mbps full duplex)
  - **1Gbps Full** (1 Gbps Full duplex)
  - **Disable** (Disable)
- **Flow Control:** Specify whether flow control support is:
  - **On** (enabled)
  - **Off** (disabled)
- **Default Priority**: Assigns packet priority for packets arriving at the port without tagging.

  If the packet comes in with tag or priority-tag, the priority is retrieved from the priority field of the tag.

- **Port Description**: Indicates the description for the port.

4. Click **Next Port** to set the configuration settings of the next port.
5. Click **Apply** to update the port configuration settings.

Statistics

This page shows information from each port's internal counters.

1. Click **Statistics** in the blue navigation panel. A screen similar to that shown below appears.

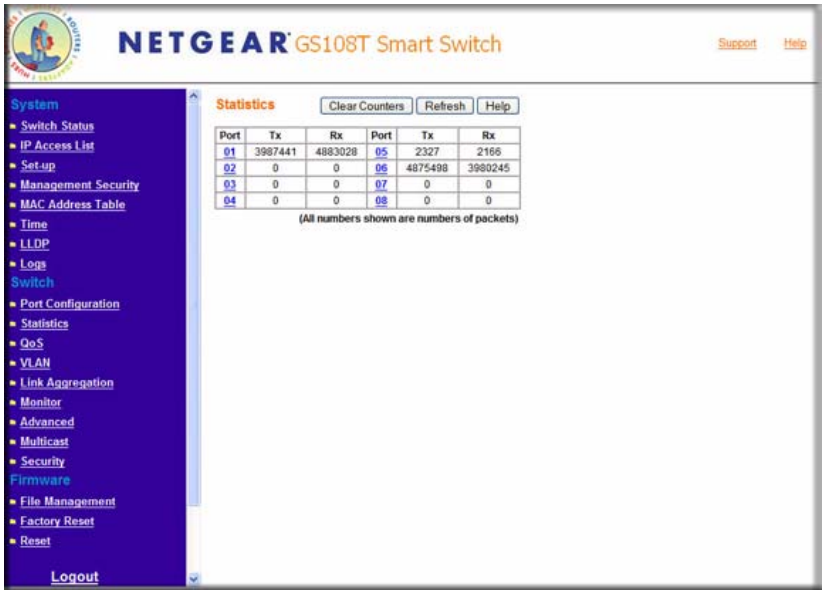


Figure 4-26

The following statistics are displayed for all of the ports:

- **Tx** indicates total packets transmitted from a port.
- **Rx** indicates total packets received from a port.

Clear Counters resets all counters to zero.

Refresh retrieves current count from the device and updates the page.

2. To view an individual port in detail, click that port number. A screen similar to that shown below appears.

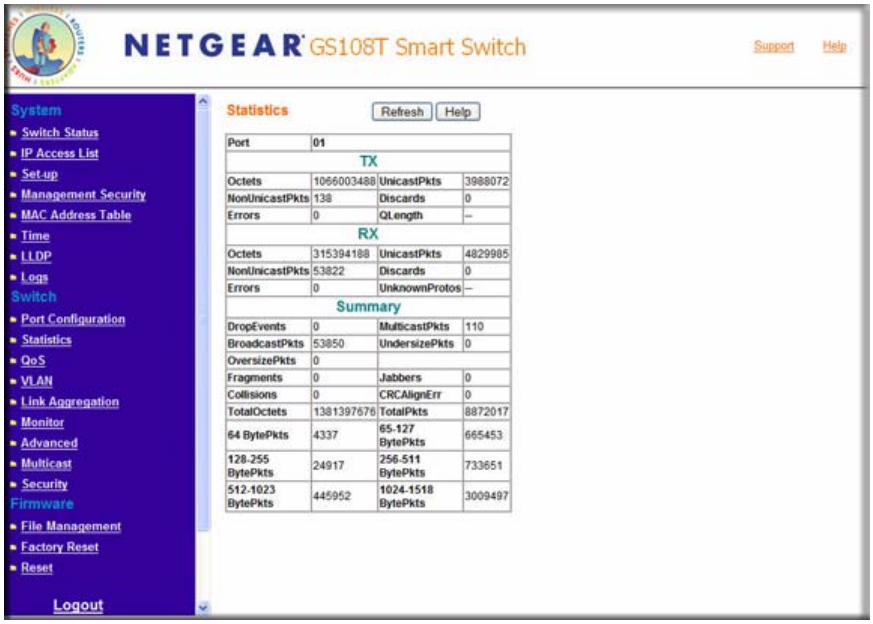


Figure 4-27

Port indicates the port number statistics being displayed.

3. View the statistics per port:

TX statistics

- **Octets**: indicates total octets transmitted.
- **UnicastPkts**: indicates transmitted unicast packets.
- **NonUnicastPkts**: indicates transmitted non-unicast packets.
- **Discards**: indicates discarded packets.
- **Errors**: indicates excessive collision packets.
- **QLength**: indicates count of packets currently buffered.

RX statistics

- **Octets**: indicates total octets transmitted.
- **UnicastPkts**: indicates transmitted unicast packets.
- **NonUnicastPkts**: indicates transmitted non-unicast packets.
- **Discards**: indicates discarded packets.
- **Errors**: indicates undersize/fragment/FCS error/oversized with good FCS packets.

- **UnkonwnProtos**: indicates received packets using unknown protocols.

Summary statistics

- **DropEvents**: indicates packets which are dropped due to GBP or backpressure discard.
- **MulticastPkts**: indicates transmitted/received multicast packets.
- **BrodcastPkts**: indicates transmitted/received broadcast packets.
- **UndersizePkts**: indicates received packets with length less than minimum packet size.
- **OversizePkts**: indicates received packets with length more than maximum packet size.
- **Fragments** indicates received packets (length 10 ~ 63 bytes) with invalid FCS or alignment error.
- **Jabbers**: indicates received packets (invalid FCS or code error) which exceed counter maximum size to maximum receive frame length.
- **Collisions**: indicates total transmitted collision packets.
- **CRCAlignErr**: indicates received packets (invalid FCS) which lengths are between 64 bytes to counter maximum size.
- **TotalOctets**: indicates total received (excluding framing bits, but including FCS bytes) and transmitted (including fragments of frames that were involved with collisions, but excluding preamble/SFD or jam bytes) byte.
- **TotalPkts**: indicates total received and transmitted packet count (including bad packets, all unicast, broadcast, multicast and MAC control packets).
- **64 BytePkts**: indicates transmitted packets with packet length less than or equal to 64 bytes.
- **65-127 BytePkts**: indicates transmitted packets with packet length between (include) 65 ~ 127 bytes.
- **128-255 BytePkts**: indicates transmitted packets with packet length between (include) 125 ~ 255 bytes.
- **256-511 BytePkts**: indicates transmitted packets with packet length between (include) 256 ~ 511 bytes.
- **512-1023 BytePkts**: indicates transmitted packets with packet length between (include) 512 ~ 1023 bytes.
- **1024-1518 BytePkts**: indicates transmitted packets with packet length between (include) 1024 ~ 1518 bytes.

4. Click **Refresh** to update the port statistics.

QoS

There are two possible priority tag settings for the quality of service:

- **802.1p Based**: The eight priority tags specified in IEEE 802.1p (p0 to p7). The QoS setting enables users to map each of the eight priority levels to one of four internal hardware priority queues: High, Normal, Low, and Lowest.
- **DSCP Based**: The six most significant bits of the DiffServ field are called the DSCP (Differentiated Services Code Point). Map the DSCP value to one of the eight priority levels (p1 to P7) of IEEE 802.1p. Then, assign the IEEE 802.1p priority level to one of the four internal hardware queues.

The switch empties the four hardware priority queues in order, beginning with the highest priority queue to the lowest priority queue. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets.

1. Click **QoS** in the blue navigation panel.
   - A screen similar to that shown below appears when **IEEE 802.1p Based** is selected for the QoS.

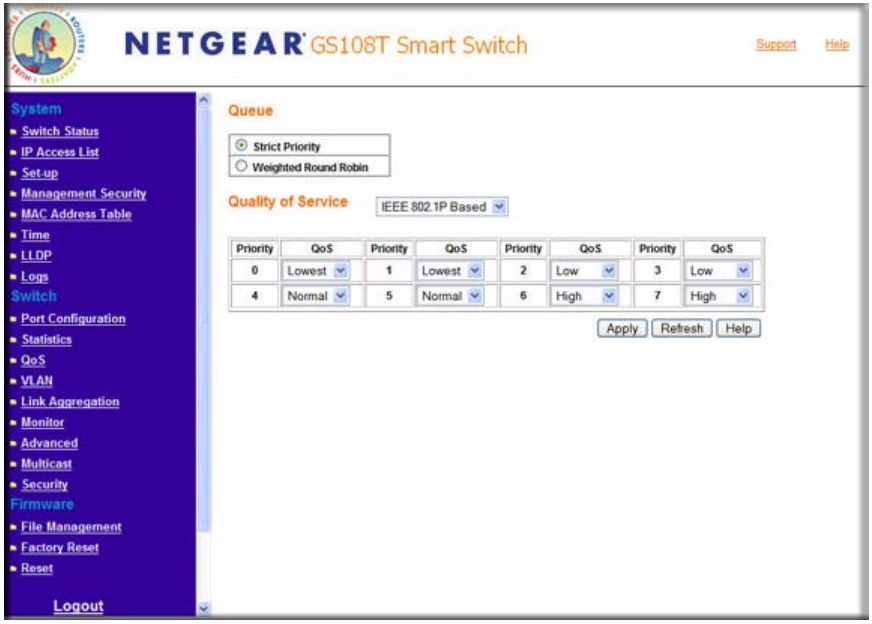


Figure 4-28

- A screen similar to that shown below appears when **DSCP Based** is selected for the QoS.

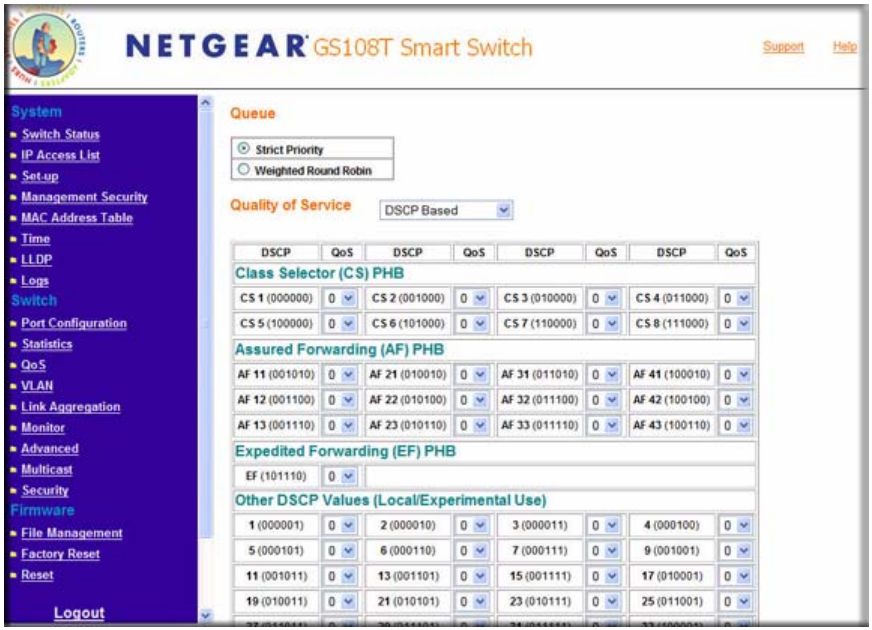


Figure 4-29

2. Specify the **Queue** setting:
   - Strict Priority
   - Weighted Round Robin
3. Select the **Quality of Service** setting:
   - 802.1p Based
   - DSCP Based
4. Click **Apply** to update the QoS settings.

VLAN

Click **VLAN** in the middle part of the blue navigation panel to expand the item to **VLAN Group Setting** and **Management VLAN**.

VLAN Group Setting

Possible VLAN group settings include IEEE 802.1Q VLAN and port-based VLAN.

IEEE 802.1Q VLAN

The settings on the IEEE 802.1Q VLAN page control the VLAN membership of each port for transmitting packets. Also, these settings determine if transmitted packets from each port are tagged with the VLAN ID and other information. The switch supports 64 Tag-based VLANs.

By default, every port is a member of VLAN 1 and so they have a Port VLAN ID (PVID) of 1.

Click **VLAN Group Setting** in the blue navigation panel. A screen similar to that shown below appears when **IEEE 802.1Q VLAN** is selected for the VLAN group setting.

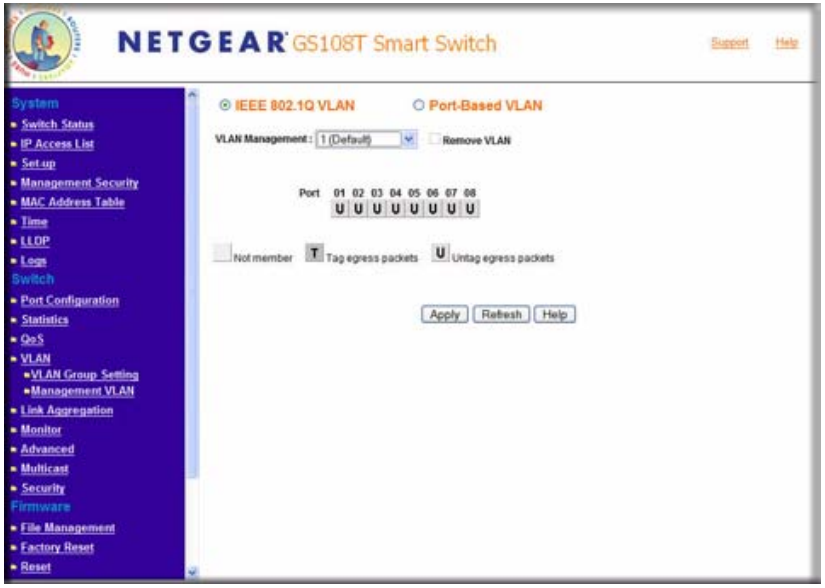


Figure 4-30

You can add, change, or delete VLANs and ports.

To create a new VLAN Group:

1. Select **Add new VLAN** in the pulldown menu. A screen similar to that shown below appears.

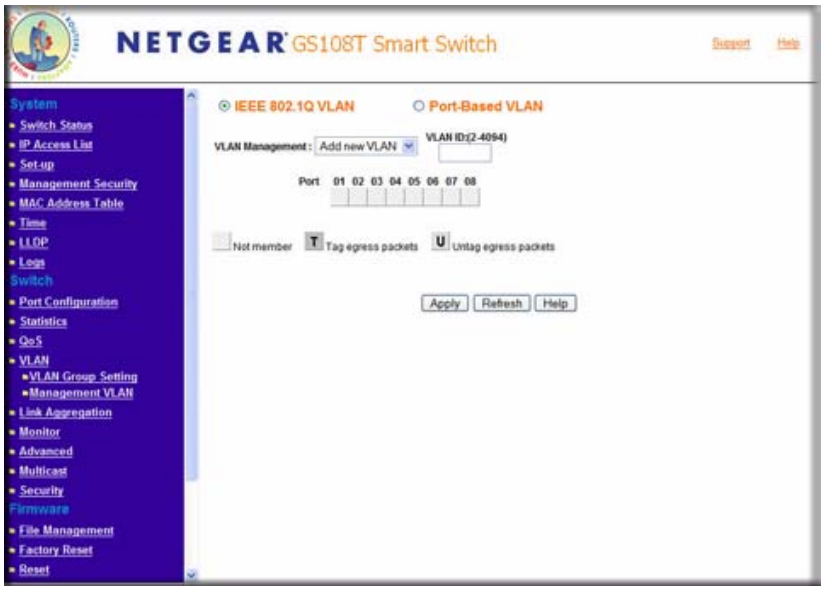


Figure 4-31

2. Input the VLAN ID in the provided field.
3. Add VLAN members as desired.
4. Click **Apply**.

To delete a VLAN Group:

1. Select the **VLAN ID** for the VLAN you want to delete.

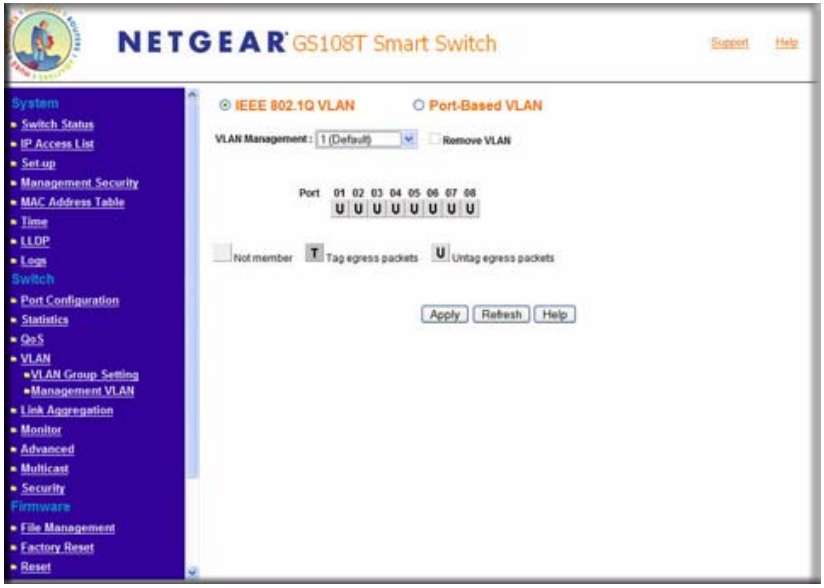


Figure 4-32

2. Check the **Remove VLAN** check box.
3. Click **Apply**.

To add or remove a port to a VLAN Group:

1. Select the **VLAN ID** for the VLAN you want to add or remove. A screen similar to that shown below appears.

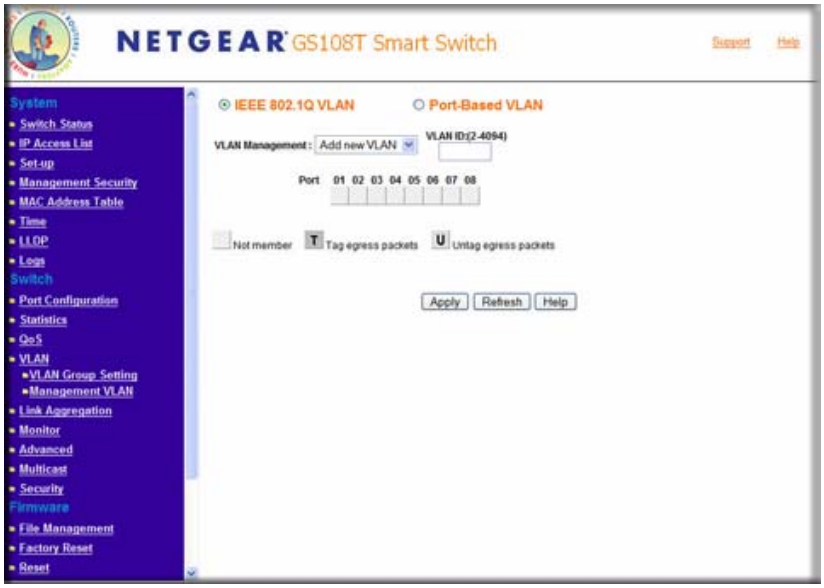


Figure 4-33

2. Check or uncheck the **Port ID** you want to add or remove.
3. Click **Apply**.

To change the PVID:

1. Select the **PVID Setting** option box. A screen similar to that shown below appears.

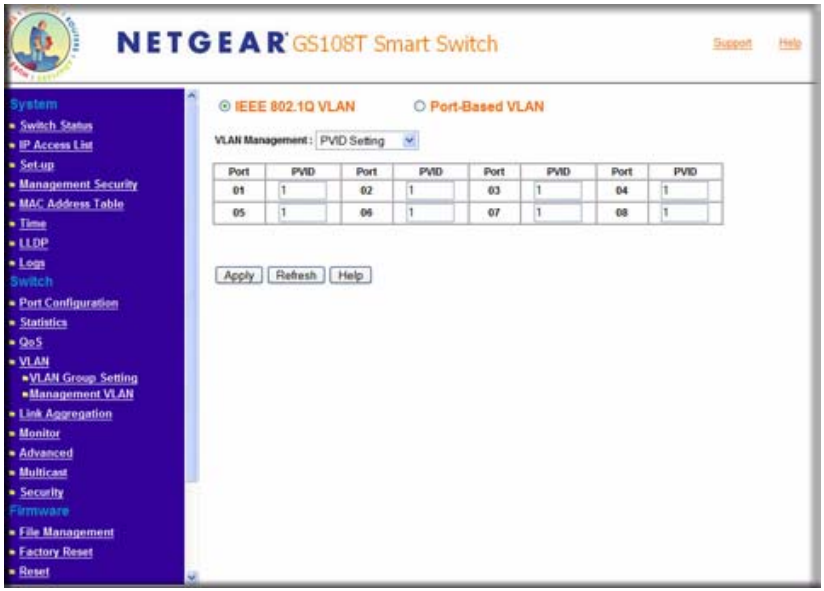


Figure 4-34

2. Input the **PVID** for each port.
3. Click **Apply**.

	Note: If you want to change the port's default PVID, you must first add the VLAN Group including the port.

Port-Based VLAN

Single or multiple ports are grouped into a smaller virtual network, which is independent of the other ports. The switch supports 8 port-based VLANs. Any user-assigned VLAN cannot have member ports that belong to different port groups.

Click **VLAN Group Setting** in the blue navigation panel. A screen similar to that shown below appears when **Port-Based VLAN** is selected for the VLAN group setting.

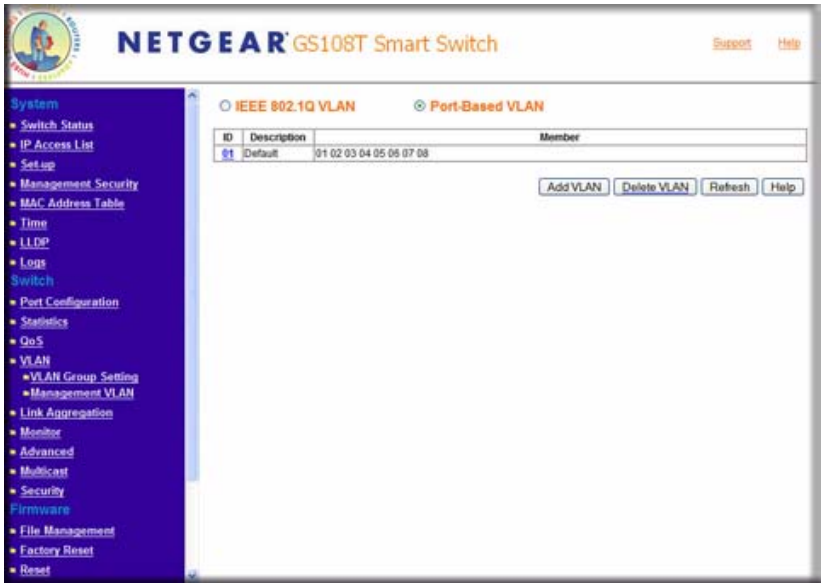


Figure 4-35

You can add or delete a VLAN.

To create a new VLAN:

1. Click **Add VLAN**. A screen similar to that shown below appears.

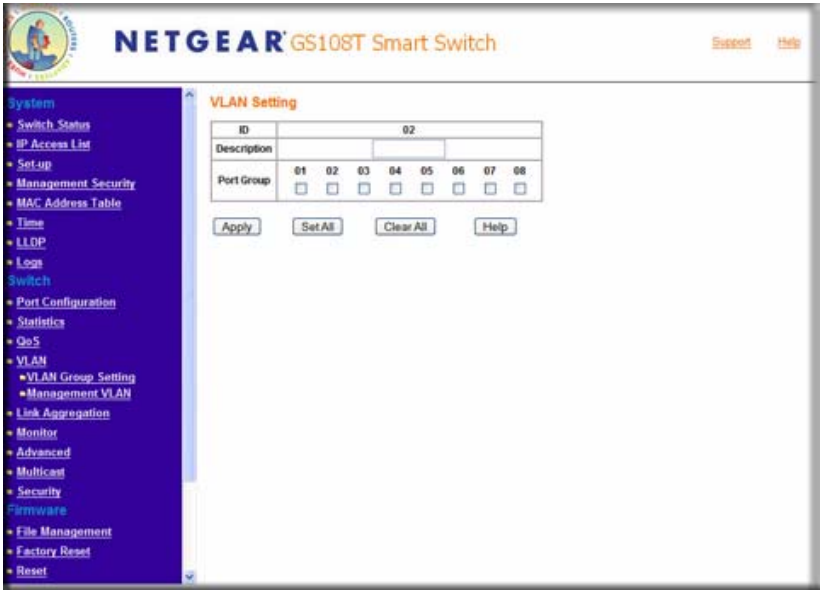


Figure 4-36

2. Input description in the provided field.
3. Select the ports from the group in which desired members located.
4. Add VLAN members as desired.
5. Click **Apply**.

To delete a VLAN:

1. Click **Delete VLAN**. A screen similar to that shown below appears.

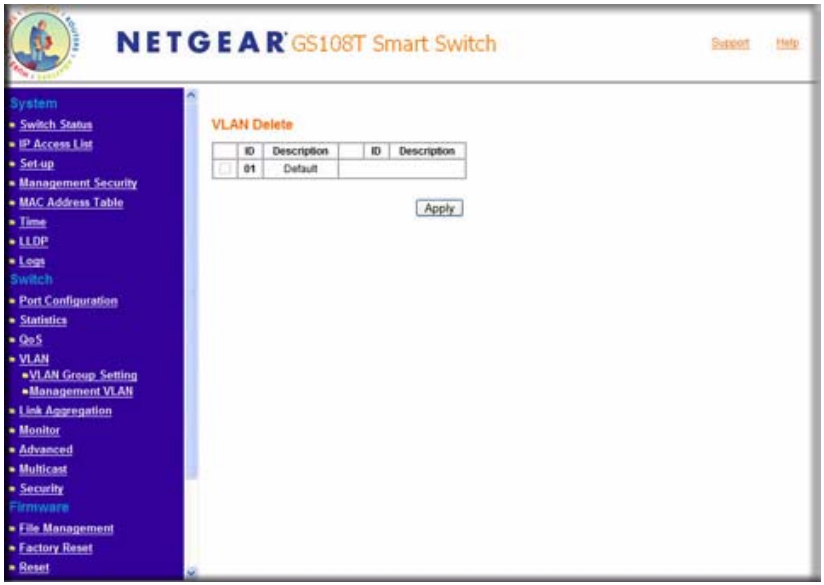


Figure 4-37

2. Check the **ID** check box for the VLAN you want to delete.
3. Click **Apply**.

Management VLAN Setting

When the switch is in 802.1Q mode, only the VLAN that is configured to management can access the Web, SNMP, and PING.

Click **Management VLAN** in the blue navigation panel. A screen similar to that shown below appears.

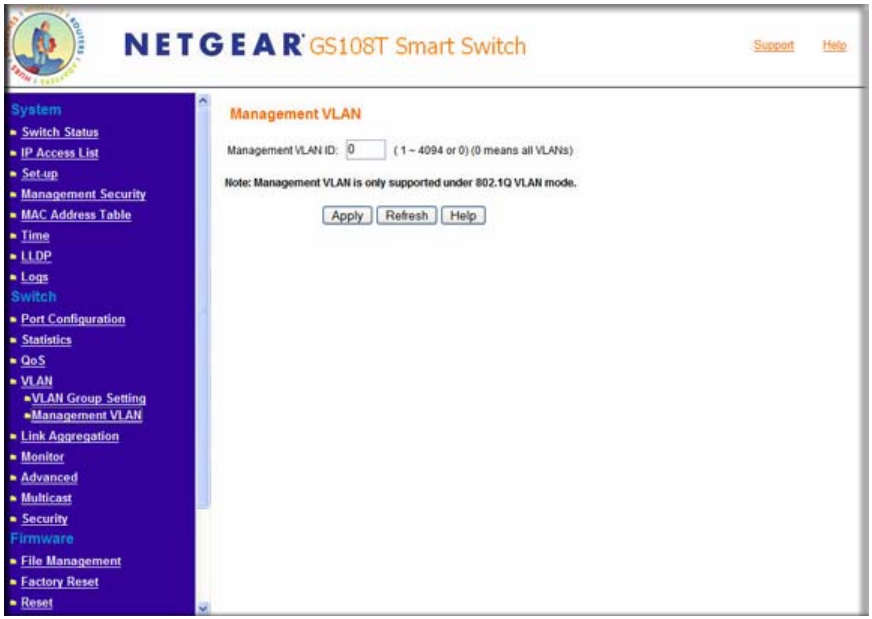


Figure 4-38

- If a user sets VLAN 0, all created VLANs are allowed.
- When the system works on the port-based VLAN mode, the VLAN value is always set to 0.

Link Aggregation

Two types of link aggregation are supported:

- **Static Trunking**: the ports are grouped manually.
- **Link Aggregation Control Protocol** (LACP): part of IEEE specification (802.3ad) that allows several physical ports to be bundled together to form a single logical channel. Link aggregation allows one or more links to be aggregated together to form a Link Aggregation Group, such that a MAC Client can treat the Link Aggregation Group as if it were a single link. Link aggregation can be used on 10-Mbps, 100-Mbps, or 1000-Mbps Ethernet full duplex ports.

Example: A network administrator could combine a group of five 100-Mbps ports into a logical link that will function as a single 500-Mbps port (the actual throughput however will be less than the sum total of the links).

Click **Link Aggregation** in the middle part of the blue navigation panel to expand the item to **LAG Setting** and **LACP**.

LAG Setting

1. Click **LAG Setting** in the blue navigation panel. A screen similar to that shown below appears.

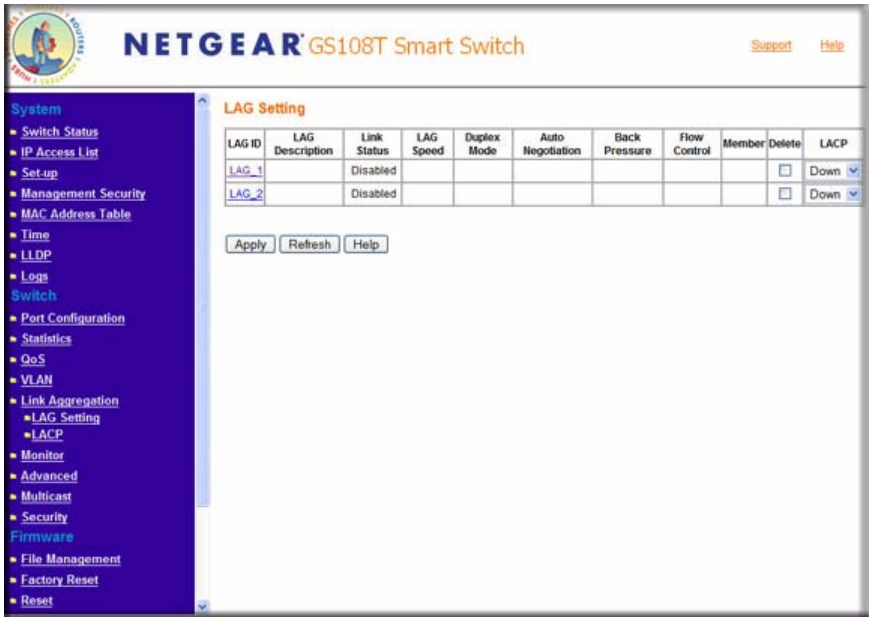


Figure 4-39

2. View the LAG settings:
   - **LAG Description**: Description of the LAG.
   - **Link Status**: Up/Down Status of the LAG.
   - **LAG Speed**: The speed will be either Auto/10/100/1000 M.
   - **Duplex Mode**: Half/Full duplex of the LAG.
   - **Auto Negotiation**: On/Off status of auto negotiation.
   - **Back Pressure**: On/Off status of back pressure.
   - **Flow Control**: On/Off status of flow control.
   - **Member**: List of the ports part of the LAG.

- **Delete**: Checked lags will be deleted in Apply.
- **LACP**: Enable/Disable LACP for the selected LAG.

c. Click **Apply** to apply the changes.

3. Click **LAG ID** on the LAG Setting page. A screen similar to that shown below appears.

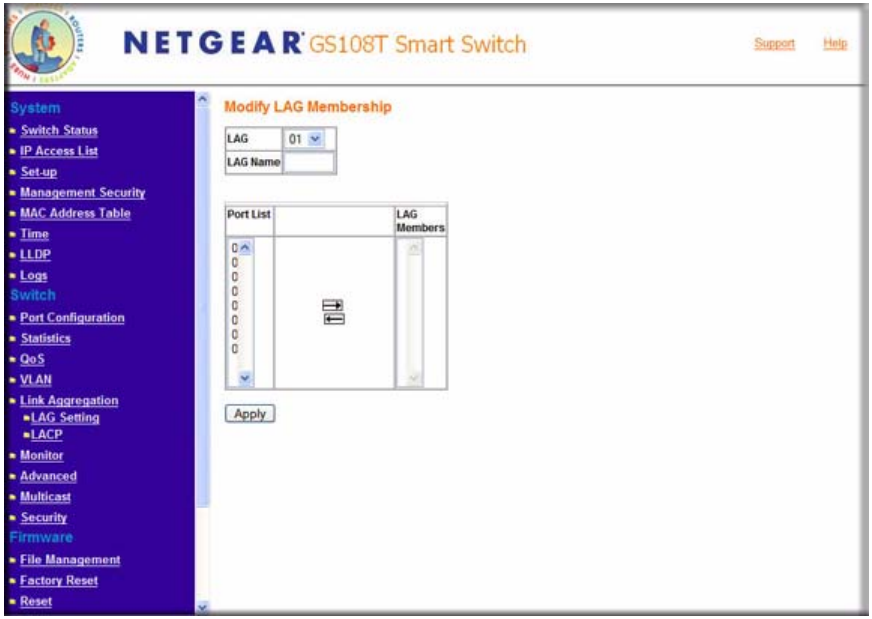


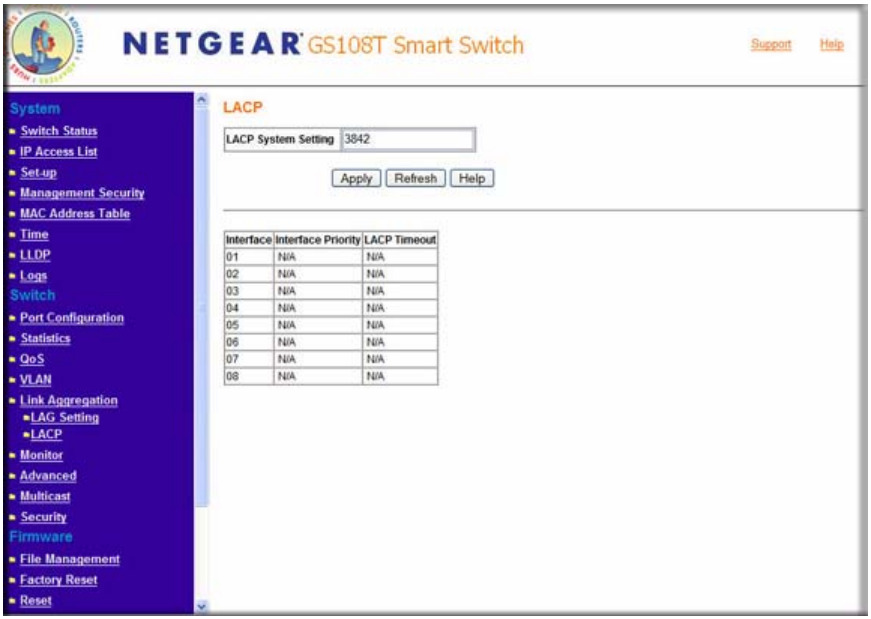
Figure 4-40

4. Modify the LAG membership.

5. Click **Apply** to apply the changes.

LACP

1. Click **LACP** in **the blue navigation panel**. A screen similar to that shown below appears.



2. View the LACP settings:

- **LACP System Setting**: Set LACP System Priority.
- **Interface Priority**: LACP Port priority ranges from 0 - 65536.
- **Interface Timeout**: Supports two modes of Timeout, Long/Short.

Monitor

The Monitor page allows you to configure any port's incoming and outgoing traffic to be mirrored to a predefined sniffer port.

1. Click **Monitor** in the blue navigation panel. A screen similar to that shown below appears.

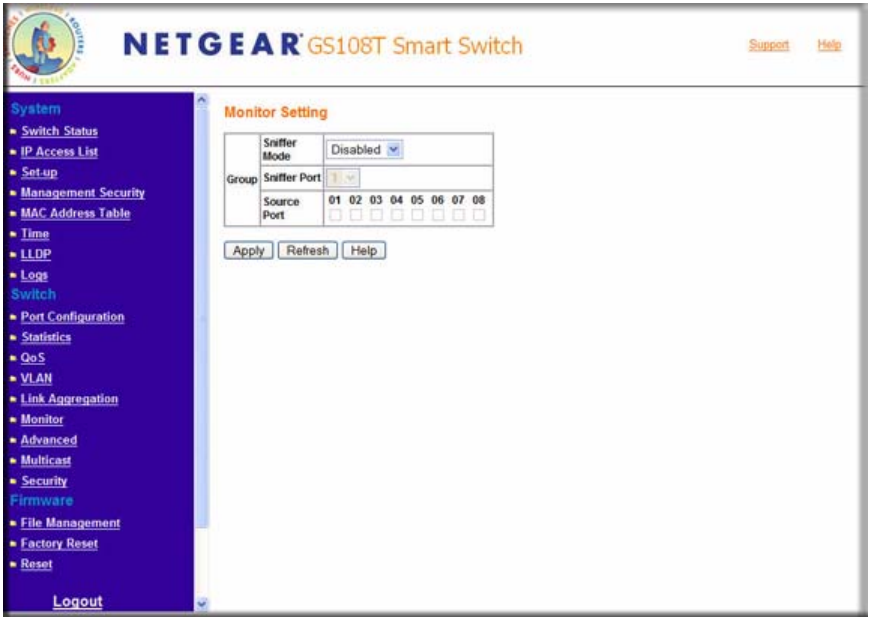


Figure 4-41

2. **Sniffer Mode**: Select the sniffer mode:
   - **Disable**: disable port mirroring globally.
   - **Ingress**: mirroring only the ingress traffic to the designated source ports.
   - **Egress**: mirroring only the egress traffic to the designated source ports.
   - **Both**: mirroring both incoming and outgoing traffic on the designated source ports.
3. **Sniffer Port**: Select from 1 to 8 ports.
4. **Source Ports**: Select any number of ports to be monitored (mirrored). The ports can not be the sniffer port.
5. Click **Apply** to update the monitor settings.

Advanced

Click **Advanced** in the middle part of the blue navigation panel to expand the item to **Jumbo Frame**, **Rate Limiting**, **Storm Control**, **Spanning Tree**, and **SNMP**.

Jumbo Frame

The Jumbo Frame page allows you to enable or disable the Jumbo Frame support. The default frame size is 1518 bytes. When jumbo frame support is enabled the frame size may vary from 1,518 to 9,728 bytes.

1. Click **Jumbo Frame** in the blue navigation panel. A screen similar to that shown below appears.

Figure 4-42

2. Click **Disable** or **Enable**.
3. Click **Apply**.

Rate Limiting

Rate Control determines the bandwidth of ingress and egress traffic for a specific port.

1. Click **Rate Limiting** in the blue navigation panel. A screen similar to that shown below appears.

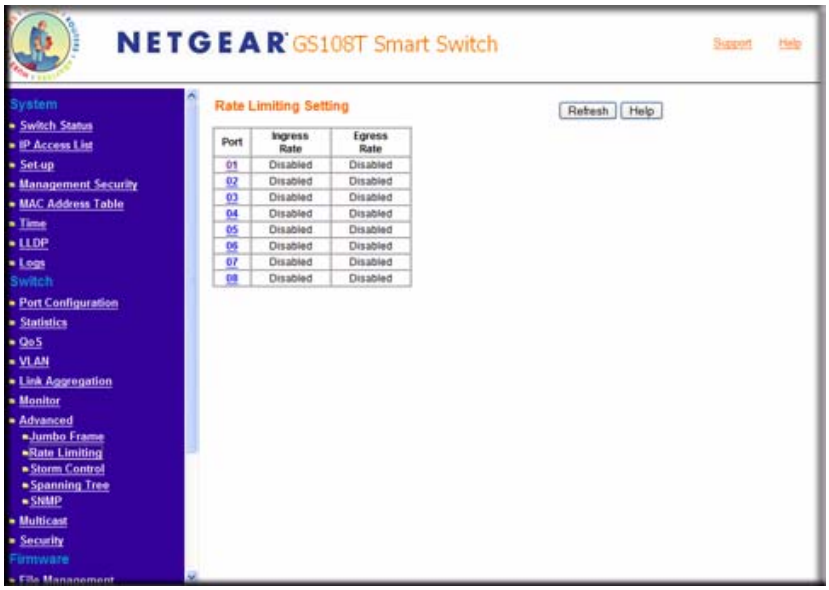


Figure 4-43

The parameters on this screen are as follows:

- **Port**: indicates the port number.
- **Ingress Rate**: indicates the rate limitation of incoming traffic in this port.
- **Egress Rate**: indicates the rate limitation of outgoing traffic in this port.

2. Click the port number to control ingress and egress rates for the port. A screen similar to that shown below appears.

Figure 4-44

3. Specify the ingress and egress rates for the port.
4. Click **Apply**.

Storm Control

The Storm Control page assigns storm rate limitations to the entire system.

1. Click **Storm Control** in the blue navigation panel. A screen similar to that shown below appears.

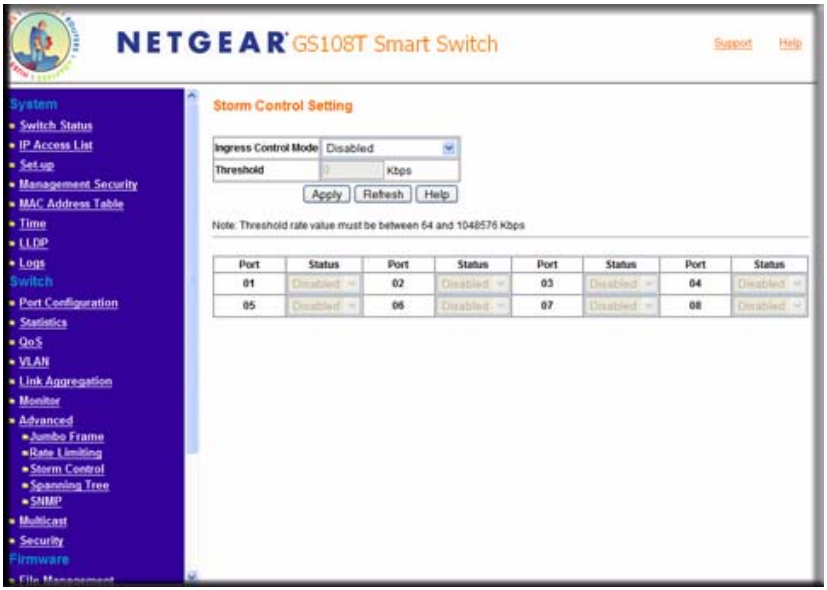


Figure 4-45

2. Specify the storm control settings:
   - **Ingress Control Mode**: Selects the type of the packet storm. The available options include:
     - Disabled
     - DLF
     - Broadcast
     - Multicast & Broadcast
   - **Storm Control Rate**: Used to enter the threshold limit for storm control.
   - **Per Port Setting**: Enable or disable the control type for every particular port.
3. Click **Apply**.

Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) provides rapid convergence of the spanning tree by assigning port roles and by determining the active topology. The RSTP builds upon the IEEE 802.1D STP protocol to select the switch with the highest switch priority as the root switch. Reconfiguration of the spanning tree can occur in less than 1 second.

1. Click **Spanning Tree** in the blue navigation panel. A screen similar to that shown below appears.

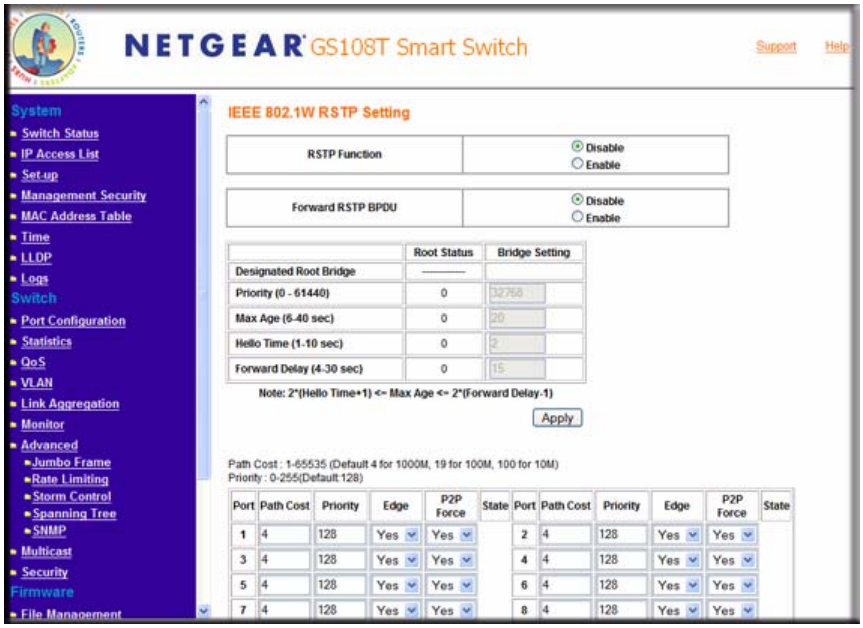


Figure 4-46

2. View and change the spanning tree settings as desired:

- **BPDU**: When Spanning tree is disabled, BPDU flooding is a configurable option. If BPDU flooding is enabled, the BPDU will be forwarded to all the linkup ports
- **RSTP Switch Setting**: The RSTP switch settings allow you to control the RSTP parameter from the bridge point of view.
- **Designated Root Bridge**: The bridge identifier of the root of the spanning tree is determined by the RSTP protocol as executed by this node. The bridge identifier value is used as the Root Identifier parameter in all configuration bridge PDUS originated by this node.
- **Priority**: configures the priority of the current bridge.
- **Max Age**: configures the maximum age of the current bridge. This is the maximum age of spanning tree protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.

- **Hello Time**: indicates the amount of hello time of the current bridge. Hello time is the amount of time between the transmission of configuration bridge PDUS by this node on any port when it is the root of the spanning tree or trying to become so, in units of hundredths of a second.
- **Forward Delay**: indicates the amount of forward delay of the current bridge. Forward delay is a time value, measured in units of hundredths of a second, which controls how fast a port changes its state. The value determines how long the port stays in each of the listening and learning states which precede the forward state. This value is also used to age all dynamic entries in the forwarding databases when a topology change has been detected and is underway.
- **RSTP Port Setting**: RSTP port settings control and monitor port-based spanning tree status.
- **Path Cost**: displays the cost of this port. *Cost* means the contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Priority**: displays the priority of this port. This is the value of the priority field contained in the first octet of the Port ID.
- **Edge**: indicates if this port is the edge port. Once configured as an edge port, the port immediately transitions to the forwarding state.
- **P2P Force**: indicates if this port is a point-to-point link. If you connect a port to another port though a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port to ensure a loop-free topology.
- **State**: displays the RSTP port status.

3. Click **Apply**.

SNMP

The SNMP page allows you to limit the IP address which can access the MIB of the switch and to which the switch will send the trap.

- The switch only responds to requests from computers with the IP address in the list.
- You can also select the traps which the switch will send to the hosts in the following trap events.

The setting of a host will not be active until it is set to **Enable** in the Admin field.

1. Click **SNMP** in the blue navigation panel. A screen similar to that shown below appears.

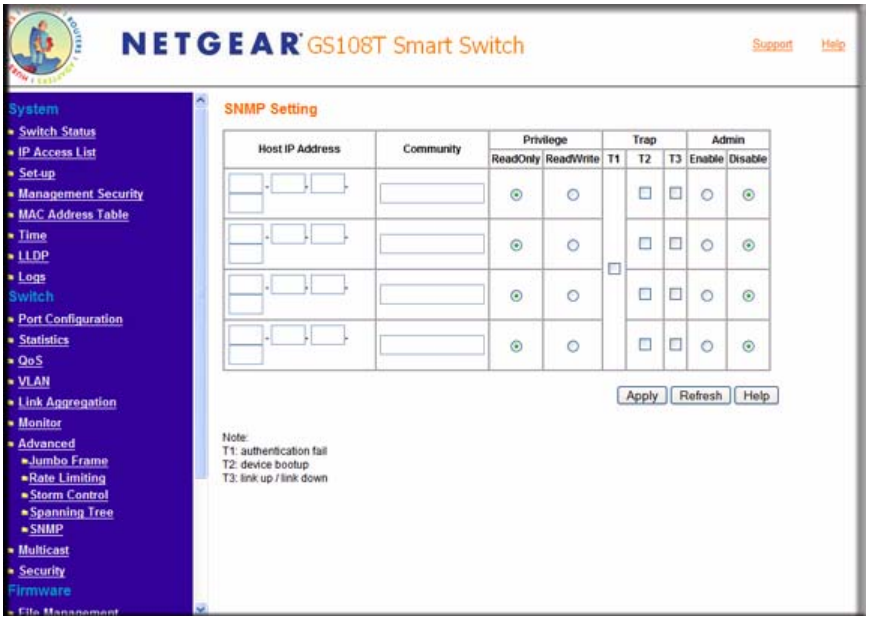


Figure 4-47

2. View or specify the SNMP settings as desired:
   - **Remote Station IP**: sets the Community's management station IP address.
   - **Community String**: sets the Community String.
   - **Privilege**: sets the access privilege (read and write) state of the Group.
   - **Trap Events**:
     - **T1: Authentication Fail**: The switch generates an SNMP trap when a host tries to gain access to the switch but the host's IP is not in the SNMP host table.
     - **T2: Device Bootup**: The switch generates an SNMP trap when it reboots.
     - **T3: Link Up/Down**: The switch generates an SNMP trap when one of its ports changes its link status.
   - **Admin State**: Enable or disable this community.
3. Click **Apply**.

Multicast

Click **Multicast** in the middle part of the blue navigation panel to expand the item to **IGMP Snooping**, **Unknown Multicast**, and **Static Multicast Group**.

IGMP Snooping

IGMP specifies how a host can register to a router in order to receive specific multicast traffic. Configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward multicast traffic only to those ports that want to receive it. IGMP is a standard defined in RFC1112 for IGMPv1 and in RFC2236 for IGMPv2.

1. Click **IGMP Snooping** in the blue navigation panel. A screen similar to that shown below appears.

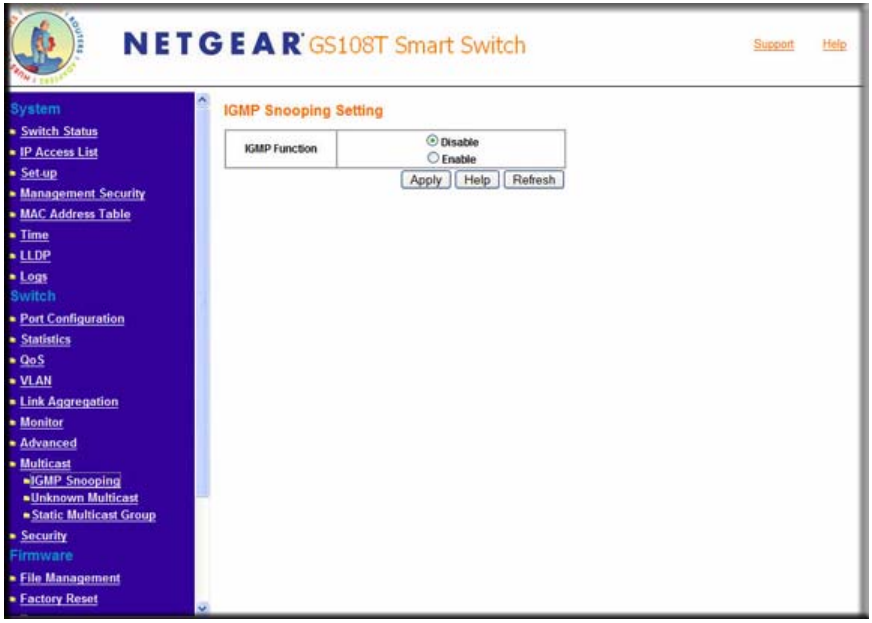


Figure 4-48

2. View or configure the IGMP settings as desired:

- **IGMP Function**: allows to enable/disable the IGMP snooping feature per switch. This feature is disabled by default.
- **Dynamic Multicast Entry Table**: displays the Dynamic Layer 2 multicast entries. **VID** is VLAN ID.
- **Multicast Entry**: Layer 2 multicast group address.
- **Member Port(s)**: the membership associated with the group.

3. Click **Apply**.

Unknown Multicast

The Unknown Multicast page allows you to enable or disable the unknown multicast flooding feature.

1. Click **Unknown Multicast** in the blue navigation panel. A screen similar to that shown below appears.

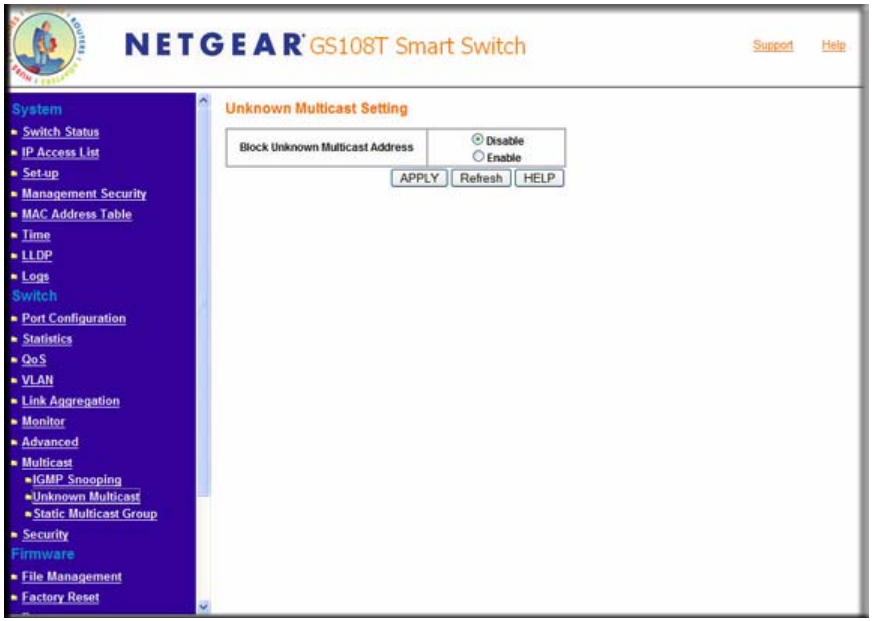


Figure 4-49

2. Enable or disable the unknown multicast flooding feature.
3. Click **Apply**.

Static Multicast Group

Static Multicast Addressing provides a way to add or delete a static multicast address and VLAN ID in the system.

1. Click **Static Multicast Group** in the blue navigation panel. A screen similar to that shown below appears.

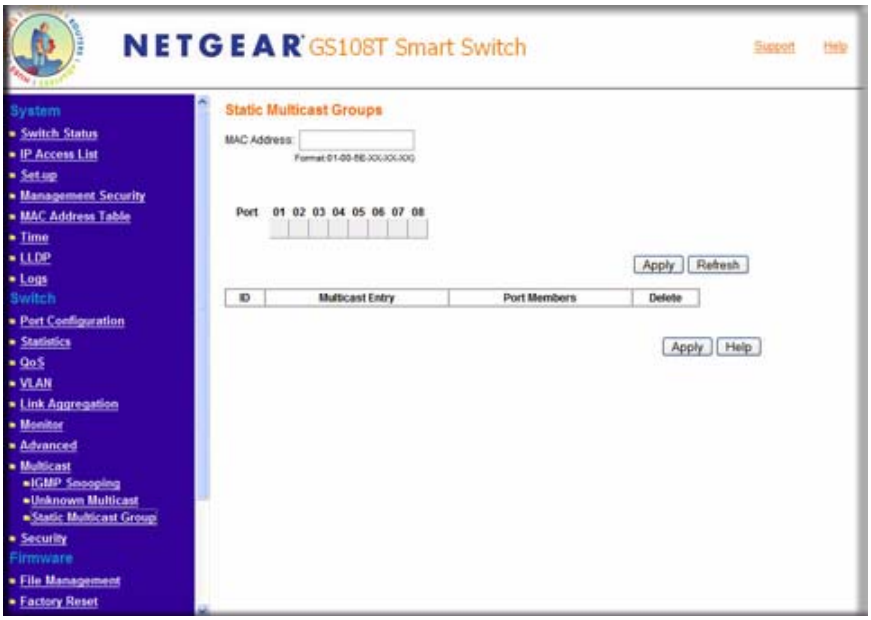


Figure 4-50

2. View or specify the Static Multicast Group settings as desired.
3. Click **Apply**.

Security

Click **Security** in the middle part of the blue navigation panel to expand the item to **Properties**, **Port Authentication**, **EAP Statistics**, **Statistics**, **Port Security**, and **Trusted MAC**.

Properties

The Network Authentication Properties page allows network managers to configure port authentication parameters. Guest VLANs are also enabled from the Network Authentication Properties page.

1. Click **Properties** in the blue navigation panel. A screen similar to that shown below appears.

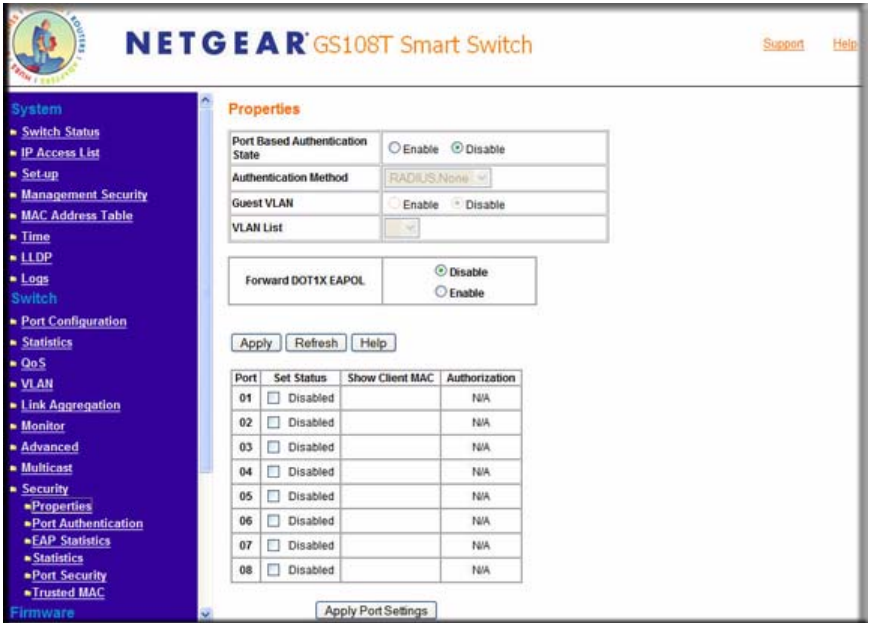


Figure 4-51

2. 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:
     - **None**: Indicates that no authentication method is used to authenticate the port.
     - **RADIUS**: Provides port authentication using the RADIUS server.

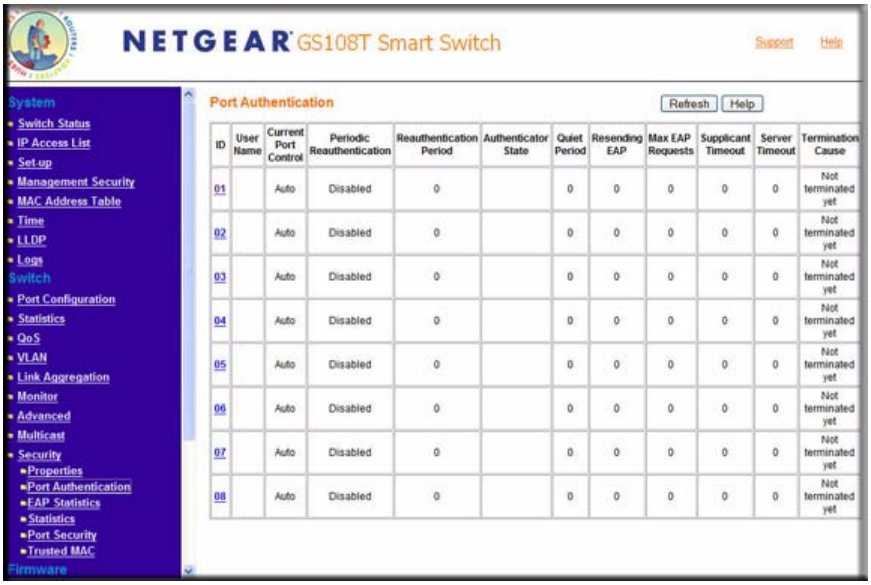
  - **RADIUS, None**: Provides port authentication, first using the RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.
- **Guest VLAN**: Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
  - **Enable**: 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.
- **Forward DOT1x EAPOL**: When the Port-based Authentication State is disabled, users can enable or disable flooding EAPOL.

3. Click **Apply**.

Port Authentication

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

1. Click **Port Authentication** in the blue navigation panel. A screen similar to that shown below appears.



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
01		Auto	Disabled	0		0	0	0	0	0	Not terminated yet
02		Auto	Disabled	0		0	0	0	0	0	Not terminated yet
03		Auto	Disabled	0		0	0	0	0	0	Not terminated yet
04		Auto	Disabled	0		0	0	0	0	0	Not terminated yet
05		Auto	Disabled	0		0	0	0	0	0	Not terminated yet
06		Auto	Disabled	0		0	0	0	0	0	Not terminated yet
07		Auto	Disabled	0		0	0	0	0	0	Not terminated yet
08		Auto	Disabled	0		0	0	0	0	0	Not terminated yet

Figure 4-52

2. View the Port Authentication settings.

To modify the port authentication settings:

1. Click the **ID** of the port on the Port Authentication page. A screen similar to that shown below appears.

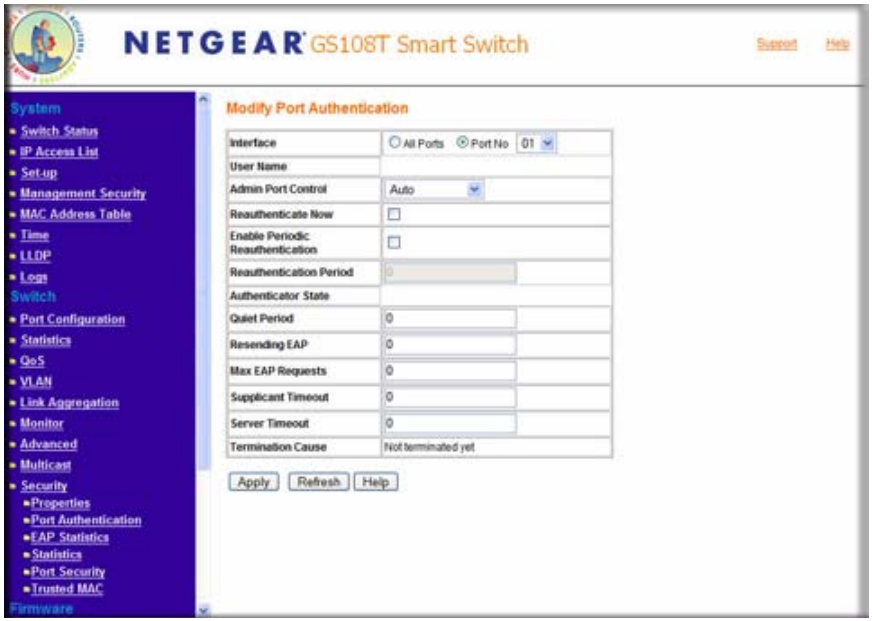


Figure 4-53

2. The Port Authentication Page contains the following fields:

- **ID**: Displays a list of interfaces on which port-based authentication is enabled.
- **User Name**: Displays the supplicant user name.
- **Admin Port Control**: Displays the current port authorization state.
- **ReAuthenticate Now**: Forces reauthentication of all existing clients.
- **Enable 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 3,600 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 exchange. The possible field range is 0-65,535. 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, please reference to help age of real device FW V1.0.1_03.

3. Click **Apply**.

EAP Statistics

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

1. Click **EAP Statistics** in the blue navigation panel. A screen similar to that shown below appears.

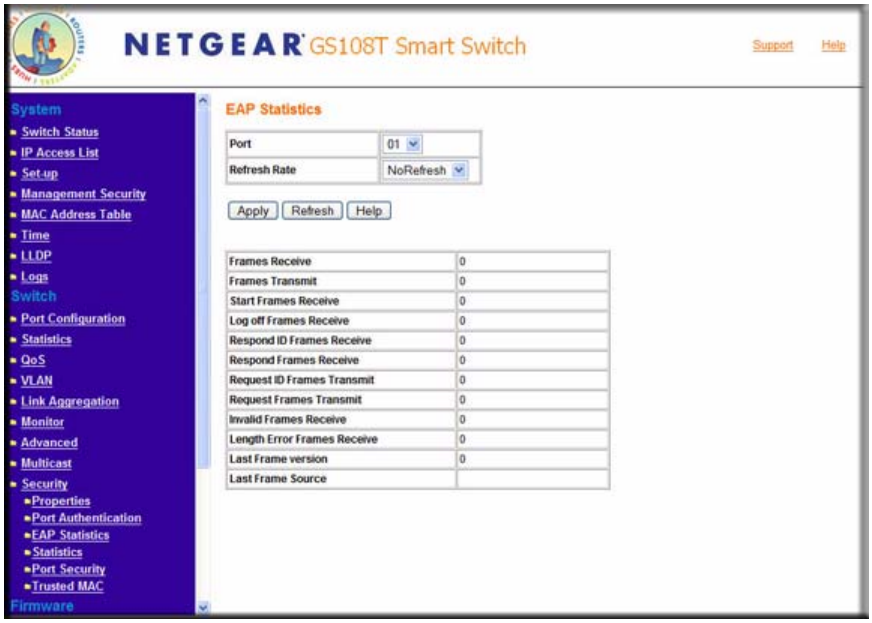


Figure 4-54

2. The EAP Statistics page contains the following fields:

- **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:
  - **15 Sec**: Indicates that the EAP statistics are refreshed every 15 seconds.
  - **30 Sec**: Indicates that the EAP statistics are refreshed every 30 seconds.
  - **60 Sec**: Indicates that the EAP statistics are refreshed every 60 seconds.
  - **No Refresh**: Indicates that the EAP statistics are not refreshed.
- **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 by on this 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.

3. Click **Apply**.

Statistics

The DOT1x Statistics page contains information packets received on a specific port.

1. Click **Statistics** in the blue navigation panel. A screen similar to that shown below appears.

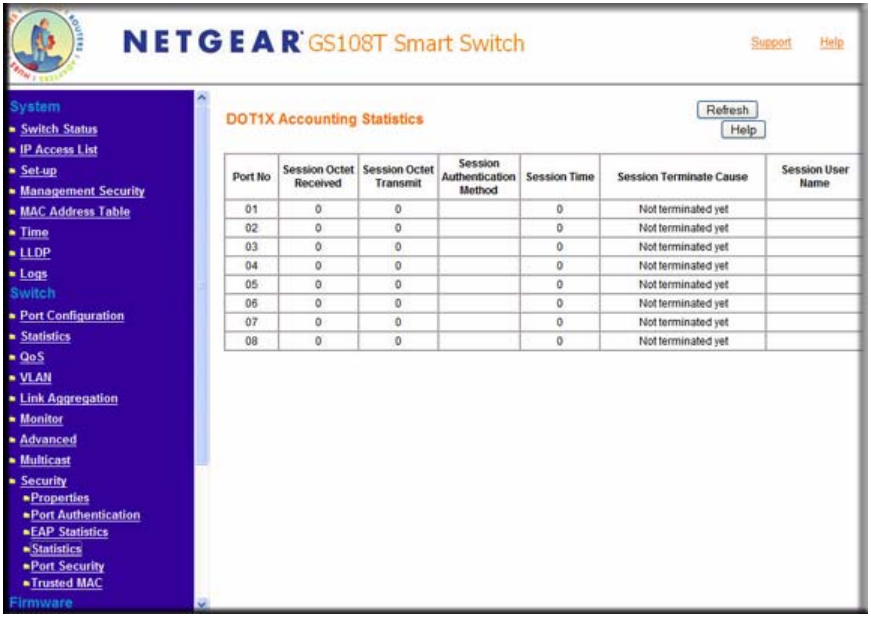


Figure 4-55

2. The DOT1x Statistics Page contains the following fields:

- **Port**: Indicates the port that is polled for statistics.
- **Session Octet Received**: Indicates the number of bytes received on the port.
- **Session Octet Transmit**: Indicates the number of bytes transmitted via the port.
- **Session Authentication Method**: Specifies the authentication method used for port authentication.
- **Session Time**: Indicates the time elapsed since the session is established.
- **Session Terminate Cause**: Indicates the reason for which the port authentication was terminated.
- **Session User Name**: Indicates the session user name

Port Security

The Port Security page allows you to enable/disable port learning. If the learning mode is disabled, you can configure the action for unknown source MAC address packets.

1. Click **Port Security** in the blue navigation panel. A screen similar to that shown below appears.

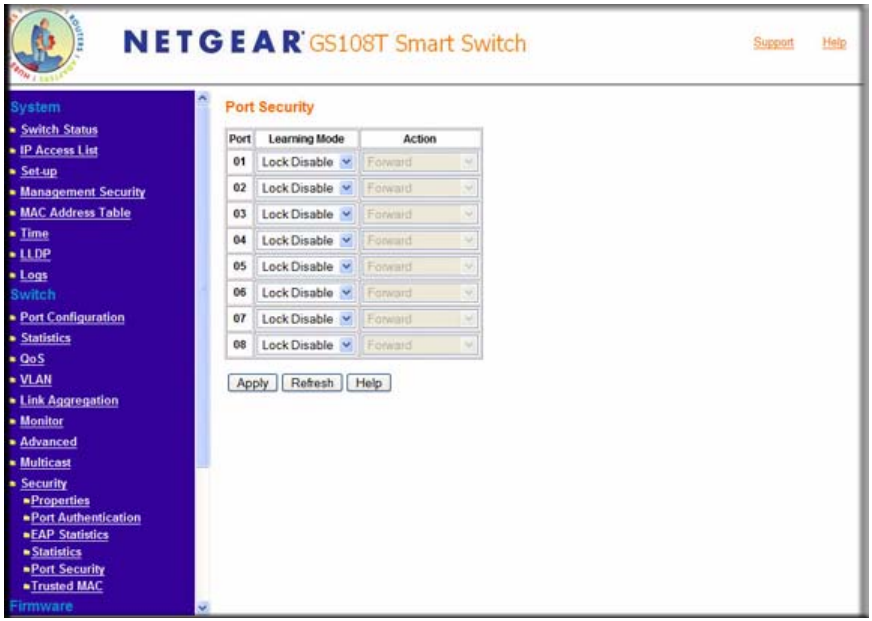


Figure 4-56

2. The Port Security page contains the following fields:
   - **Port**: Indicates the port number.
   - **Learning Mode**: Allows to enable/disable learning on the port.
   - **Action**: Specifies the action to Forward or Discard unknown source mac address packets. Limited Learning dynamically learns 16 MAC addresses and stop learning hereafter.
   - **Trap**: Specifies whether to send trap notification to logging servers when security violation occurs.
3. Click **Apply**.

Trusted MAC

The Trusted MAC protects the device from untrusted intruder invade the system. Only the SA of the packet in the trusted MAC table can be switched to the destination port. The trusted MAC is configured by the user; it is per port based; and total 100 trusted MACs can be added.

Click **Trusted MAC** in the blue navigation panel. A screen similar to that shown below appears.

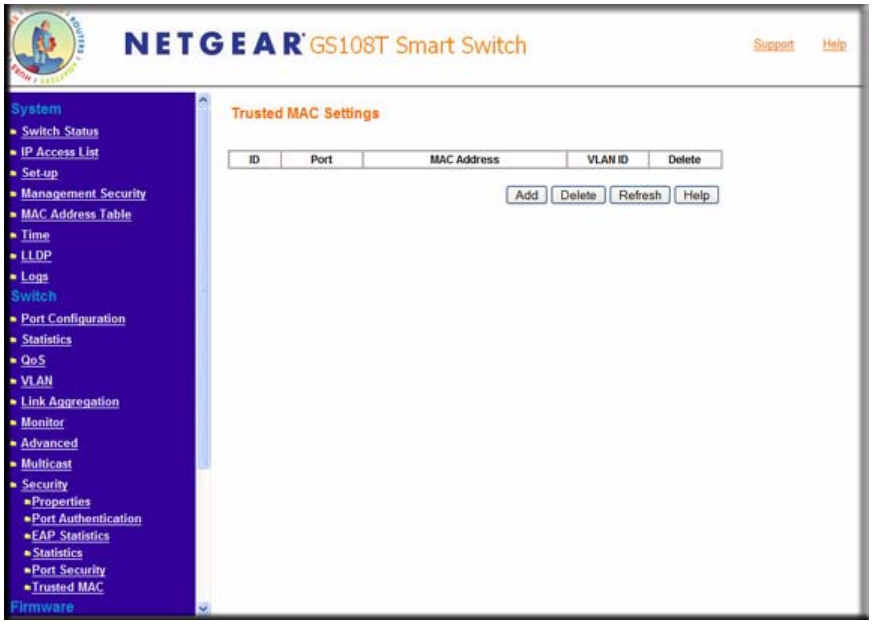


Figure 4-57

All Source MACs are trusted when Trusted MAC list is empty.

- When VLAN setting is in 802.1Q mode (see "IEEE 802.1Q VLAN" on page 4-9), the filter parameters will be {PORT, VLAN ID, SRC MAC}.
- When VLAN setting is in Port-based mode (see "Port-Based VLAN" on page 4-13), the filter parameters will be {PORT, SRC MAC}.

You can add or delete a MAC address:

To add a MAC address:

1. Click **Add** on the Trusted MAC page. A screen similar to that shown below appears.

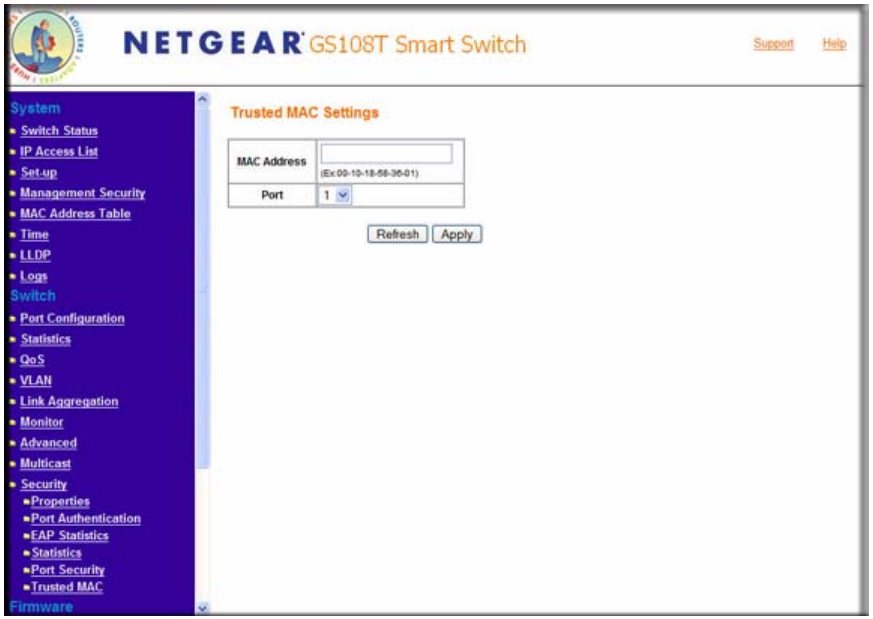


Figure 4-58

2. Add the MAC address for each port number.

3. Click **Apply**.

To delete a MAC address:

1. Select the MAC address to delete.

2. Click **Apply**.

Chapter 5
Managing Firmware and Reset Options

The **Firmware** selections on the navigation menu enable you to manage the switch's firmware and configuration files and reset the switch:

- Upload or download the firmware and configuration files between a TFTP Server or HTTP Host and the switch so that you can back up and either restore or update the switch.
- Reset the switch to its factory default values.
- Restart the switch with its current configuration.

The section includes this information under the following headings:

File Management

Click **File Management** in the lower part of the blue navigation panel to expand the item to **File Upload** and **File Download**.

File Upload

File Upload enables you to back up the current firmware and configuration switch files to a TFTP Server or HTTP Host.

1. Click **File Upload** in the blue navigation panel. A screen similar to that shown below appears.

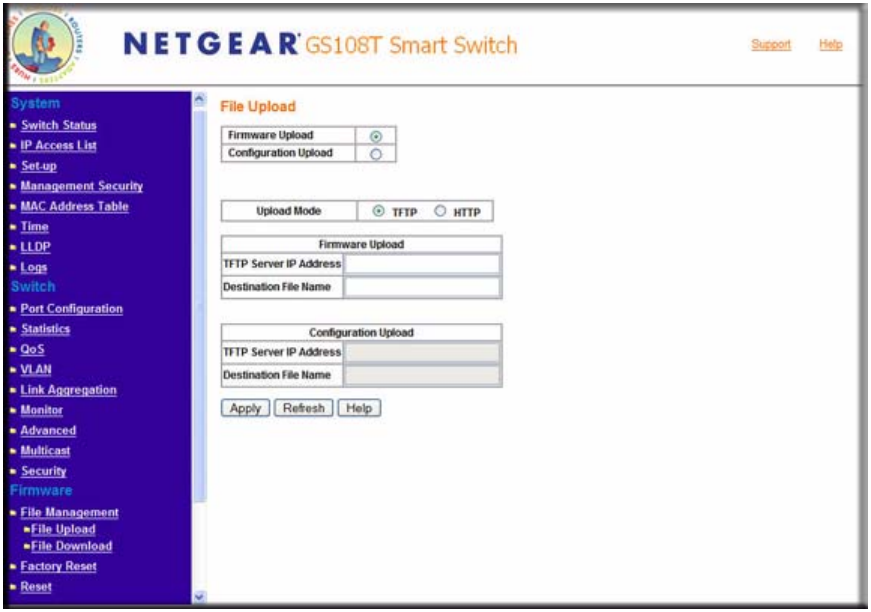


Figure 5-59

2. Click **Firmware Upload** or **Configuration Upload** to select the type of file for upload.
3. Click **TFTP** or **HTTP** to select the upload mode.

   If the **TFTP** mode is selected:

   a. Enter the IP Address of the TFTP Server.

   b. Enter the name of the firmware or configuration destination file in the TFTP server.

   If the **HTTP** mode is selected:

   a. Enter the name of the firmware or configuration destination file in the HTTP Host.
4. Click **Apply** to start the upload.

File Download

File Download enables you to download the firmware and configuration from the TFTP Server or HTTP Host to restore or update the switch.

Note: You can also update the firmware using the in the SmartWizard Discovery utility (see "Firmware Upgrade" on page 1-8).

1. Click **File Download** in the blue navigation panel. A screen similar to that shown below appears.

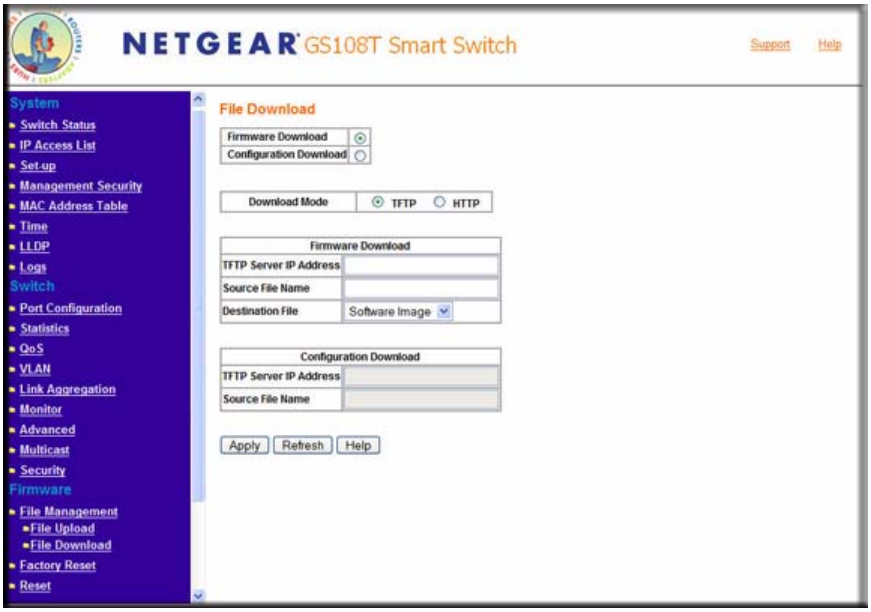


Figure 5-60

2. Click **Firmware Download** or **Configuration Download** to select the type of file for download.
3. Click **TFTP** or **HTTP** to select the download mode.

   If the **TFTP** mode is selected:

   a. Enter the IP Address of the TFTP Server.

   b. Enter the name of the firmware or configuration source file in the TFTP server.

c. Select either **Software Image** or **Boot Code** for saving the firmware in the destination file.

If the **HTTP** mode is selected:

a. Enter the name of the firmware or configuration file to download.

b. Select either **Software Image** or **Load Flash** for saving the firmware in the destination file.

4. Click **Apply** to start the download.

Factory Reset

Factory Reset enables you reset the switch to its factory default values.

	Note: You can also use the Factory Defaults button on the front panel to reset the switch to its factory default values.

1. Click **Factory Reset** in the blue navigation panel. A screen similar to that shown below appears.

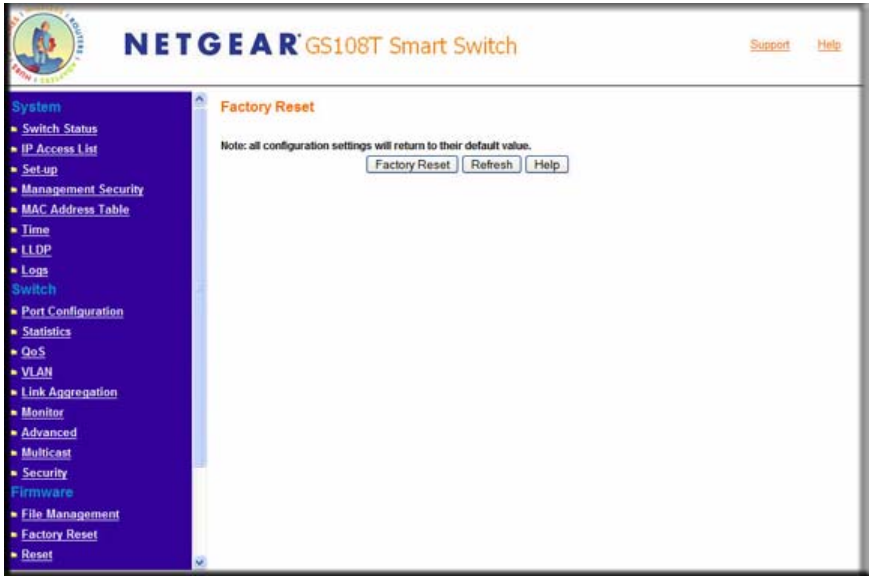


Figure 5-61

2. Click **Factory Reset** to reset the system.
   - If there is no DHCP server on the network, the IP address will become **192.168.0.239**.
   - The password will return to the factory default **password**.

Reset

Reset enables you restart the switch with its current configuration.

	Note: You can also use the Reset button on the front panel to reset the switch to its current configuration.

To reset and restart the switch:

1. Click **Reset** in the blue navigation panel. A screen similar to that shown below appears.

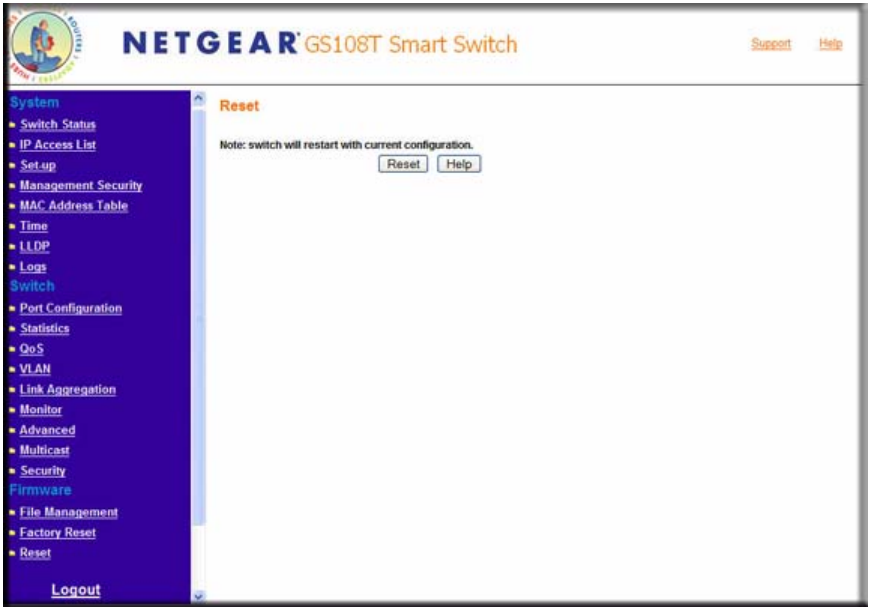


Figure 5-62

2. Click **Reset** to restart the switch.

Appendix A
Specifications and Default Values

GS108T Gigabit Smart Switch Specifications

The GS108T Gigabit Smart Switch conforms to the TCP/IP, UDP, HTTP, ICMP, TFTP, DHCP, 802.1D, 802.1p, and 802.1Q standards.

Table A-1. GS108T Gigabit Smart Switch Specifications

Feature	Value
Interfaces	8G (P01 - P08)
PoE	N/A
Flash Memory Size	2MB
SRAM Size and Type	16MB DDR

Table A-2. Switch Performance

Feature	Value
Switching Capacity	8 x 2 Gbps
Forwarding Method	Store and Forward
Packet Forwarding Rate	10M:14,880 pps / 100M:148,809 pps / 1G:1,488,095 pps
MAC addresses	4K
Packet RAM buffer capacity	128K-bytes

GS108T Gigabit Smart Switch Features and Defaults

Table A-3. Port Characteristics

Feature	Sets Supported	Default
Auto-Negotiation / Static Speed / Duplex	8 (per-port)	Auto-Negotiation
Auto MDI/MDIX	N/A	Enabled
802.3x flow control / Back Pressure	8 (per-port)	Enabled
Port Mirroring	1	Disabled
Port Trunking (Aggregation)	2	2
802.1D Spanning Tree	1	Disabled
802.1w RSTP	1	Disabled
IGMP Snooping	1	Disabled
Static 802.1Q Tagging	256	VID = 1 MemberPorts = [1-8]
Port Based Private VLAN	8X1	MemberPorts[1] = [1-8]
Learning Process	N/A	N/A

Table A-4. Quality Of Service

Feature	Sets Supported	Default
Number of Queues	N/A	N/A
Port Based	8 (per port)	Normal for all ports
802.1p	1	Disabled
DSCP	1	Disabled

Table A-5. Security

Feature	Sets Supported	Default
IP Access List	10	All IP addresses allowed
Password Control Access	1	LoginTimeOut = 5 mins. Password = “password”

Table A-5. Security (continued)

Feature	Sets Supported	Default
Trust MacAddress Filter	256	Disabled
Port -MAC lock down	8 (per port)	Disabled
Management VLAN	1	0

Table A-6. Traffic Control

Feature	Sets Supported	Default
Rate control	8 (per port)	Disabled
Storm control	8 (per port)	Disabled
Jumbo frame	1 (per system)	Disabled

Table A-7. System Setup

Feature	Sets Supported	Default
DHCP\Manual IP	1	192.168.0.239
System Name Configuration	1	NULL
Configuration Save/Restore	1	N/A
Firmware Upgrade	1	N/A
Factory Reset	1	N/A

Table A-8. Other Features

Feature	Sets Supported	Default
Static Multicast Entry	64	Disabled
Filter Multicast Control	1	Disabled

Table A-9. Management

Feature	Sets Supported	Default
SNMPv1/V2c	4	Disabled
MIB Support	1	Disabled

Table A-9. Management (continued)

Feature	Sets Supported	Default
SmartWizard	N/A	Enabled
Statistics	31 (per port)	N/A

Appendix B
Virtual Local Area Networks (VLANs)

A Local Area Network (LAN) can generally be defined as a broadcast domain. Hubs, bridges or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local-area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application). To communicate between VLANs, traffic must go through a router, just as if they were on two separate LANs.

A VLAN is a group of PCs, servers and other network resources that behave as if they were connected to a single, network segment—even though they may not be. For example, all marketing personnel may be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

The Advantages of VLANs:

- Easy to do network segmentation: Users that communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is largely contained within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- Easy to manage: The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- Increased performance: VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- Enhanced network security: VLANs create virtual boundaries that can only be crossed through a router. So standard, router-based security measures can be used to restrict access to each VLAN

IEEE 802.1Q VLANs

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID tag number. Each port has a default VLAN ID setting that is user-configurable (the default setting is 1). The default VLAN ID setting for each port can be changed in the PVID Setting page.
- When a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID Setting. The packet proceeds to the VLAN specified by its VLAN ID (VID) tag number.
- If the port in which the packet entered does not have membership with the VLAN specified by the VLAN ID tag, the packet is dropped.
- If the port is a member of the VLAN specified by the packet's VLAN ID, the packet is able to be sent to other ports with the same VLAN ID.
- Packets leaving the switch are either tagged or untagged, depending on the setting for that port's VLAN membership properties. A 'U' for a given port means that packets leaving the switch from that port are Untagged. Inversely, a 'T' for a given port means that packets leaving the switch from that port are tagged with the VLAN ID associated with the port.

The example given in this section comprises numerous steps to illustrate a wide range of configurations to help provide an understanding of tagged VLANs.

Example

This example demonstrates several scenarios of VLAN use and describes how the switch handles Tagged and Untagged traffic.

1. Setup the following VLANs: VLAN 10, 20.

2. Configure the VLAN membership. Be sure to set all of them as follows.
   - Setting up first VLAN group, VLAN ID = 10:
   - Setting up second VLAN group, VLAN ID = 20:

3. Modify PVID Setting to apply previous two VLAN groups: Modify Default VLAN group (VLAN ID = 1) to apply two new VLAN groups:

   The specific ports above have the following Port VLAN ID settings:
   - Default VLAN: Port 7 – Port 8 (all U), VID = 1
   - VLAN 1: Port 1 (U), Port 2 (U), Port 3 (T), VID = 10
   - VLAN 2: Port 4 (U), Port 5 (T), Port 6 (U), VID = 20.

4. The following situations produce results as described:

- If an untagged packet enters Port 1, the switch tags it with a VLAN tag value 10. The packet has access to Port 2 and Port 3. The outgoing packet is stripped of its tag to leaves Port 2 as an untagged packet. For Port 3, the outgoing packet leaves as a tagged packet with a VLAN tag value of 10.
- If a tagged packet with a VLAN tag value 10 enters Port 3, the packet has access to Port 1 and Port 2. If the packet leaves Port 1 and/or Port 2, it is stripped of its tag to leave the switch as an untagged packet.
- If an untagged packet enters Port 4, the switch tags it with a VLAN tag value 20. The packet will have access to Port 5 and Port 6. The outgoing packet is stripped of its tag to become an untagged packet as it leaves Port 6. For Port 5, the outgoing packet leaves as a tagged packet with a VLAN tag value of 20.

Port-based VLANs

Port-based VLANs help to confine broadcast traffic to the switch ports. This switch allows up to 8 port-based VLAN group, Any one port can belong to different VLAN groups. The default VLAN group is a port-based VLAN that has all ports belonging to VLAN 1.

Packets received by the switch are treated in the following way:

- When a packet enters a port, it can only proceed to ports with the same VLAN membership as that ingress port.
- If a port on the switch does not have a common VLAN membership with the source port, the packet is dropped.

Port-based VLAN Example Configuration

This example basically demonstrates how the port-based VLANs work to meet your needs.

Setup the following VLANs, each with defined descriptions:

- VLAN 1 (IT department)
- VLAN 2 (Sales department)
- VLAN 3 (Marketing department)
- VLAN 4 (Accounting department).
- Configure the VLAN membership. Be sure to set all of them as follows.
- Setting up second VLAN group (Sales), VLAN ID = 02, with membership of ports 1~3 and 8.

- Setting up third VLAN group (Marketing), VLAN ID = 03, with membership of ports 2~4 and 8.
- Setting up fourth VLAN group (Accounting), VLAN ID = 04, with membership of ports 5, 6, and 8.
- Setting up first VLAN group (IT), VLAN ID = 01, with membership of all ports.
- Since VLAN ID 01 has been setup by default, you will have to remove the ports that belong to all other VLAN groups except port 8.
- Ports 2 and 3 are kept for connected file server and printer server use. Sales and Marketing departments can share file archives and printing services.
- Port 8 provides Gigabit speed for e-mail server and Internet connection.

The specific ports above have the following functions:

- VLAN 1: Port 7, for IT department to monitor and control activities on all other VLANs.
- VLAN 2: Port 1, for Sales department, port 2 and 3 connect to file archives and printer server.
- VLAN 3: Port 4, for Marketing department, port 2 and 3 connect to file archives and printer server.
- VLAN 4: Port 5 and 6, for Accounting department, its work is kept secret from other departments except IT.

Results of this Configuration

If a packet comes in on port 1, it can go to ports 1, 2, 3, and 8, as those are the only ports in that VLAN. A Sales person on port 1 can get to the Internet, send and receive e-mail, access the marketing department print server or file archives, but can not access any marketing user nor any Accounting user.

If a Marketing user sends out a broadcast message, the Sales and Accounting departments are not affected by the message, because it does not go out on their ports. Only the Marketing department and the IT group will receive the broadcast message.

If an IT user sends out a broadcast message, everyone receives it.

Appendix C
Network Cabling

This appendix provides specifications for cables used with a NETGEAR GS108T Gigabit Smart Switch.

Fast Ethernet Cable Guidelines

Fast Ethernet uses UTP cable, as specified in the IEEE 802.3u standard for 100BASE-TX.The specification requires Category 5 UTP cable consisting of either two-pair or four-pair twisted, insulated copper conductors bound in a single plastic sheath. Category 5 cable is certified up to 100 MHz bandwidth. 100BASE-TX operation uses one pair of wires for transmission and the other pair for receiving and for collision detection.

When installing Category 5 UTP cabling, use the following guidelines to ensure that your cables perform to the following specifications:

- Certification: Ensure that your Category 5 UTP cable has completed the Underwriters' Laboratories (UL) or Electronic Testing Laboratories (ETL) certification process.
- Termination method: To minimize cross-talk noise, maintain the twist ratio of the cable up to the point of termination; untwist at any RJ-45 plug or patch panel should not exceed 0.5 inch (1.5 cm).

Category 5 Cable

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

- 20 ft. (6 m) between the hub and the patch panel (if used)
- 295 ft. (90 m) from the wiring closet to the wall outlet
- 10 ft. (3 m) from the wall outlet to the desktop device

The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

Category 5 Cable Specifications

Ensure that the fiber cable is crossed over to guarantee link.

Table C-1 lists the electrical requirements of Category 5 UTP cable.

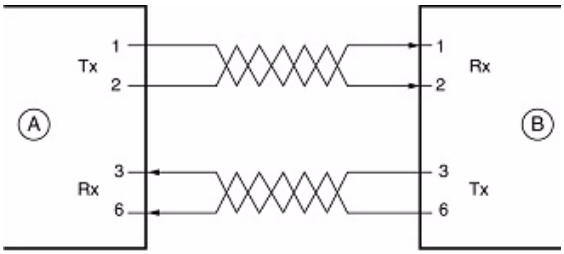
Table C-1. Electrical Requirements of Category 5 Cable

Specifications	Category 5 Cable Requirements
Number of pairs	Four
Impedance	100 ± 15%
Mutual capacitance at 1 KHz	5.6 nF per 100 m
Maximum attenuation (dB per 100 m, at 20° C)	at 4 MHz: 8.2 at 31 MHz: 11.7 at 100 MHz: 22.0
NEXT loss (dB minimum)	at 16 MHz: 44 at 31 MHz: 39 at 100 MHz: 32

Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

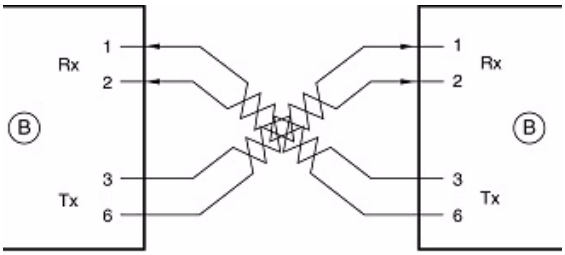
Figure C-1 illustrates straight-through twisted pair cable.



Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure C-1

Figure C-2 illustrates crossover twisted pair cable.



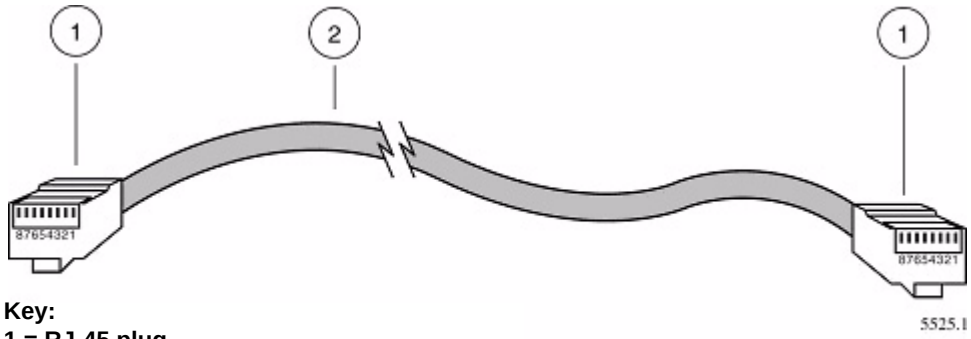
Key:
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure C-2

Patch Panels and Cables

If you are using patch panels, make sure that they meet the 100BASE-TX requirements. Use Category 5 UTP cable for all patch cables and work area cables to ensure that your UTP patch cable rating meets or exceeds the distribution cable rating.

To wire patch panels, you need two Category 5 UTP cables with an RJ-45 plug at each end, as shown in Figure C-3.



Key:
1 = RJ-45 plug
2 = Category 5 UTP patch cable

Figure C-3

	Note: Flat “silver satin” telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Using 1000BASE-T Gigabit Ethernet over Category 5 Cable

When using the new 1000BASE-T standard, the limitations of cable installations and the steps necessary to ensure optimum performance must be considered. The most important components in your cabling system are patch panel connections, twists of the pairs at connector transition points, the jacket around the twisted-pair cable, bundling of multiple pairs on horizontal runs and punch down blocks. All of these factors affect the performance of 1000BASE-T technology if not correctly implemented. The following sections are designed to act as a guide to correct cabling for 1000BASE-T.

Cabling

The 1000BASE-T product is designed to operate over Category 5 cabling. To further enhance the operation, the cabling standards have been amended. The latest standard is Category 5e, which defines a higher level of link performance than is available with Category 5 cable.

If installing new cable, we recommend using Category 5e cable, since it costs about the same as Category 5 cable. If using the existing cable, be sure to have the cable plant tested by a professional who can verify that it meets or exceeds either ANSI/EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications.

Length

The maximum distance limitation between two pieces of equipment is 100 m, as per the original Ethernet specification. The end-to-end link is called the “channel.”

TSB-67 defines the “Basic Link” which is the portion of the link that is part of the building infrastructure. This excludes patch and equipment cords. The maximum basic link length is 295 feet (90 m).

Return Loss

Return loss measures the amount of reflected signal energy resulting from impedance changes in the cabling link. The nature of 1000BASE-T renders this measurement very important; if too much energy is reflected back on to the receiver, the device does not perform optimally.

Unlike 10BASE-T and 100BASE-TX, which use only two of the four pairs of wires within the Category 5, 1000BASE-T uses all four pairs of the twisted pair. Make sure all wires are tested — this is important.

Factors that affect the return loss are:

- The number of transition points, as there is a connection via an RJ-45 to another connector, a patch panel, or device at each transition point.
- Removing the jacket that surrounds the four pairs of twisted cable. It is highly recommended that, when RJ-45 connections are made, this is minimized to 1-1/4 inch (32 mm).
- Untwisting any pair of the twisted-pair cabling. It is important that any untwisting be minimized to 3/8 inch (10 mm) for RJ-45 connections.
- Cabling or bundling of multiple Category 5 cables. This is regulated by ANSI/EIA/TIA-568A-3. If not correctly implemented, this can adversely affect all cabling parameters.

Near End Cross Talk (NEXT)

This is a measure of the signal coupling from one wire to another, within a cable assembly, or among cables within a bundle. NEXT measures the amount of cross-talk disturbance energy that is detected at the near end of the link—the end where the transmitter is located. NEXT measures the amount of energy that is “returned” to the sender end. The factors that affect NEXT and cross talk are exactly the same as outlined in the Return Loss section. The cross-talk performance is directly related to the quality of the cable installation.

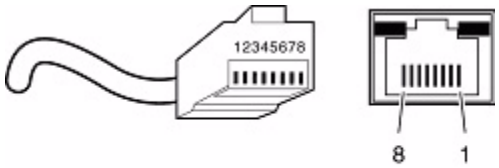
Patch Cables

When installing your equipment, replace old patch panel cables that do not meet Category 5e specifications. As pointed out in the NEXT section, this near end piece of cable is critical for successful operation.

RJ-45 Plug and RJ-45 Connectors

In a Fast Ethernet network, it is important that all 100BASE-T certified Category 5 cabling use RJ-45 plugs. The RJ-45 plug accepts 4-pair UTP or shielded twisted-pair (STP) 100-ohm cable and connects into the RJ-45 connector. The RJ-45 connector is used to connect stations, hubs, and switches through UTP cable; it supports 10 Mbps, 100 Mbps, or 1000 Mbps data transmission.

Figure C-4 shows an RJ-45 plug and RJ-45 connector with built-in LEDs.



Key:
1 to 8 = pin numbers

Figure C-4

Table C-2 lists the pin assignments for the 10/100 Mbps RJ-45 plug and the RJ-45 connector.

Table C-2. 0/100 Mbps RJ-45 Plug and RJ-45 Connector Pin Assignments

Pin	Normal Assignment on Ports 1 to 8	Uplink Assignment on Port 8
1	Input Receive Data +	Output Transmit Data +
2	Input Receive Data –	Output Transmit Data –
3	Output Transmit Data +	Input Receive Data +
6	Output Transmit Data –	Input Receive Data –
4, 5, 7, 8	Internal termination, not used for data transmission	

Table C-2 lists the pin assignments for the 100/1000 Mbps RJ-45 plug and the RJ-45 connector.

Table C-3. 100/1000 Mbps RJ-45 Plug and RJ-45 Connector Pin Assignments

Pin	Channel	Description
1 2	A	Rx/Tx Data + Rx/Tx Data
3 6	B	Rx/Tx Data + Rx/Tx Data
4 5	C	Rx/Tx Data + Rx/Tx Data
7 8	D	Rx/Tx Data + Rx/Tx Data

Conclusion

For optimum performance of your 1000BASE-T product, it is important to fully qualify your cable installation and ensure that it meets or exceeds ANSI/EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications. Install Category 5e cable where possible, including patch panel cables. Minimize transition points, jacket removal, and untwisted lengths. Cable bundles must be properly installed to meet the requirements in ANSI/EIA/TIA-568A-3.

Index

L

M

N

P

Q

R

S

T

U

V

W