GS700TR Smart Switch Software Administration Manual

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

202-10303-01
May, 2008

Technical Support

Please refer to the support information card that shipped with your product. By registering your product at *http://www.netgear.com/register*, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

E-mail: support@netgear.com

North American NETGEAR website: *http://www.netgear.com*

Trademarks

NETGEAR, the NETGEAR logo, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

May, 2008

Statement of Conditions

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

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

Certificate of the Manufacturer/Importer

It is hereby certified that the 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.

Bestätigung des Herstellers/Importeurs

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

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

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing

Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Product and Publication Details

Model Number:	GS700TR
Publication Date:	May, 2008
Product Family:	GS700TR Smart Switch
Product Name:	Gigabit Smart Switch
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10303-01
Publication Version Number:	1.0

Contents

GS700TR Smart Switch Software Administration Manual

Chapter 3
Configuring Switching Information

About This Manual

The *NETGEAR® GS700TR Smart Switch™ Software Administration Manual* describes how to configure and operate the Gigabit Smart Switch using its included software features by using the Web-based graphical user interface (GUI). The book describes the software configuration procedures and explains the options available within those procedures. The Smart Switch software architecture accommodates a variety of software modules so that a platform running Smart Switch software can be a Layer 2 switch in a basic network or a Layer 3 router with static routing support in a large, complex network.

Audience

The information in this guide is intended for any of the following individuals:

- System administrators who are responsible for configuring and operating a network using GS700TR Smart Switch software
- Level 1 and/or Level 2 Support providers

To obtain the greatest benefit from this guide, you should have basic knowledge of Ethernet and networking concepts. Once basic configuration of the switch 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 give your network the full benefit of the switch's features. The web interface simplifies this configuration at all levels.

Organization

The *GS700TR Smart Switch Software Administration Manual* contains the following chapters:

- Chapter 1, "Getting Started"on page 1-1 contains information about performing the initial system configuration and accessing the user interface.
- Chapter 2, "Configuring System Information" on page 2-1 describes how to configure administrative features such as SNMP, DHCP, and port information.
- Chapter 3, "Configuring Switching Information" on page 3-1 describes how to manage and monitor the layer 2 switching features.

- Chapter 4, “Configuring Routing” on page 4-1 describes how to configure the layer 3 routing features.
- Chapter 5, “Configuring Quality of Service” on page 5-1 describes how to manage the GS700TR Smart Switch software ACLs, and how to configure the Differentiated Services and Class of Service features.
- Chapter 6, “Managing Device Security” on page 6-1 contains information about configuring switch security information such as port access control, TACACS+, and RADIUS server settings.
- Chapter 7, “Monitoring the System” on page 7-1 describes how to view a variety of information about the switch and its port, and to configure how the switch monitors events.
- Chapter 8, “Maintenance” on page 8-1 describes features to help you manage the switch.

Additional Documentation

The following documentation provides additional information about GS700TR Smart Switch software:

- Release notes for this GS700TR Smart Switch product describes issues and workarounds.

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::

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

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

	**Note:** A note provides more information about a feature or technology.

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

	**Warning:** A caution provides information about critical aspects of the configuration, combination of settings, events, or procedures that can adversely affect network connectivity, security, and so on.

	**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 Smart Switch according to these specifications:

Product Version	GS700TR Gigabit Smart Switch
Manual Publication Date	May, 2008

	**Note:** Product updates for the GS724TR are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/GS724TR.asp*. Product updates for the GS748TR are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/GS748TR.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print this Manual

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

- **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.** Use the *PDF of This Chapter* link at the top left of any page.
    - 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**. Use the *Complete PDF Manual* link at the top left of any page.
    - Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

- Click the print icon in the upper left of 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
202-10303-01	1.0	May, 2008	Product update: New software and new user Interface

Chapter 1
Getting Started

This chapter provides an overview of starting your NETGEAR GS700TR Gigabit Smart Switch and accessing the user interface. It also leads you through the steps to use the SmartWizard Discovery utility. This chapter contains the following sections:

Connecting the Switch to the Network

To enable remote management of the switch through a Web browser or SNMP, you must connect the switch to the network. The switch comes up with a default IP address of 192.168.0.239, and DHCP is enabled by default.

To access the switch over a network you must first configure it with network information (an IP address, subnet mask, and default gateway). You can assign the IP information automatically by using a BOOTP or DHCP server.

After you configure network information, such as the IP address and subnet mask, and the switch is physically and logically connected to the network, you can manage and monitor the switch remotely through a Web browser or an SNMP-based network management system.

After you perform the physical hardware installation, you need to make a connection to the switch so that you can do one of the following:

- Manually configure network information for the management interface, or
- Enable the management interface as a DHCP or BOOTP client on your network (if not already enabled) and then view the network information after it is assigned by the DHCP server.

Follow these steps:

1. Power on the switch.
2. Configure network information.
3. The switch comes up with a default IP address of 192.168.0.239.

After the switch is connected to the network, you can use the default IP address for remote access to the switch by using a Web browser and logging in to the web interface. You should then be able to select the IP Configuration, under the **System > Management > IP Configuration** menu, for either Static, BOOTP, or DHCP IP assignment.

Switch Management Interface

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 the IP address or subnet mask. Following such configuration, this program leads you into the Web User Interface.

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

Table 1-1. SmartWizard Discovery Utility

Management Method	
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 (available at the application level, i.e. when the switch is not at the boot level) • Provides entry to web configuration of switch

For more details about the SmartWizard Discovery utility, see "SmartWizard Discovery in a Network with a DHCP Server" on page 1-3 or "SmartWizard Discovery in a Network without a DHCP Server" on page 1-4.

SmartWizard Discovery in a Network with a DHCP Server

To install the switch in a network with a DHCP server, use the following steps:

1. Connect the GS700TR 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 GS700TR Gigabit Smart Switch. You should see a screen similar to the one shown in Figure 1-1.

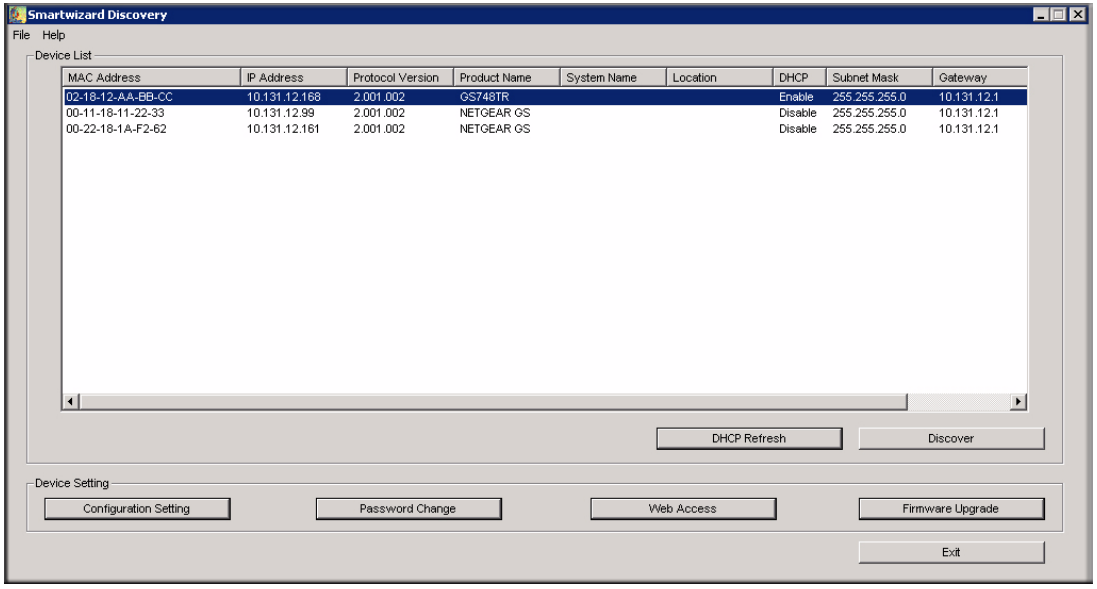


Figure 1-1

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 SmartWizard Discovery utility displays a login window similar to Figure 1-2 on page 1-4.

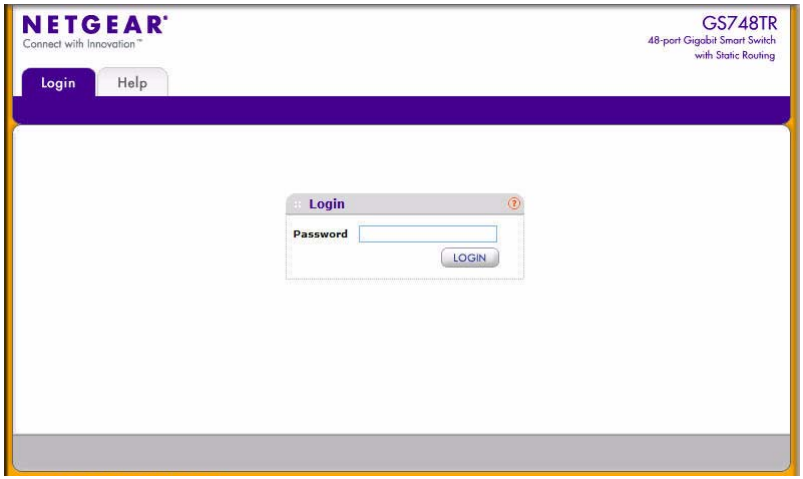


Figure 1-2

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 "Using the Web Interface" on page 1-9.

SmartWizard Discovery in a 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 Assigning Network Parameters" on page 1-4
- "NIC Setting on the Host that Accesses the GS700TR Gigabit Smart Switch" on page 1-5

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.

To assign a static IP address:

1. Connect the GS700TR 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 GS700TR Gigabit Smart Switch. You should see a screen similar to Figure 1-1 on page 1-3.
6. Click **Configuration Setting**. A screen similar to Figure 1-3 appears.

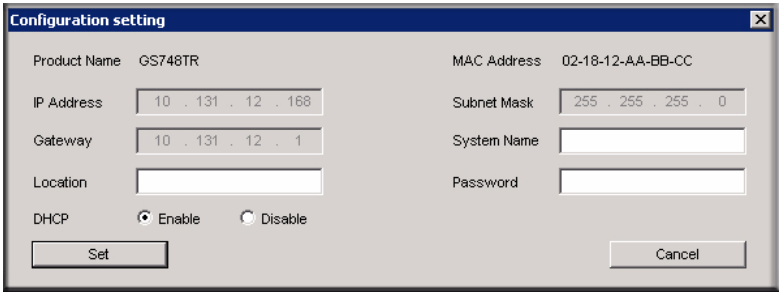


Figure 1-3

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 GS700TR 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 GS700TR Gigabit Smart Switch

The settings of your network interface card (NIC) under the MS Windows OS are made with entries into Windows screen pages similar to the ones shown in Figure 1-4. For comparison, refer to the settings pages of the switch shown in Figure 1-1 on page 1-3 and in Figure 1-3 on page 1-5, although they do not appear in the Windows view. You need Windows Administrator privileges to change these settings.

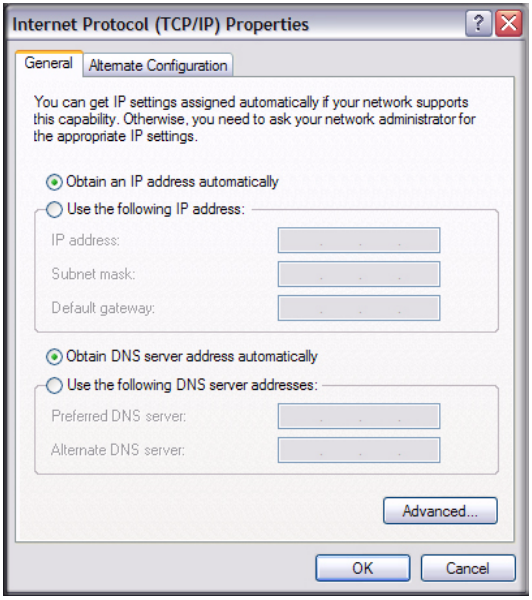


Figure 1-4

To modify your NIC 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 “SmartWizard Discovery Utilities”.

SmartWizard Discovery Utilities

Alternatively, from the SmartWizard Discovery utility’s main page, shown in Figure 1-1 on page 1-3, you can access these additional functions:

- “Password Change” on page 1-7
- “Firmware Upgrade” on page 1-7

Password Change

To set a new password:

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.

> **Note:** Password Change is only available at the application level, i.e. when the switch is not at the boot level

2. Click **Set** to enable the new password.

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

Firmware Upgrade

The application software for the GS700TR Gigabit 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 below. 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.

> **Note:** You can also upgrade the firmware using the TFTP Download and HTTP Download features mentioned in this book. See "Download File To Switch (TFTP)" on page 8-5.

To upgrade your firmware:

1. 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:

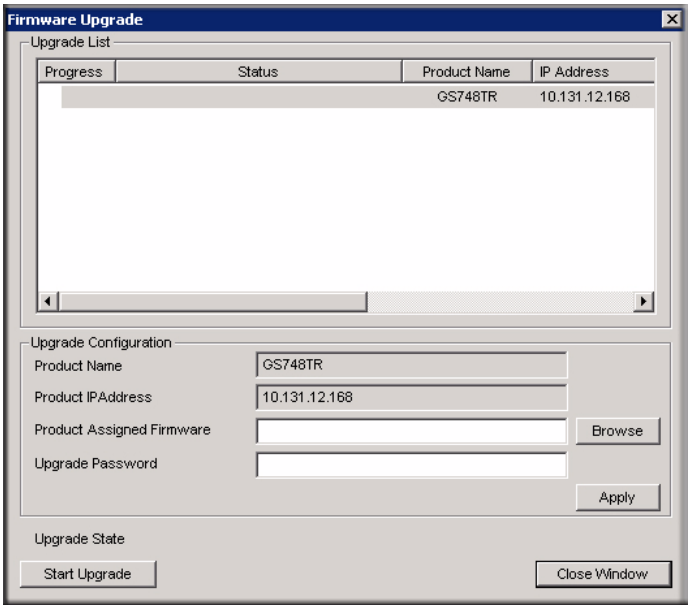


Figure 1-5

2. 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.
3. Click **Start** to begin loading the upgrade. The system software is automatically loaded. When the process is complete, the switch automatically reboots.

Exit

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

Understanding the User Interfaces

GS700TR Smart Switch software includes a set of comprehensive management functions for configuring and monitoring the system by using one of the following methods:

- Web User Interface
- Simple Network Management Protocol (SNMP)

Each of the standards-based management methods allows you to configure and monitor the components of the GS700TR Smart Switch software. The method you use to manage the system depends on your network size and requirements, and on your preference.

The *GS700TR Smart Switch Software Administration Manual* describes how to use the Web-based interface to manage and monitor the system.

Using the Web Interface

To access the switch by using a Web browser, the browser must meet the following software requirements:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript™ version 1.5, or later

Use the following procedures to log on to the Web Interface:

1. Open a Web browser and enter the IP address of the switch in the Web browser address field.
2. The factory default password is **password**. Type the password into the field on the login screen, and then click **Login**. Passwords are case sensitive.

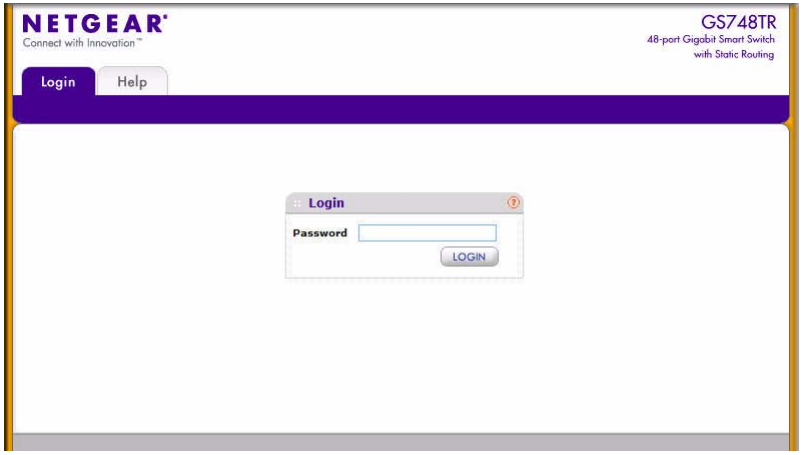


Figure 1-6

3. After the system authenticates you, the System Information page displays.

Figure 1-1 shows the layout of the GS700TR Smart Switch software Web interface. Each Web page contains three main areas: navigation tree on the left, the configuration status and options, and the tabs at the top that provide access to all the configuration functions of the switch and remain constant.

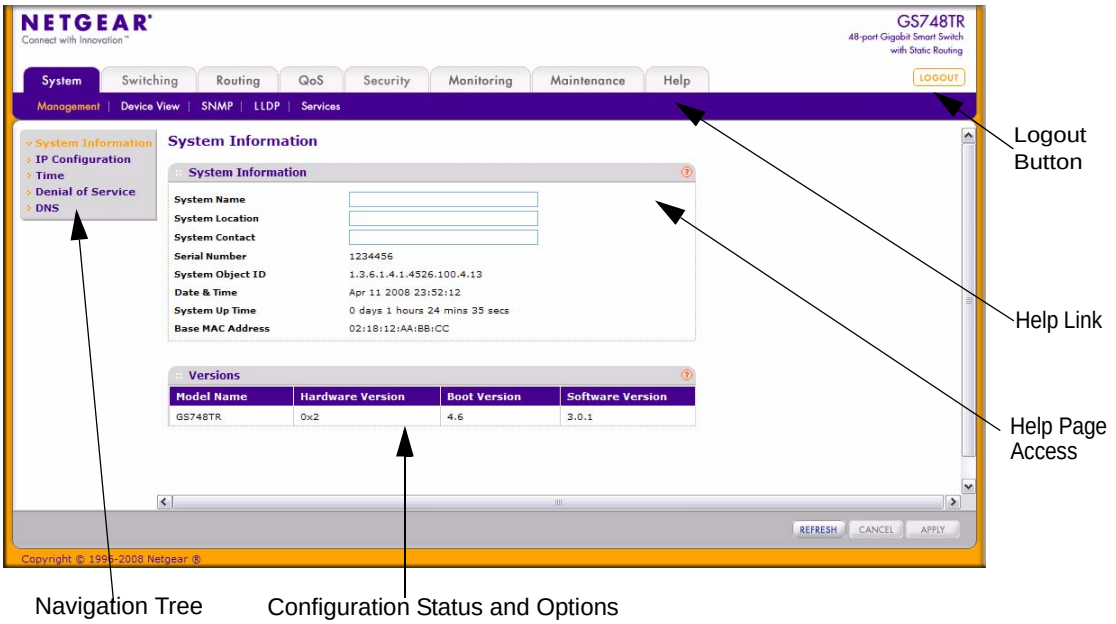


Figure 1-7

Navigation Tabs

The navigation tabs are along the top of the Web interface. The tabs give you quick access to the various device functions.

When you select a tab, its hierarchical-tree view is on the left side of the Web interface. The tree view contains a list of various device features. The branches in the navigation tree can be expanded to view all the components under a specific feature, or retracted to hide the feature's components.

The tree consists of a combination of folders, subfolders, and configuration and status HTML pages. Click the folder to view the options in that folder. Each folder contains either subfolders or HTML pages, or a combination of both. Figure 1-8 on page 1-11 shows an example of a folder, subfolder, and HTML page in the navigation menu. When you click a folder or subfolder, it becomes preceded by a down arrow symbol and, if there is a subfolder, the folder expands to display the contents. If you click an HTML page, a new page displays in the main frame.

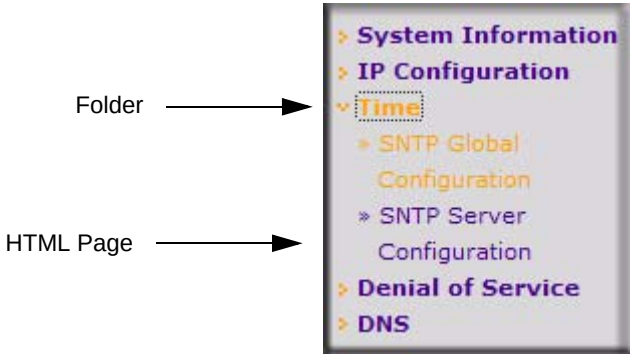


Figure 1-8

Configuration and Monitoring Options

The panel directly under the tabs and to the right of the navigation menu displays the configuration information or status for the page you select. On pages that contain configuration options, you can input information into fields or select options from dropdown menus.

Each page contains access to the HTML-based help that explains the fields and configuration options for the page. Many pages also contain command buttons.

The following command buttons are used throughout the pages in the Web interface:

Table 1-2. Common Command Buttons

Button	Function
Add	Click **Add** to update the switch with the values on a screen. If you want the switch to retain the new values across a power cycle, you must perform a **Save**. Use the **Maintenance > Save Config > Save Configuration** page. For more information, see "Save All Applied Changes" on page 8-1.
Apply	Clicking the **Apply** button sends the updated configuration to the switch. Configuration changes take effect immediately, but some changes are not retained across a power cycle unless you save them to the system configuration file.
Cancel	Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Delete	To remove a configured item, select it and click **Delete**.
Refresh	Clicking the **Refresh** button refreshes the page with the latest information from the router.
Logout	Clicking the **Logout** button ends the session.

Warning: Submitting changes makes them effective during the current boot session only. You must save any changes if you want them to be retained across a power cycle (reboot).

Note: To save configuration changes across a reboot, use the **Maintenance > Save Config > Save Configuration** page. For more information, see "Save All Applied Changes" on page 8-1.

Device View

The Device View is a Java® applet that displays the ports on the switch. This graphic provides an alternate way to navigate to configuration and monitoring options. The graphic also provides information about device ports, current configuration and status, table information, and feature components.

The Device View is available from the **System> Device View** page.

The port coloring indicates if a port is currently active. Green indicates that the port is enabled, red indicates that an error has occurred on the port, and blue indicates that the link is disabled.

Figure 1-9 shows the Device View of the system.

Figure 1-9

Click the port you want to view or configure to see a menu that displays statistics and configuration options. Click the menu option to access the page that contains the configuration or monitoring options.

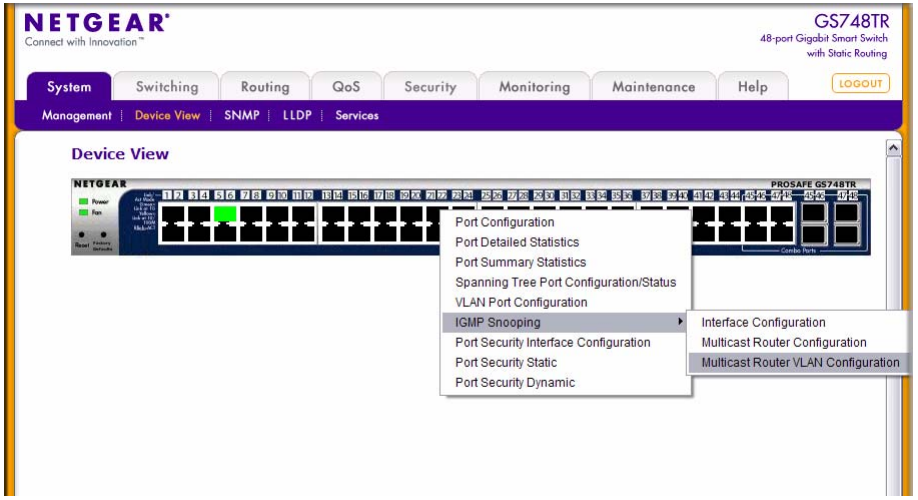


Figure 1-10

If you click the graphic but do not click a specific port, the main menu appears, as Figure 1-11 shows. This menu contains the same option as the navigation tabs at the top of the page.

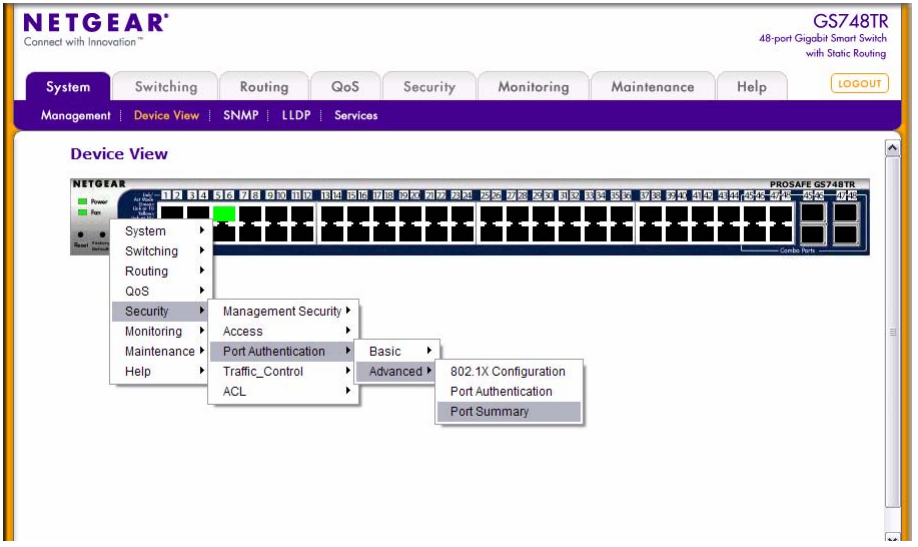


Figure 1-11

Help Page Access

Every page contains a link to the online help  , which contains information to assist in configuring and managing the switch. The online help pages are context sensitive. For example, if the IP Addressing page is open, the help topic for that page displays if you click Help. Figure 1-7 on page 1-10 shows the location of the Help link on the Web interface.

User-Defined Fields

User-defined fields can contain 1-159 characters, unless otherwise noted on the configuration Web page. All characters may be used except for the following (unless specifically noted in for that feature):

\	<
/	>|
*	|
?	

Using SNMP

For GS700TR Smart Switch software that includes the SNMP module, you can configure SNMP groups and users that can manage traps that the SNMP agent generates.

GS700TR Smart Switch uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. All private MIBs begin with a “-” prefix. The main object for interface configuration is in -SWITCHING-MIB, which is a private MIB. Some interface configurations also involve objects in the public MIB, IF-MIB.

SNMP is enabled by default. The **System > Management > System Information** web page, which is the page that displays after a successful login and, for the supported MIBs, the **System > SNMP > SNMP v1/v2 > Supported MIBs** web page, display the information you need to configure an SNMP manager to access the switch.

Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, the switch supports only one user which is **admin**; therefore there is only one profile that can be created or modified.

To configure an SNMPv3 profile by using the Web interface:

1. Select **System > SNMP > SNMPv3 > User Configuration** from the hierarchical tree on the left side of the Web interface.
2. From the **User** menu, select the **User Name.**

To use SNMPv3 Authentication for this user, set a password of eight or more alphanumeric characters.

3. To enable authentication, use the **Authentication Protocol** menu to select either **MD5** or **SHA** for the authentication protocol.
4. To enable encryption, use the **Encryption Protocol** menu to select **DES** for the encryption scheme. Then, enter an encryption code of eight or more alphanumeric characters in the **Encryption Key** field.
5. Click **Apply**.

To access configuration information for SNMPv1 or SNMPv2, click **System** > **SNMP** > **SNMPv1/v2** and click the page that contains the information to configure.

Common Parameter Values

Parameter values might be names (strings) or numbers.To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (““) are not valid user-defined strings. Table 1-3 describes common parameter values and value formatting.

Table 1-3. Parameter Descriptions

Parameter	Description
ipaddr	This parameter is a valid IP address. You can enter the IP address in the following formats: `a.b.c.d (8.8.8.8)`
Interface	g1, g2, etc. for the physical interfaces.
Logical Interface	Represents a logical interface. This is applicable for a LAG (port-channel) interface which is represented as l1, l2...., and applicable for a VLAN routing interface represented as r1, r2....

Interface Naming Convention

GS700TR Smart Switch Switch supports physical and logical interfaces. Interfaces are identified by their type and the interface number. The physical ports are gigabit interfaces and are numbered on the front panel. You configure the logical interfaces by using the software. The following table describes the naming convention for all interfaces available on the switch.

Table 1-4. Types of Interface

Interface	Description	Example
Physical	The physical ports are gigabit Ethernet interfaces and are numbered sequentially starting from one.	g1, g2, g3
Link Aggregation Group (LAG)	LAG interfaces are logical interfaces that are only used for bridging functions.	l1, l2, l3 LAG1, LAG2
VLAN Routing	VLAN routing interfaces are only used for routing functions.	r1, r2, r3

Chapter 2
Configuring System Information

Use the features in the **System** tab to define the switch's relationship to its environment. The **System** tab contains links to the following features:

System Information

After a successful login, the System Information page displays. Use this page to configure and view general device information.

To display the System Information page:

1. Click **System** > **Management** > **System Information** in the navigation tree.

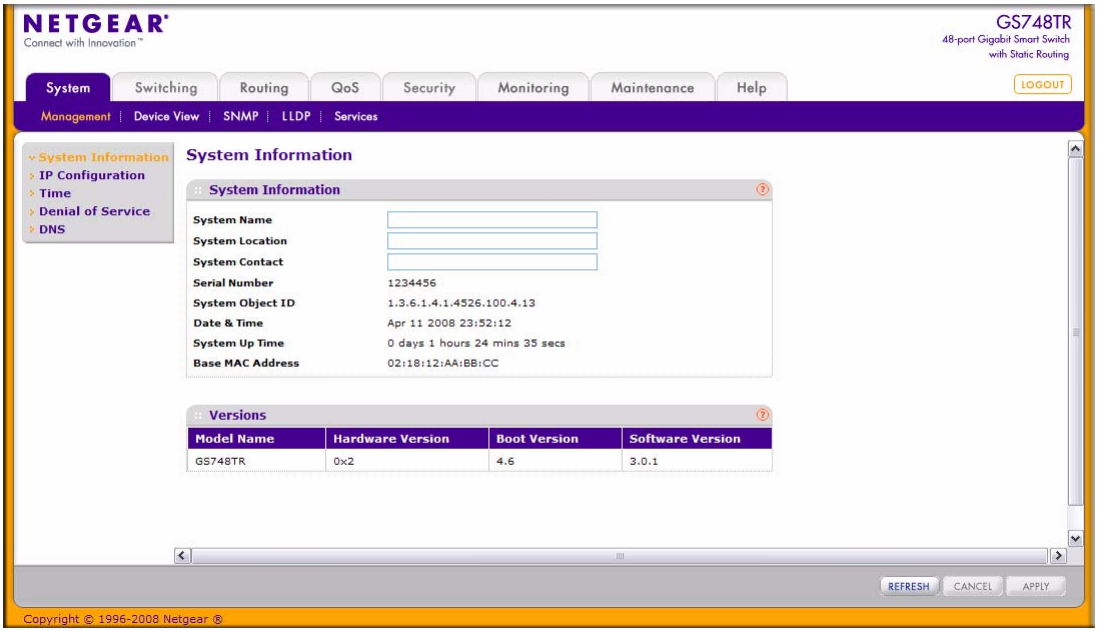


Figure 2-1

Table 2-1. System Description Fields

Field	Description
System Name	Enter the name you want to use to identify this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
System Location	Enter the location of this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
System Contact	Enter the contact person for this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
Serial Number	The serial number of the switch.
System Object ID	The base object ID for the switch's enterprise MIB.
Date & Time	The current date and time.
System Up Time	Displays the number of days, hours, and minutes since the last system restart.
Base MAC Address	The universally assigned network address.
Model Name	The model name of this switch.
Hardware Version	The hardware version of the switch.

Table 2-1. System Description Fields (continued)

Field	Description
Boot Version	The bootcode version of the switch.
Software Version	The software version of the switch.

Defining System Information

1. Open the **System Information** page.
2. Define the following fields: **System Name**, **System Location**, and **System Contact**.
3. Click **Apply**.

   The system parameters are applied, and the device is updated.

Note: If you want the switch to retain the new values across a power cycle, you must perform a save. Click **Maintenance > Save Configuration** to save all applied changes.

Network Connectivity

The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

The Network Connectivity page allows you to change the IP information using the Web interface.

To access the page:

1. Click **System > Management > IP Configuration** in the navigation tree.

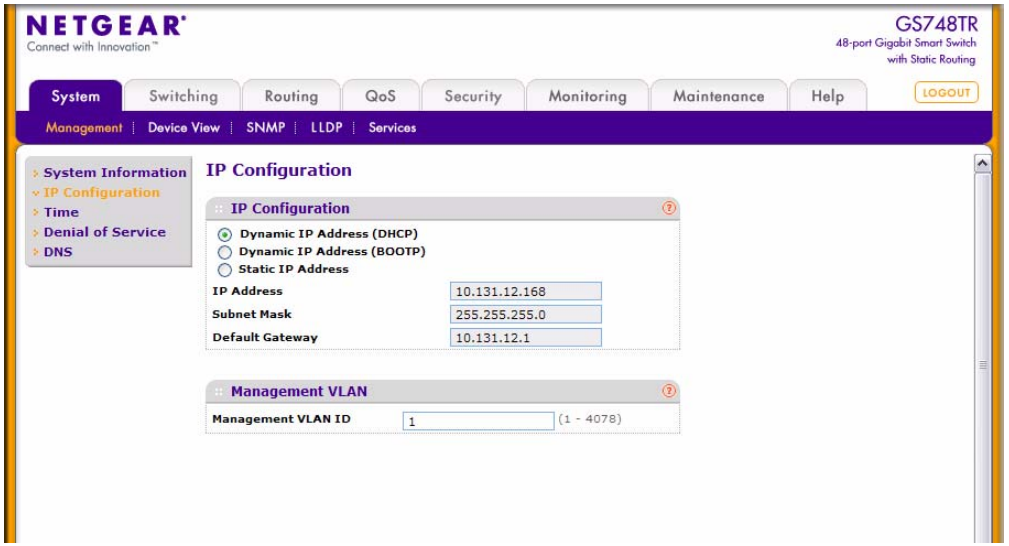


Figure 2-2

2. To access the switch over a network, you must first configure it with IP information (IP address, subnet mask, and default gateway). You can configure the IP information using any of the following options:

- Dynamic IP Address (DHCP)
- Dynamic IP Address (BOOTP)
- Static IP Address

Table 2-2. Network Connectivity Fields

Field	Description
IP Address	The IP address of the network interface. The factory default value is 192.168.0.239. **Note**: Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.
Subnet Mask	The IP subnet mask for the interface. The factory default value is 255.255.255.0.

Table 2-2. Network Connectivity Fields (continued)

Field	Description
Default Gateway	The default gateway for the IP interface. The factory default value is 192.168.0.1.
Management VLAN ID	Specifies the management VLAN ID of the switch. The range is 1-4078. The management VLAN is used for management of the switch. This field is configurable for administrative users and read-only for other users.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you change any of the network connection parameters, click **Apply** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save by clicking **Maintenance** > **Save Configuration**. For more information, see "Save All Applied Changes" on page 8-1.

Time

GS700TR Smart Switch software supports the Simple Network Time Protocol (SNTP).

SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. GS700TR Smart Switch software operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by Stratums. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above since it is itself a stratum 2 device.

The following is an example of stratums:

- **Stratum 0:** A real time clock is used as the time source, for example, a GPS system.
- **Stratum 1:** A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2**: The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the time level and server type.

SNTP time definitions are assessed and determined by the following time levels:

- **T1**: Time at which the original request was sent by the client.
- **T2**: Time at which the original request was received by the server.
- **T3**: Time at which the server sent a reply.
- **T4**: Time at which the client received the server's reply.

The device can poll Unicast and Broadcast server types for the server time.

Polling for Unicast information is used for polling a server for which the IP address is known. SNTP servers that have been configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the SNTP Server Configuration page.

Broadcast information is used when the server IP address is unknown. When a Broadcast message is sent from an SNTP server, the SNTP client listens to the message. If Broadcast polling is enabled, any synchronization information is accepted, even if it has not been requested by the device. This is the least secure method.

The device retrieves synchronization information, either by actively requesting information or at every poll interval. If Unicast and Broadcast polling are enabled, the information is retrieved in this order:

- Information from servers defined on the device is preferred. If Unicast polling is not enabled or if no servers are defined on the device, the device accepts time information from any SNTP server that responds.
- If more than one Unicast device responds, synchronization information is preferred from the device with the lowest stratum.
- If the servers have the same stratum, synchronization information is accepted from the SNTP server that responded first.

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

Time Configuration

Use the Time Configuration page to view and adjust SNTP parameters.

To display the Time Configuration page:

1. Click **System > Management** > **Time > SNTP Global Configuration** in the navigation menu.
2. Use the **Time** option to set the time locally on the switch. Select the **Clock Source** as **Local** by checking the radio button to configure the local time.

Note: If you do not enter a Date and Time, the switch will calculate the date and time using the CPU's clock cycle.

3. In the **Date** field, enter the date in the DD/MM/YYYY format.
4. In the **Time** field, enter the time in HH:MM:SS format.
5. When the Clock Source is set to **Local**, the **Time Zone** field is grayed out (disabled):
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

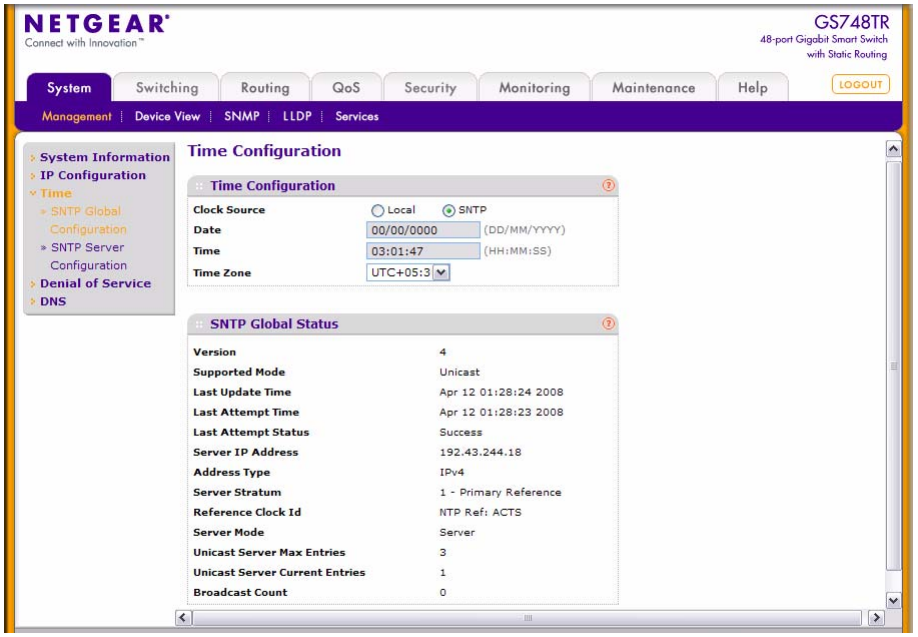


Figure 2-3

To configure the time through SNTP:

1. Select the **Clock Source** as **SNTP** by checking the radio button.
2. When the **Clock Source** is set to ‘SNTP’, the Date and Time fields are grayed out (disabled). The switch gets the date and time from the network.
3. Use the menu to select the Time Zone in which the switch is located, expressed as the number of hours and, optionally, the number of minutes difference from Coordinated Universal Time (UTC) with Offset Hours and Offset Minutes.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

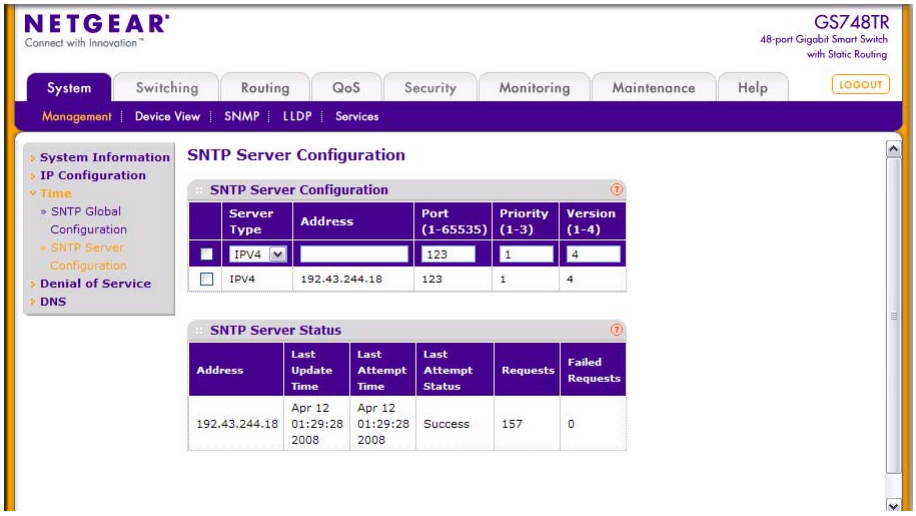


Figure 2-4

Table 2-3. Time Configuration Fields

Field	Description
Clock Source	Use this field to configure time locally or through SNTP. The default is **Local**.
Date	Specifies the duration of the box in days, months and years since the last reboot. This is the default behavior unless you enter a new Date **and** Time. The Time and Date will subsequently be changed to match the Time you entered.
Time	Specifies the duration of the box in hours, minutes and seconds since the last reboot.
Time Zone	When using SNTP/NTP time servers to update the switch's clock, the time data received from the server is based on Coordinated Universal Time (UTC), which is the same as Greenwich Mean Time (GMT). This may not be the time zone in which the switch is located. Time Zone configures a time zone specifying the number of hours and, optionally, the number of minutes difference from UTC with Offset Hours and Offset Minutes. The time zone can affect the display of the current system time. The default value is UTC.

5. Click **Refresh** to refresh the page with the most current data from the switch.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

SNTP Global Status

Use the SNTP Global Status page to view information about the system's SNTP client.

To access the SNTP Global Status page:

1. Click **System > Management > Time > SNTP Global Configuration** in the navigation menu.

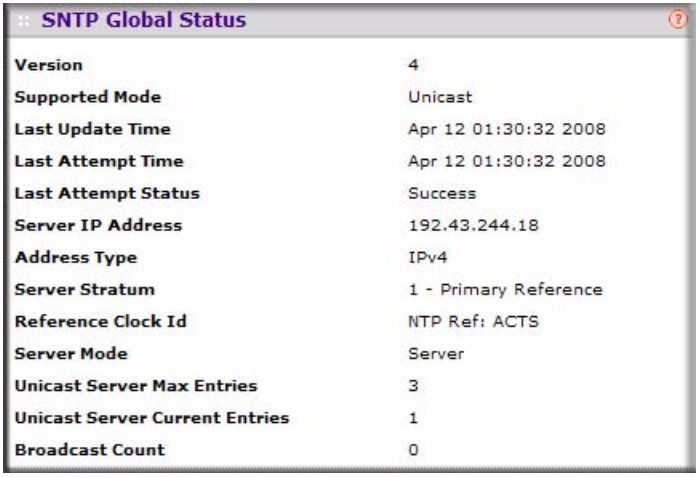


Figure 2-5

Table 2-4. SNTP Global Configuration Fields

Field	Description
Version	Specifies the SNTP Version the client supports.
Supported Mode	Specifies the SNTP modes the client supports. Multiple modes may be supported by a client.
Last Update Time	Specifies the local date and time (UTC) the SNTP client last updated the system clock.
Last Attempt Time	Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.

Table 2-4. SNTP Global Configuration Fields (continued)

Field	Description
Last Attempt Status	Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes: • **Other:** None of the following enumeration values. • **Success:** The SNTP operation was successful and the system time was updated. • **Request Timed Out:** A directed SNTP request timed out without receiving a response from the SNTP server. • **Bad Date Encoded:** The time provided by the SNTP server is not valid. • **Version Not Supported:** The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized:** The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • **Server Kiss Of Death:** The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Server IP Address	Specifies the IP address of the server for the last received valid packet. If no message has been received from any server, an empty string is shown.
Address Type	Specifies the address type of the SNTP Server address for the last received valid packet.
Server Stratum	Specifies the claimed stratum of the server for the last received valid packet.
Reference Clock Id	Specifies the reference clock identifier of the server for the last received valid packet.
Server Mode	Specifies the mode of the server for the last received valid packet.
Unicast Sever Max Entries	Specifies the maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	Specifies the number of current valid unicast server entries configured for this client.
Broadcast Count	Specifies the number of unsolicited broadcast SNTP messages that have been received and processed by the SNTP client since last reboot.

2. Click **Refresh** to refresh the page with the most current data from the switch.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

SNTP Server Configuration

Use the SNTP Server Configuration page to view and modify information for adding and modifying Simple Network Time Protocol SNTP servers.

To display the SNTP Server Configuration page:

1. Click **System > Management > Time > SNTP Server Configuration** in the navigation tree.

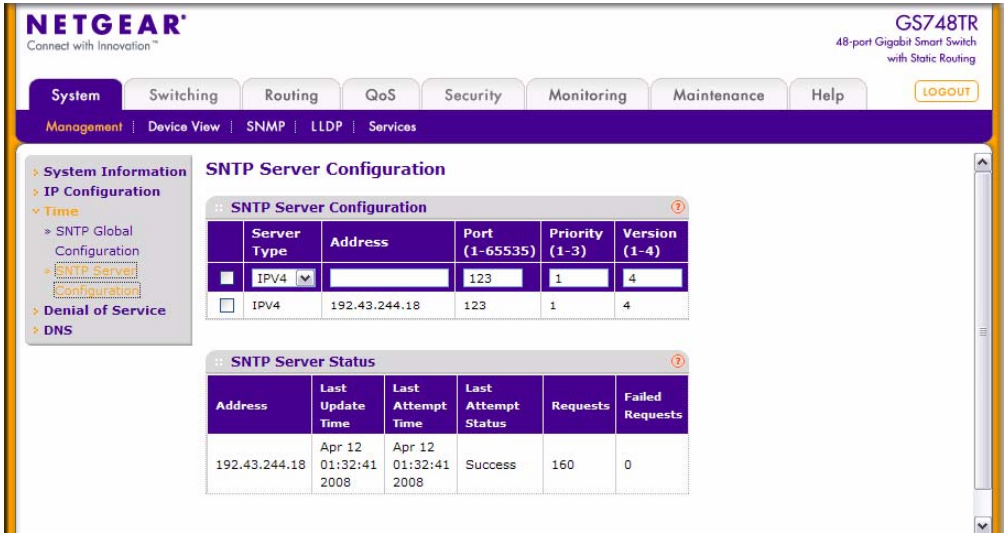


Figure 2-6

Table 2-5. SNTP Server Configuration Fields

Field	Description
Server Type	Specifies the address type of the configured SNTP server to view or modify information about, or select **Add** to configure a new SNTP server. You can define up to three SNTP servers. Select **IPv4** if you entered an IPv4 address or **DNS** if you entered a hostname. The default value is **Unknown**.
Address	Enter the IP address or the hostname of the SNTP server.

Table 2-5. SNTP Server Configuration Fields (continued)

Field	Description
Port	Enter a port number from 1 to 65535. The default is 123.
Priority	Specifies the priority of this server entry in determining the sequence of servers to which SNTP requests are sent. Enter a priority from 1 to 3, with 1 being the default and the highest priority. Servers with lowest numbers have priority.
Version	Enter the protocol version number. The range is 1-4.

2. To add an SNTP server, select **Add**, complete the remaining fields as desired, and click **Apply**. The SNTP server is added, and is now reflected in the Server list. You must perform a save to retain your changes over a power cycle.
3. To removing an SNTP server, select the IP address of the server to remove from the **Server** list, and then click **Delete**. The entry is removed, and the device is updated.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

SNTP Server Status

The SNTP Server Status page displays status information about the SNTP servers configured on your switch.

To access the SNTP Server Status page:

1. Click **System > Management > Time > SNTP Server Configuration** in the navigation menu.

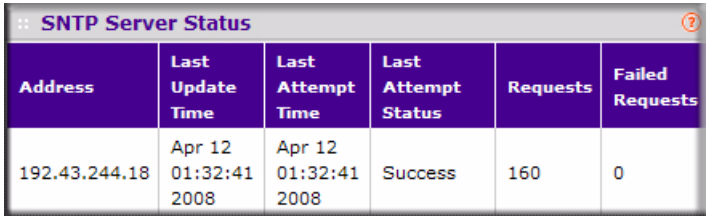


Figure 2-7

Table 2-6. SNTP Server Status Fields

Field	Description
Address	Specifies all the existing Server Addresses. If no Server configuration exists, a message saying “No SNTP server exists” flashes on the screen.
Last Update Time	Specifies the local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	Specifies the local date and time (UTC) that this SNTP server was last queried.
Last Attempt Status	Specifies the status of the last SNTP request to this server. If no packet has been received from this server, a status of Other is displayed: • **Other:** None of the following enumeration values. • **Success:** The SNTP operation was successful and the system time was updated. • **Request Timed Out:** A directed SNTP request timed out without receiving a response from the SNTP server. • **Bad Date Encoded:** The time provided by the SNTP server is not valid. • **Version Not Supported:** The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized:** The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • **Server Kiss Of Death:** The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Requests	Specifies the number of SNTP requests made to this server since last agent reboot.
Failed Requests	Specifies the number of failed SNTP requests made to this server since last reboot.

2. Click **Refresh** to refresh the page with the most current data from the switch.

Denial of Service

Use the Denial of Service (DoS) page to configure DoS control. GS700TR Smart Switch software provides support for classifying and blocking specific types of DoS attacks. You can configure your system to monitor and block six types of attacks:

- **SIP=DIP**: Source IP address = Destination IP address.

- **First Fragment**: TCP Header size smaller then configured value.
- **TCP Fragment**: IP Fragment Offset = 1.
- **TCP Flag**: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port**: Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP**: Limiting the size of ICMP Ping packets.

To access the **Denial of Service** page:

1. Click **System > Management > Denial of Service** in the navigation menu.

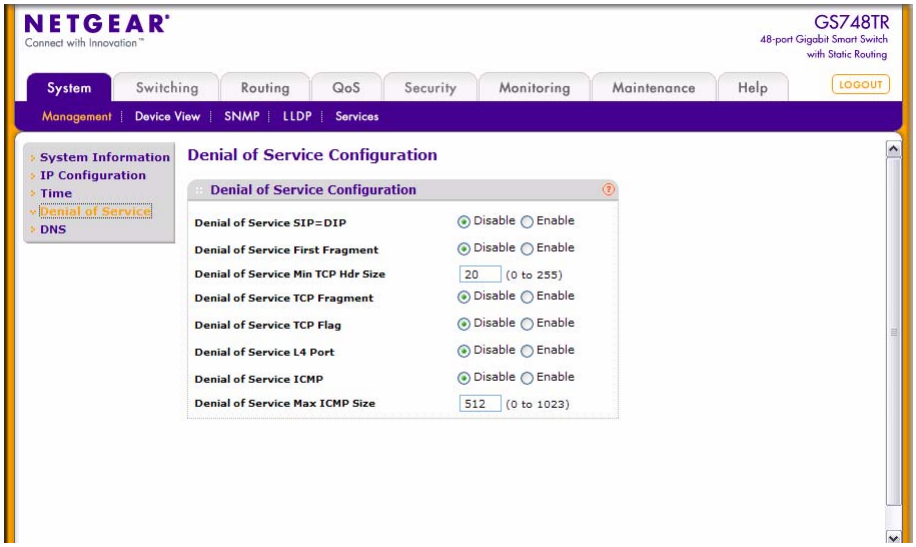


Figure 2-8

Table 2-7. Denial of Service Configuration Fields

Field	Description
Denial of Service SIP=DIP	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling SIP=DIP DoS prevention causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
Denial of Service First Fragment	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling First Fragment DoS prevention causes the switch to drop packets that have a TCP header smaller than the configured Min TCP Hdr Size. The factory default is disabled.
Denial of Service Min TCP Hdr Size	Specify the Min TCP Hdr Size allowed. If First Fragment DoS prevention is enabled, the switch will drop packets that have a TCP header smaller then this configured Min TCP Hdr Size. The factory default is disabled.
Denial of Service TCP Fragment	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Fragment DoS prevention causes the switch to drop packets that have an IP fragment offset equal to 1. The factory default is disabled.
Denial of Service TCP Flag	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Flag DoS prevention causes the switch to drop packets that have TCP flag SYN set and TCP source port less than 1024 or TCP control flags set to 0 and TCP sequence number set to 0 or TCP flags FIN, URG, and PSH set and TCP sequence number set to 0 or both TCP flags SYN and FIN set. The factory default is disabled.
Denial of Service L4 Port	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling L4 Port DoS prevention causes the switch to drop packets that have TCP/UDP source port equal to TCP/UDP destination port. The factory default is disabled.
Denial of Service ICMP	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling ICMP DoS prevention causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMP Pkt Size. The factory default is disabled.
Denial of Service Max ICMP Size	Specify the Max ICMP Pkt Size allowed. If ICMP DoS prevention is enabled, the switch will drop ICMP ping packets that have a size greater then this configured Max ICMP Pkt Size. The factory default is disabled.

2. If you change any of the DoS settings, click **Apply** to apply the changes to the switch.

To preserve the changes across a switch reboot, you must perform a save by clicking **Maintenance > Save Configuration**. For more information, see "Save All Applied Changes" on page 8-1.

Configuring DNS

You can use these pages to configure information about DNS servers the network uses and how the switch/router operates as a DNS client.

DNS Global Configuration

Use this page to configure global DNS settings and to view DNS client status information.

To access this page:

1. Click **System > Management > DNS > DNS Configuration**.

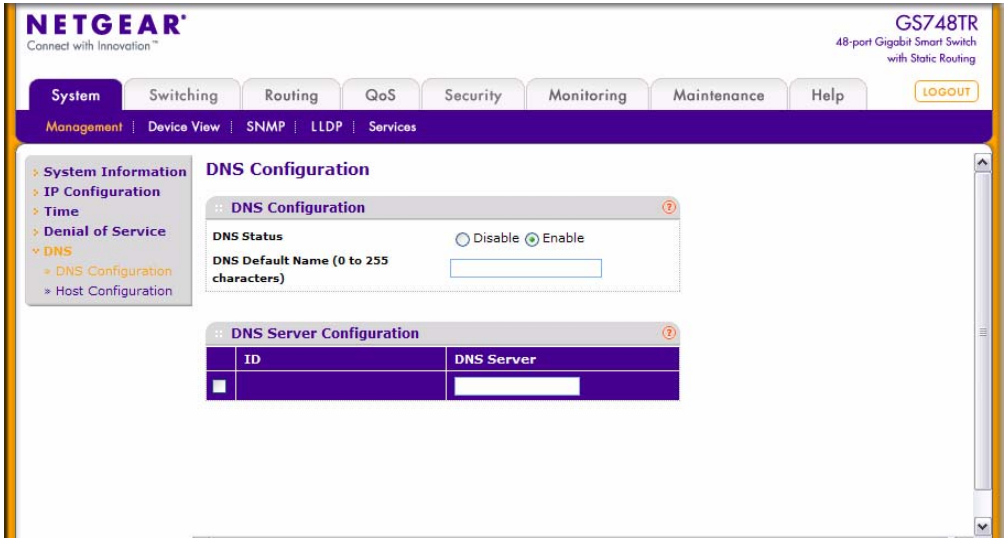


Figure 2-9

Table 2-8. DNS Global Configuration Fields

Field	Description
DNS Status	Select **Enable** or **Disable** to set the administrative status of DNS Client. The default is **Enable**.
DNS Default Name	Enter the default domain name for DNS client messages. When the system is performing a lookup on an unqualified hostname, this field is provided as the domain name (e.g., if default domain name is *.com* and the user enters *hotmail*, then hotmail is changed to *hotmail.com* to resolve the name). By default, no default domain name is configured in the system.

2. To create a new list of domain names, enter a name of the list and click **Apply**. Repeat this step to add multiple domains to the default domain list.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you change any settings, click **Apply** to send the information to the router.

DNS Server Configuration

Use this page to add a specified DNS server to the list of DNS servers.

To access this page:

1. Click **System > Management > DNS > DNS Configuration**.

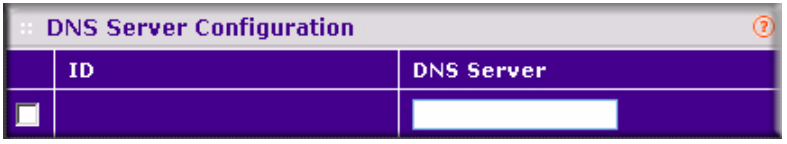


Figure 2-10

Table 2-9. DNS Server Configuration Fields

Field	Description
ID	The ID of the listed DNS Server.
DNS Server	Use this field to specify the DNS Server IP Address.You can add a maximum of eight DNS Servers.

2. To create a new DNS server, enter an IP address in standard IPv4 dot notation in the **DNS Server Address** and click **Add**. The server appears in the list below. The precedence is set in the order created.
3. To remove a DNS server from the list, select the check box next to the item you want to remove and click **Delete**. If no DNS server is specified, the check box is global and will delete all the DNS servers listed.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Host Configuration

Use this page to configure information about DNS servers that the router will use. The order in which you create them determines their precedence; i.e., DNS requests will go to the higher precedence server first. If that server is unavailable or does not respond in the configured response time, then the request goes to the server with the next highest precedence.

To access this page:

1. Click **System > Management > DNS > Host Configuration**.

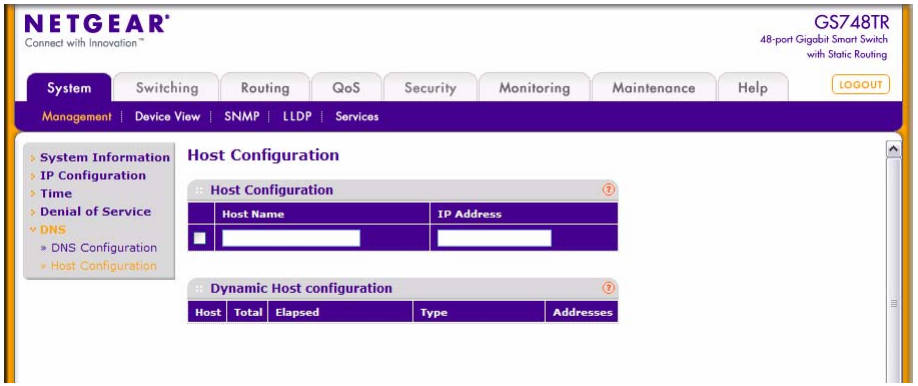


Figure 2-11

Table 2-10. DNS Host Configuration Fields

Field	Description
Host Name	Specify the static host name to be added. Its length cannot exceed 158 characters. This field is mandatory for the user.
IP Address	To add a new DNS server to the list, enter the DNS server IP address in numeric notation.

2. To create a new DNS server, enter an IP address in standard IPv4 dot notation in the **IP Address** field and click **Add**. The server appears in the list below. The precedence is set in the order created.
3. To change precedence, you must remove the server(s) by clicking **Delete**, then add the server(s) in the preferred order.

DNS Dynamic Host Configuration

Use this page to configure static DNS host names for hosts on the network. The host names are associated with IP addresses on the network, which are statically assigned to particular hosts.

To access this page:

1. Click **System > Management > DNS > Host Configuration**.

Figure 2-12

Table 2-11. DNS Host Name Mapping Configuration Fields

Field	Description
Host	Lists the host name you assign to the specified IP address.
Total	Total time of the dynamic entry.
Elapsed	Elapsed time of the dynamic entry.
Type	The type of the dynamic entry.
Addresses	Lists the IP address associated with the host name.

2. Click **Refresh** to refresh the page with the most current data from the switch.
3. Click **Clear** to delete Dynamic Host Entries.

4. Enter a name and click **Add**, or click **Cancel** to cancel and redisplay the list.
5. To remove a hostname, select the box and click **Delete**.
6. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

SNMP V1/V2

The System > SNMP > SNMP V1/V2 folder contains links to the following pages:

- "Community Configuration" on page 2-21
- "Trap Configuration" on page 2-24
- "Trap Flags" on page 2-25

Community Configuration

To display this page, click **System > SNMP > SNMP V1/V2 > Community Configuration** in the navigation tree.

By default, two SNMP Communities exist:

- Private, with Read/Write privileges and status set to **Enable**.
- Public, with Read Only privileges and status set to **Enable**.

These are well-known communities. Use this page to change the defaults or to add other communities. Only the communities that you define using this page will have access to the switch using the SNMPv1 and SNMPv2c protocols. Only those communities with read/write level access can be used to change the configuration using SNMP.

Use this page when you are using the SNMPv1 and SNMPv2c protocol. If you want to use SNMPv3, you should use the User Accounts page.

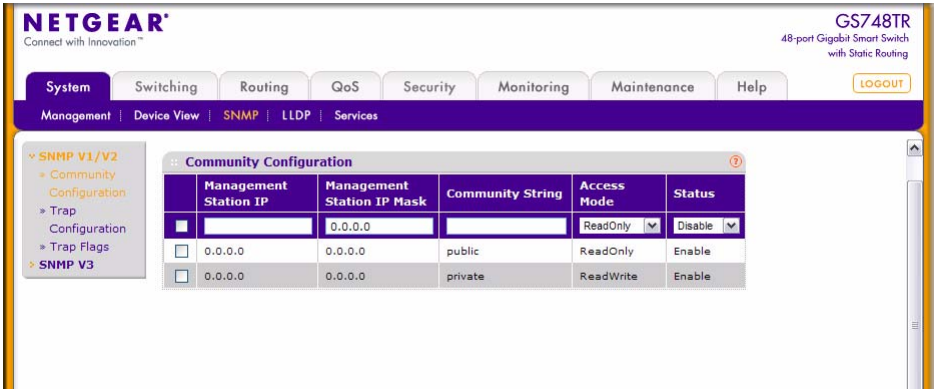


Figure 2-13

Table 2-12. SNMP V1/V2 Community Configurable Data

Field	Description
Management Station IP	Taken together, the Management Station IP and the Management Station IP Mask denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (Management Station IP or Management Station IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's address is ANDed with the mask, as is the Management Station IP Address; and, if the values are equal, access is allowed. For example, if the Management Station IP and Management Station IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Management Station IP Mask value of 255.255.255.255, and use that machine's IP address for Client Address.
Management Station IP Mask	Taken together, the Management Station IP and the Management Station IP Mask denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (Management Station IP or Management Station IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's address is ANDed with the mask, as is the Management Station IP Address; and, if the values are equal, access is allowed. For example, if the Management Station IP and Management Station IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose IP address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Management Station IP Mask value of 255.255.255.255, and use that machine's IP address for Client Address.
Community String	Use this screen to reconfigure an existing community, or to create a new one. Use this pulldown menu to select one of the existing community names, or select **Create** to add a new one. A valid entry is a case-sensitive string of up to 16 characters.
Access Mode	Specify the access level for this community by selecting **Read/Write** or **Read Only** from the pulldown menu.
Status	Specify the status of this community by selecting **Enable** or **Disable** from the pulldown menu. If you select **Enable**, the Community Name must be unique among all valid Community Names or the set request will be rejected. If you select **Disable**, the Community Name will become invalid.

Table 2-13. Command Buttons

Field	Description
Add	Add the currently selected receiver configuration to the switch.
Delete	Delete the currently selected receiver configuration.
Cancel	Cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch.
Apply	Sends the updated configuration to the switch. Configuration changes take effect immediately.

Trap Configuration

This page displays an entry for every active Trap Receiver. To access this page, click **System** > **SNMP** > **SNMP V1/V2** > **Trap Configuration** in the navigation tree.

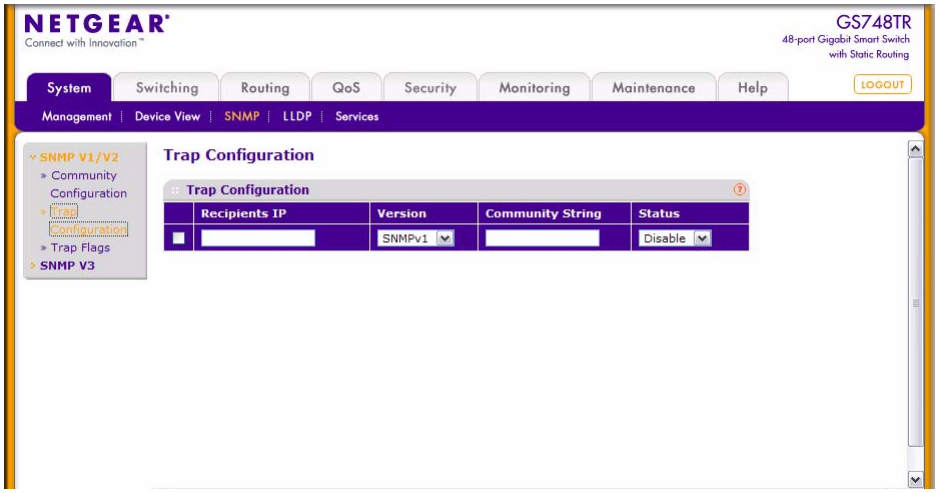


Figure 2-14

Table 2-14. SNMP Trap Configuration

Field	Description
Recipients IP	Enter the address in x.x.x.x format or a hostname starting with an alphabetical character to receive SNMP traps from this device. Length of address cannot exceed 158 characters.
Version	Select the trap version to be used by the receiver from the pulldown menu. • **SNMP v1** - Uses SNMP v1 to send traps to the receiver. • **SNMP v2** - Uses SNMP v2 to send traps to the receiver.
Community String	Enter the community string for the SNMP trap packet to be sent to the trap manager. This may be up to 16 characters and is case sensitive.
Status	Select the receiver's status from the pulldown menu: • **Enable** - Send traps to the receiver. • **Disable** - Do not send traps to the receiver.

Table 2-15. Command Buttons

Field	Description
Add	Add the currently selected receiver configuration to the switch.
Delete	Delete the currently selected receiver configuration.
Cancel	Cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch.
Apply	Sends the updated configuration to the switch. Configuration changes take effect immediately.

Trap Flags

The pages in the Trap Manager folder allow you to view and configure information about SNMP traps the system generates.

Use the Trap Flags page to enable or disable traps the switch can sent to an SNMP manager. When the condition identified by an active trap is encountered by the switch, a trap message is sent to any enabled SNMP Trap Receivers, and a message is written to the trap log.

To access the Trap Flags page:

1. Click **System > SNMP > SNMP V1/V2 > Trap Flags**.

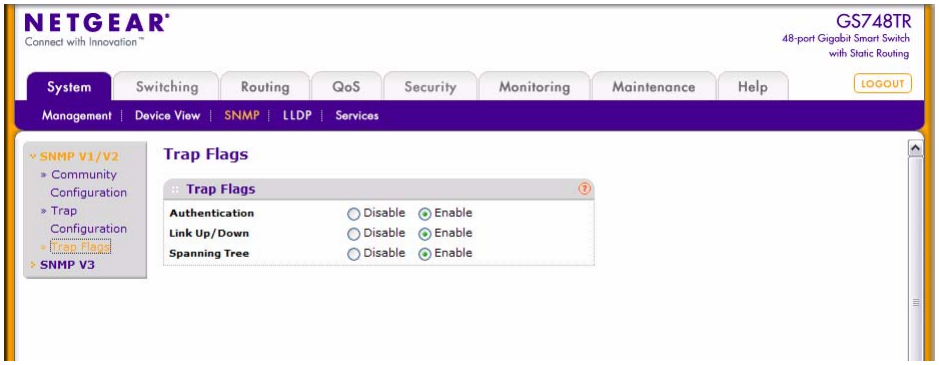


Figure 2-15

The fields available on the Trap Flags page depends on the packages installed on your system. Figure 2-15 and the following table show the fields that are available on a system with all packages installed.

Table 2-16. Trap Flags Configuration Fields

Field	Description
Authentication	Enable or disable activation of authentication failure traps by selecting the corresponding button. The factory default is enabled.
Link Up/Down	Enable or disable activation of link status traps by selecting the corresponding button. The factory default is enabled.
Spanning Tree	Enable or disable activation of spanning tree traps by selecting the corresponding button. The factory default is enabled.

2. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

SNMP v3 User Configuration

This is the configuration for SNMP v3.

To access this page:

1. Click **System > SNMP > SNMP V3 > User Configuration** in the navigation menu.

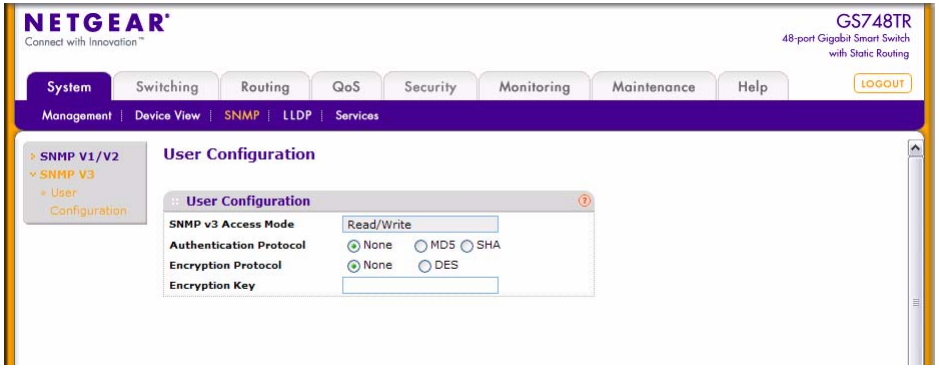


Figure 2-16

Table 2-17. SNMP v3 User Configuration

Field	Description
SNMP v3 Access Mode	The SNMPv3 access privileges for the user account. The admin account always has Read/Write access, and all other accounts have Read Only access.
Authentication Protocol	Specify the SNMPv3 Authentication Protocol setting for the selected user account. The valid Authentication Protocols are **None**, **MD5**, or **SHA**. If you select: • **None** - The user will be unable to access the SNMP data from an SNMP browser. • **MD5** or **SHA** - The user login password will be used as SNMPv3 authentication password, and you must therefore specify a password. The password must be eight characters in length.
Encryption Protocol	Specify the SNMPv3 Encryption Protocol setting for the selected user account. The valid Encryption Protocols are **None** or **DES**. If you select the DES Protocol, you must enter a key in the Encryption Key field. If **None** is specified for the Protocol, the Encryption Key is ignored.
Encryption Key	If you selected DES in the Encryption Protocol field, enter the SNMPv3 Encryption Key here. Otherwise, this field is ignored. Valid keys are 0 to 15 characters long. The Apply check box must be checked in order to change the Encryption Protocol and Encryption Key.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

LLDP

The IEEE 802.1AB defined standard, Link Layer Discovery Protocol (LLDP), allows stations residing on an 802 LAN to advertise major capabilities and physical descriptions. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The transmit and receive functions can be enabled/disabled separately per port. By default, both transmit and receive are disabled on all ports. The application is responsible for starting each transmit and receive state machine appropriately, based on the configured status and operational state of the port.

The LLDP folder contains links to the following pages:

LLDP Global Configuration

Use the LLDP Global Configuration page to specify LLDP parameters that are applied to the switch.

To display the LLDP Global Configuration page:

1. Click **System > LLDP > Global Configuration** in the navigation tree.

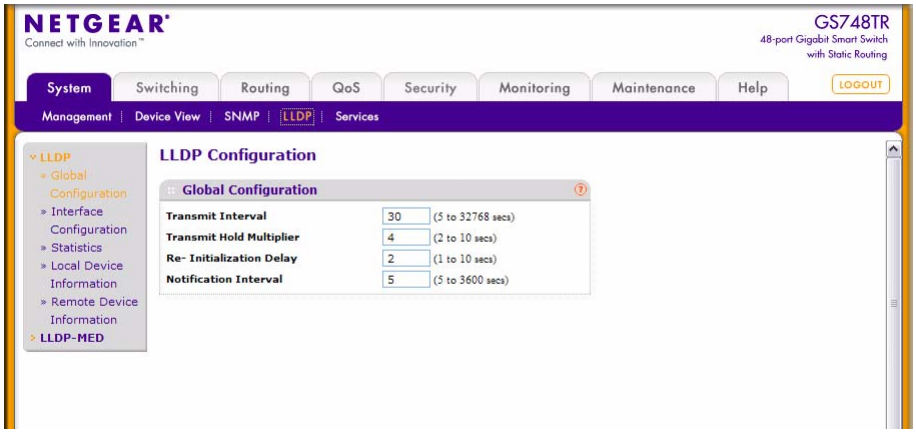


Figure 2-17

Table 2-18. LLDP Global Configuration Fields

Field	Description
Transmit Interval	Specifies the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 1-32768 seconds.
Transmit Hold Multiplier	Specifies multiplier on the transmit interval to assign to Time-to-Live (TTL). The default is 4, and the range is 2-10.
Re-Initialization Delay	Specifies delay before a re-initialization. The default is 2 seconds, and the range is 1-10 seconds.
Notification Interval	Limits the transmission of notifications. The default is 5 seconds, and the range is 5-3600 seconds.

2. If you make any changes to the page, click **Apply** to apply the new settings to the system.

Interface Configuration

Use the LLDP Interface Configuration page to specify LLDP parameters that are applied to a specific interface.

To display the LLDP Interface Configuration page:

1. Click **System** > **LLDP** > **Interface Configuration** in the navigation tree.

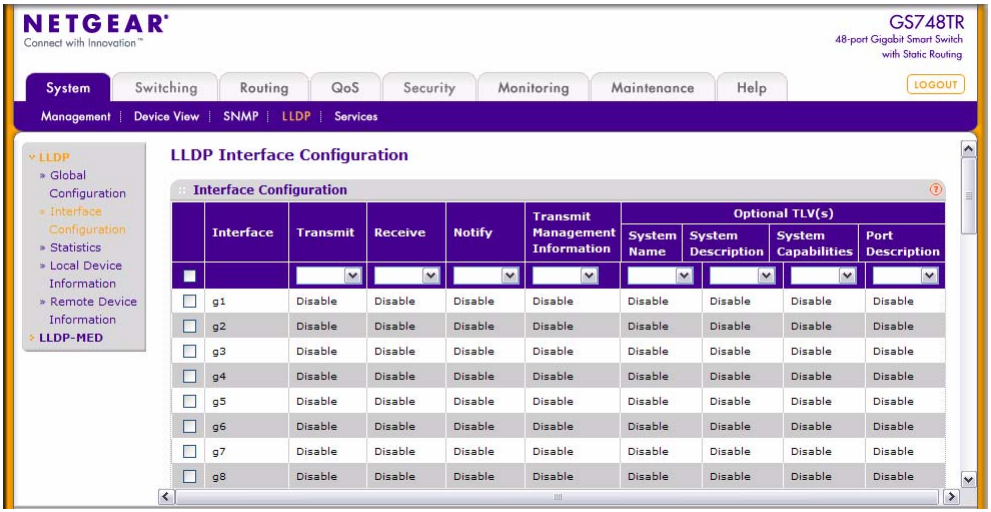


Figure 2-18

Table 2-19. LLDP Interface Configuration Fields

Field	Description
Interface	Specifies the port to be affected by these parameters.
Transmit	Enables or disables the transmission of LLDP protocol data units (PDUs). The default is disabled.
Receive	Enables or disables the ability of the port to receive LLDP PDUs. The default is disabled.
Notify	When notifications are enabled, LLDP interacts with the Trap Manager to notify subscribers of remote data change statistics. The default is disabled.
Transmit Management Information	Select the check box to enable the transmission of management address instance. Clear the check box to disable management information transmission. The default is disabled.
Optional TLV(s)	Select each check box next to the type-length value (TLV) information to transmit. Choices include **System Name**, **System Description**, **System Capabilities**, and **Port Description**. To configure the System Name, see "System Information" on page 2-1. To configure the Port Description, see "Configuring and Viewing Device Port Information" on page 3-1.

2. If you make any changes to the page, click **Apply** to apply the new settings to the system.

3. To update the page with the latest data, click **Refresh**.

LLDP Statistics

Use the LLDP Statistics page to view the global and interface LLDP statistics.

To display the LLDP Statistics page:

1. Click **System > LLDP > Statistics** in the navigation tree.

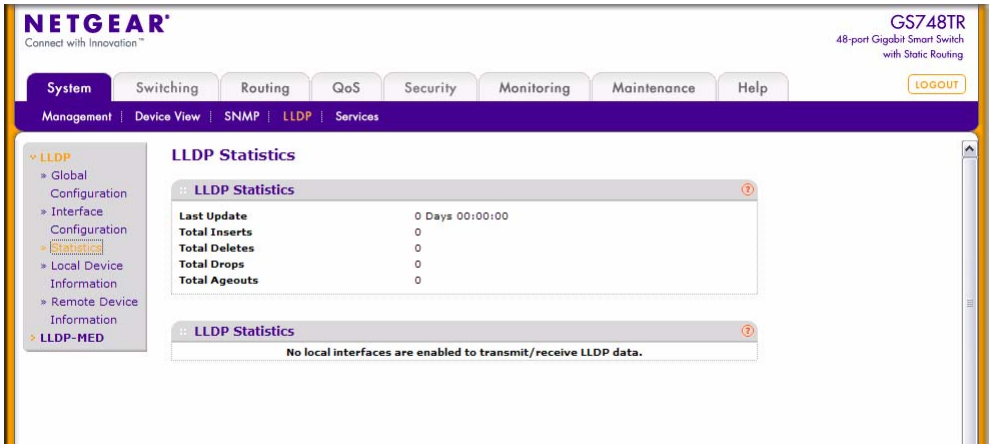


Figure 2-19

Table 2-20. LLDP Statistics Fields

Field	Description
System-wide Statistics	
Last Update	Displays the value of system up time the last time a remote data entry was created, modified, or deleted.
Total Inserts	Displays the number of times a complete set of information advertised by a remote switch has been inserted into the table.
Total Deletes	Displays the number of times a complete set of information advertised by a remote switch has been deleted from the table.
Total Drops	Displays the number of times a complete set of information advertised by a remote switch could not be inserted due to insufficient resources.
Total Ageouts	Displays the number of times any remote data entry has been deleted due to TTL (Time-to-Live) expiration.

Table 2-20. LLDP Statistics Fields (continued)

Field	Description
Port Statistics	
Interface	Displays the Unit and Port to which the statistics on that line apply.
Transmit Total	Displays the total number of LLDP frames transmitted on the indicated port.
Receive Total	Displays the total number of valid LLDP frames received on the indicated port.
Discards	Displays the number of LLDP frames received on the indicated port and discarded for any reason.
Errors	Displays the number of invalid LLDP frames received on the indicated port.
Ageouts	Displays the number of times a remote data entry on the indicated port has been deleted due to TTL expiration.
TLV Discards	Displays the number of LLDP TLVs (Type, Length, Value sets) received on the indicated port and discarded for any reason by the LLDP agent.
TLV Unknowns	Displays the number of LLDP TLVs received on the indicated port for a type not recognized by the LLDP agent.
TLV MED	Displays the total number of LLDP-MED TLVs received on the local ports.
TLV 802.1	Displays the total number of LLDP TLVs received on the local ports which are of type 802.1.
TLV 802.3	Displays the total number of LLDP TLVs received on the local ports which are of type 802.3.

2. Click **Refresh** to refresh the page with the most current data from the switch.
3. Click **Clear Counters** to reset all LLDP statistics to zero.

Local Device Information

Use the LLDP Local Device Information page to view the data that each port advertises through LLDP.

To display the LLDP Local Device Information page:

1. Click **System** > **LLDP** > **Local Device Information** in the navigation tree.

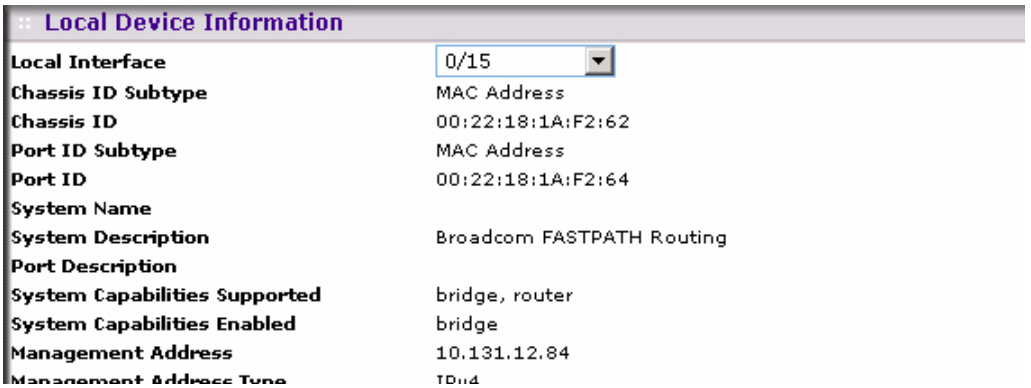


Figure 2-20

Table 2-21. LLDP Local Device Information Fields

Field	Description
Local Interface	Select the interface with the information to display.
Chassis ID Subtype	Identifies the type of data displayed in the **Chassis ID** field
Chassis ID	Identifies the 802 LAN device's chassis.
Port ID Subtype	Identifies the type of data displayed in the **Port ID** field.
Port ID	Identifies the physical address of the port.
System Name	Identifies the system name associated with the remote device. To configure the System Name, see "System Information" on page 2-1.
System Description	Specifies the description of the selected port associated with the local system.
Port Description	Identifies the user-defined description of the port. To configure the Port Description, see "Configuring and Viewing Device Port Information" on page 3-1.
System Capabilities Supported	Specifies the system capabilities of the local system.
System Capabilities Enabled	Specifies the system capabilities of the local system which are supported and enabled.
Management Address	Specifies the advertised management address of the local system.
Management Address Type	Specifies the type of the management address.

2. Click **Refresh** to refresh the page with the most current data from the switch.

Remote Device Information

Use the LLDP Remote Device Information page to view the data that a specified interface has received from other LLDP-enabled systems.

To display the LLDP Remote Device Information page:

1. Click **System** > **LLDP** > **Remote Device Information** in the navigation tree.

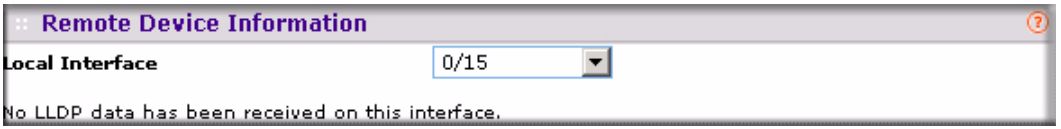


Figure 2-21

Table 2-22. LLDP Remote Device Information Fields

Field	Description
Local Interface	Select the interface on the local system to display the LLDP information it has received from a remote system. If no LLDP data has been received on the select interface, then a message stating so displays. If the selected interface has received LLDP information from a remote device, the fields listed below display.
Chassis ID Subtype	Identifies the type of data displayed in the **Chassis ID** field on the remote system.
Chassis ID	Identifies the remote 802 LAN device's chassis.
Port ID Subtype	Identifies the type of data displayed in the remote system's **Port ID** field.
Port ID	Identifies the physical address of the port on the remote system from which the data was sent.
System Name	Identifies the system name associated with the remote device.
System Description	Specifies the description of the selected port associated with the remote system.
Port Description	Identifies the user-defined description of the port.
System Capabilities Supported	Specifies the system capabilities of the remote system.
System Capabilities Enabled	Specifies the system capabilities of the remote system which are supported and enabled.
Management Address	Specifies the advertised management address of the remote system.
Management Address Type	Specifies the type of the management address.

2. Click **Refresh** to update the information on the screen with the most current data.

LLDP-MED

The Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP that features:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Diffserv settings), enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet endpoints.
- Inventory management, enabling network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial/asset number).

The LLDP-MED folder provides access to the following pages:

- "LLDP-MED Global Configuration" on page 2-35
- "LLDP-MED Interface configuration" on page 2-36
- "LLDP-MED Local Device Information" on page 2-38
- "LLDP-MED Remote Device Information" on page 2-39

LLDP-MED Global Configuration

Use this page to set global parameters for LLDP-MED operation. To display this page:

1. Click **System** > **LLDP** > **LLDP-MED** > **Global Configuration** in the navigation tree.

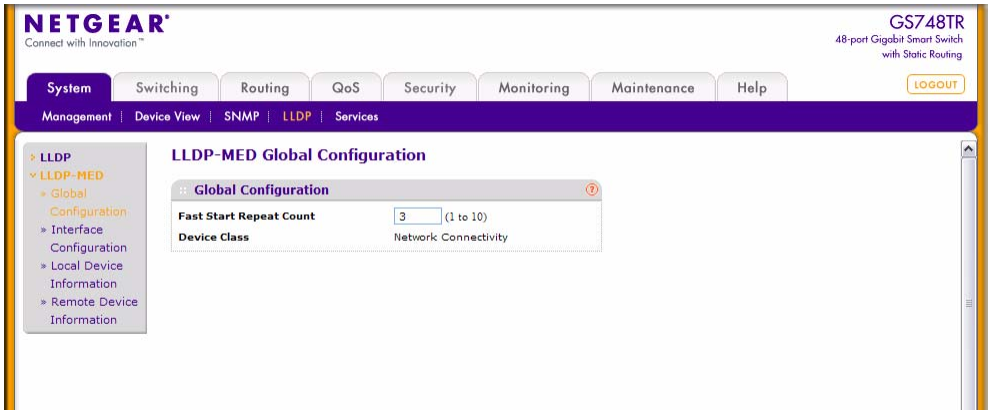


Figure 2-22

Table 2-23. LLDP Global Configuration Fields

Field	Description
Fast Start Repeat Count	Specifies the number of LLDP PDUs that will be transmitted when the protocol is enabled. The range is from 1 to 10. The default value is 3.
Device Class	Specifies local device's MED Classification. The following three represent the actual endpoints: • Class I Generic [IP Communication Controller etc.] • Class II Media [Conference Bridge etc.] • Class III Communication [IP Telephone etc.]) The fourth device is Network Connectivity Device, which is typically a LAN switch/router, IEEE 802.1 bridge, IEEE 802.11 wireless access point, etc.

2. Click **Apply** to updated the switch. The changes take effect but will not be retained across a power cycle unless a save is performed.

LLDP-MED Interface configuration

Use this page to enable LLDP-MED mode on an interface and configure its properties.

To display this page:

1. Click **System > LLDP > LLDP-MED > Interface Configuration** in the navigation tree. A portion of the web screen is shown below.

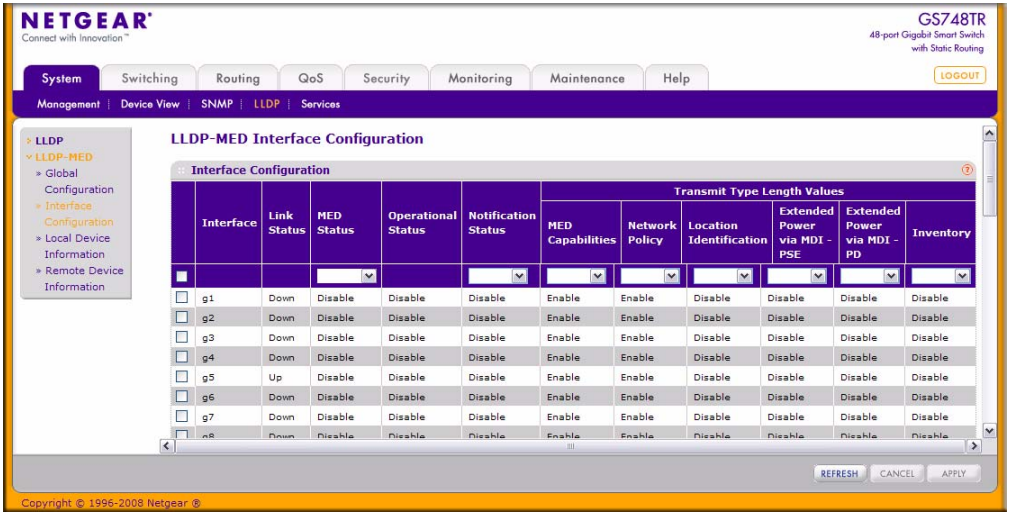


Figure 2-23

Table 2-24. LLDP-MED Interface Configuration Fields

Field	Description
Interface	Selects the port that you want to configure LLDP-MED on. You can select **All** to configure all interfaces with the same properties.
Link Status	Specifies the link status of the ports as Up/Down.
MED Status	Specifies the transmit and/or receive LLDP-MED mode is enabled or disabled on this interface.
Operational Status	Specifies whether the interface will transmit TLVs.
Notification Status	Specifies the LLDP-MED topology notification mode of the interface.
Transmit Type Length Values	Specifies which optional type length values (TLVs) in the LLDP-MED will be transmitted in the LLDP PDUs frames for the selected interface: • **MED Capabilities**: Transmits the capabilities TLV in LLDP frames. • **Network Policy**: Transmits the network policy TLV in LLDP frames. • **Location Identification**: Transmits the location TLV in LLDP frames. • **Extended Power via MDI - PSE**: Transmits the extended PSE TLV in LLDP frames. • **Extended Power via MDI - PD**: Transmits the extended PD TLV in LLDP frames. • **Inventory**: Transmits the inventory TLV in LLDP frames.

2. Click **Apply** to send the updated configuration to the switch. These changes take effect immediately but will not be retained across a power cycle unless a save is performed.

LLDP-MED Local Device Information

This page displays information on LLPD-MED information advertised on the selected local interface.

To display this page:

1. Click **System > LLDP > LLDP-MED > Local Device Information** in the navigation tree.

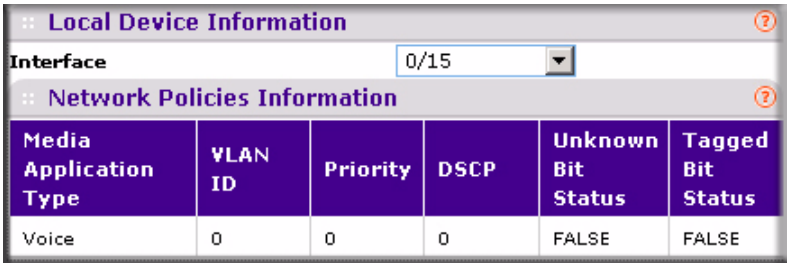


Figure 2-24

Table 2-25. LLPD-MED Local Device Information Fields

Field	Description
Interface	Selects the LLDP-enabled port to display information about.
Network Policies Information	Specifies if network policy TLV is present in the LLDP frames: • **Media Application Type**: Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Each application type that is received has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been transmitted only then would this information be displayed. • **VLAN ID**: Specifies the VLAN id associated with a particular policy type. • **Priority**: Specifies the priority associated with a particular policy type. • **DSCP**: Specifies the DSCP associated with a particular policy type. • **Unknown Bit Status**: Specifies the unknown bit associated with a particular policy type. • **Tagged Bit Status**: Specifies the tagged bit associated with a particular policy type.

2. Click **Refresh** to refresh the page with the most current data from the switch.

LLDP-MED Remote Device Information

This page displays information on LLPD-MED information received from remote clients on the selected local interface. To display this page:

1. Click **System > LLDP > LLDP-MED > Remote Device Information** in the navigation tree.

Figure 2-25

Table 2-26. LLPD-MED Local Device Information Fields

Field	Description
Local Interface	Specifies the list of all the ports on which LLDP-MED is enabled.
Capability Information	Specifies the supported and enabled capabilities that was received in MED TLV on this port: • **Supported Capabilities**: Specifies supported capabilities that was received in MED TLV on this port. • **Enabled Capabilities**: Specifies enabled capabilities that was received in MED TLV on this port. • **Device Class**: Specifies device class as advertised by the device remotely connected to the port.

Table 2-26. LLPD-MED Local Device Information Fields (continued)

Field	Description
Network Policy Information	Specifies if network policy TLV is present in the LLDP frames: • **Media Application Type**: Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, vidoesignalling. Each application type that is received has the VLAN id, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been transmitted only then would this information be displayed. • **VLAN ID**: Specifies the VLAN id associated with a particular policy type. • **Priority**: Specifies the priority associated with a particular policy type. • **DSCP**: Specifies the DSCP associated with a particular policy type. • **Unknown Bit Status**: Specifies the unknown bit associated with a particular policy type. • **Tagged Bit Status**: Specifies the tagged bit associated with a particular policy type.
Inventory	Specifies the inventory TLV present in LLDP frames: • Hardware Revisions • Firmware Revisions • Software Revisions • Serial Number • Manufacturer Name • Model Name • Asset ID
Location Information	Specifies if location TLV is present in LLDP frames: • **Sub Type**: Specifies type of location information. • **Location Information**: Specifies the location information as a string for given type of location ID.
Extended PoE	Specifies if local device is a PoE device.
Extended PoE PSE	Specifies if extended PSE TLV is present in LLDP frame: • **Available**: Specifies available power sourcing equipment's power value in tenths of watts on the port of local device. • **Source**: Specifies power source of this port. • **Priority**: Specifies PSE port power priority.
Extended PoE PD	Specifies if extended PD TLV is present in LLDP frame. • **Required**: Specifies required power device power value in tenths of watts on the port of local device. • **Source**: Specifies power source of this port. • **Priority**: Specifies PD port power priority.

2. Click **Refresh** to refresh the page with the most current data from the switch.

DHCP Filtering

DHCP Filtering is a useful feature that can be employed as a security measure against unauthorized DHCP servers. A known attack is when an unauthorized DHCP server responds to a client that is requesting an IP address. The server configures the gateway for the client to be equal to the IP address of the server. At that point, the client sends all of its IP traffic destined to other networks to the unauthorized machine. This gives the attacker the possibility of snooping traffic for passwords or employing a 'man-in-the-middle' attack. DHCP Filtering works by allowing the administrator to configure each port as either a trusted port or an untrusted port. The port that has the authorized DHCP server should be configured as a trusted port. Any DHCP responses received on a trusted port are forwarded. All other ports should be configured as untrusted. Any DHCP (or BootP) responses received are discarded.

Configuration

Use the DHCP Filtering Configuration page to enable or disable the DHCP Filtering feature on the switch.

To access the DHCP Filter Configuration page:

1. Click **System > Services > DHCP Filtering > Configuration** in the navigation tree.

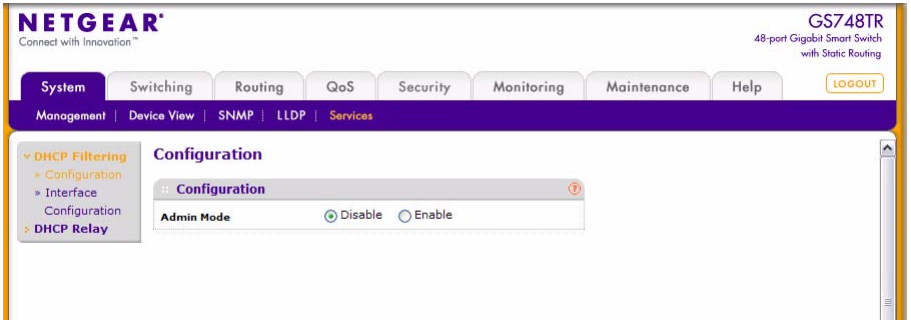


Figure 2-26

2. In the **Admin Mode** field, select **Enable** or **Disable** to turn the DHCP Filtering feature on or off, and then click **Apply** to apply the change to the system. Configuration changes take effect immediately.
3. Click **Refresh** to refresh the page with the most current data from the switch.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Interface Configuration

Use the DHCP Filtering Interface Configuration page to view and configure each port as a trusted or untrusted port. Any DHCP responses received on a trusted port are forwarded. If a port is configured as untrusted, any DHCP (or BootP) responses received on that port are discarded.

To access the DHCP Filtering Interface Configuration page:

1. Click **System** > **Services** > **DHCP Filtering** > **Interface Configuration** in the navigation tree.

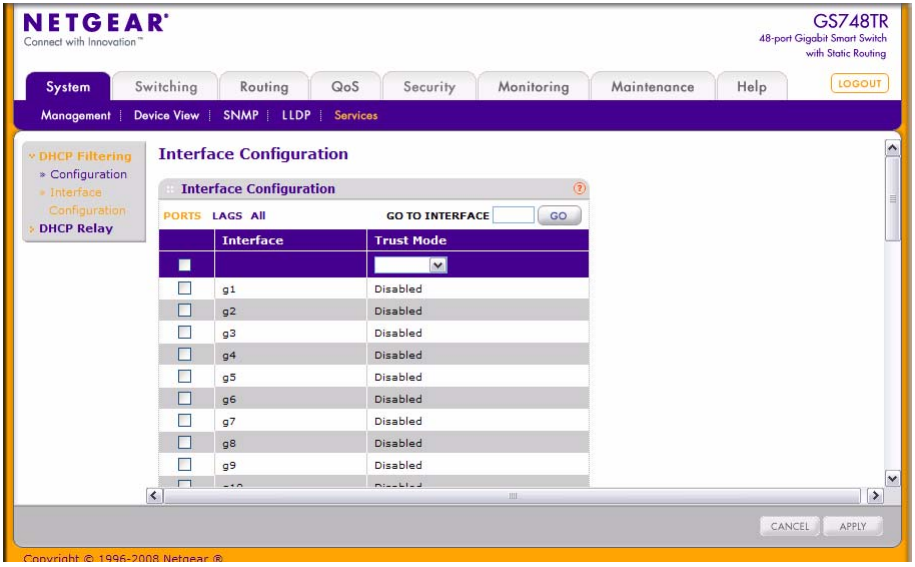


Figure 2-27

2. To display the list of physical ports, click **PORTS**. An example is shown in Figure 2-27.
3. To display the list of logical interfaces, click **LAGS**. An example is shown in Figure 2-28.

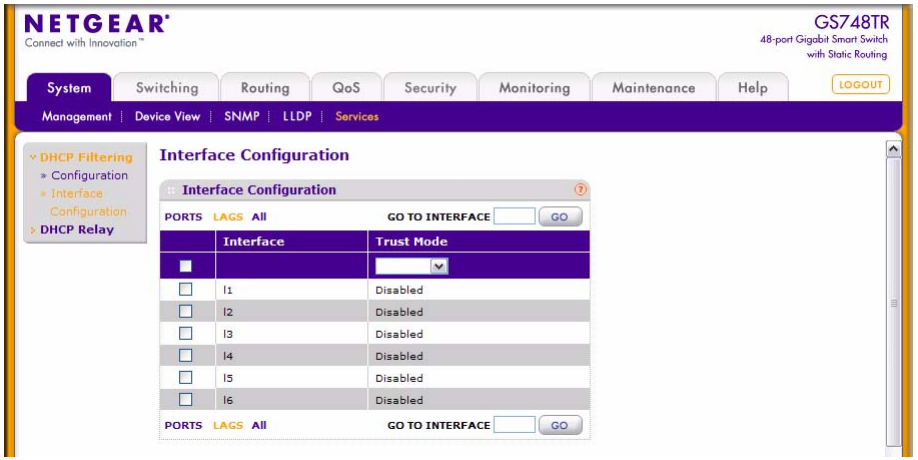


Figure 2-28

4. To display a list of both physical ports and logical interfaces, click **ALL**.
5. To go to an interface in the list that you want to do modifications to, type the interface number in the **Go To Interface** field and click **Go**, as shown in Figure 2-29.

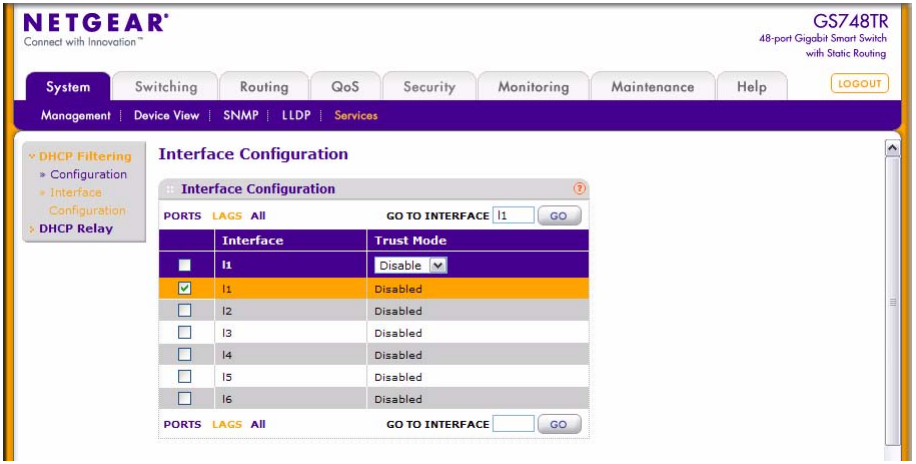


Figure 2-29

Table 2-27. DHCP Filtering Interface Configuration Fields

Field	Description
Interface	Selects the interface for which data is to be displayed or configured.
Trust Mode	Enables or disables DHCP Filtering on the selected interface. • **Enable:** Any DHCP responses received on this port are forwarded. • **Disable:** Any DHCP (or BootP) responses received on this port are discarded.

6. Click **Refresh** to refresh the page with the most current data from the switch.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
8. If you make any changes to the page, click **Apply** to apply the change to the system.

DHCP Relay

BootP/DHCP Relay enables BootP/DHCP clients and servers to exchange BootP/DHCP messages across different subnets. The relay agent receives the requests from the clients, and checks the valid hops and giaddr fields. If the number of hops is greater than the configured, the agent assumes the packet is looped through the agents and discards the packet. If giaddr field is zero the agent must fill in this field with the IP address of the interface on which the request was received. The agent unicasts the valid packets to the next configured destination. The server responds with a unicast BOOTREPLY addressed to the relay agent closest to the client as indicated by giaddr field. Upon reception of the BOOTREPLY from the server, the agent forwards this reply as broadcast or unicast on the interface form where the BOOTREQUEST was arrived. This interface can be identified by giaddr field.

GS700TR Smart Switch also supports DHCP relay agent options to identify the source circuit when customers are connected to the Internet with high-speed modem. The relay agent inserts these options when forwarding the request to the server and removes them when sending the reply to the clients.

If an interface has more than one IP address, the relay agent should use the primary IP address configured as its relay agent IP address.

The BOOTP/DHCP Relay Agent folder contains links to the following web pages that configure and display BOOTP/DHCP relay agent:

- “BOOTP/DHCP Relay Configuration” on page 2-45

• "BOOTP/DHCP Status" on page 2-46

BOOTP/DHCP Relay Configuration

Use the BOOTP/DHCP Relay page to configure and display a BOOTP/DHCP relay agent.

To display the page:

1. Click **System > Services > DHCP Relay** in the navigation tree.

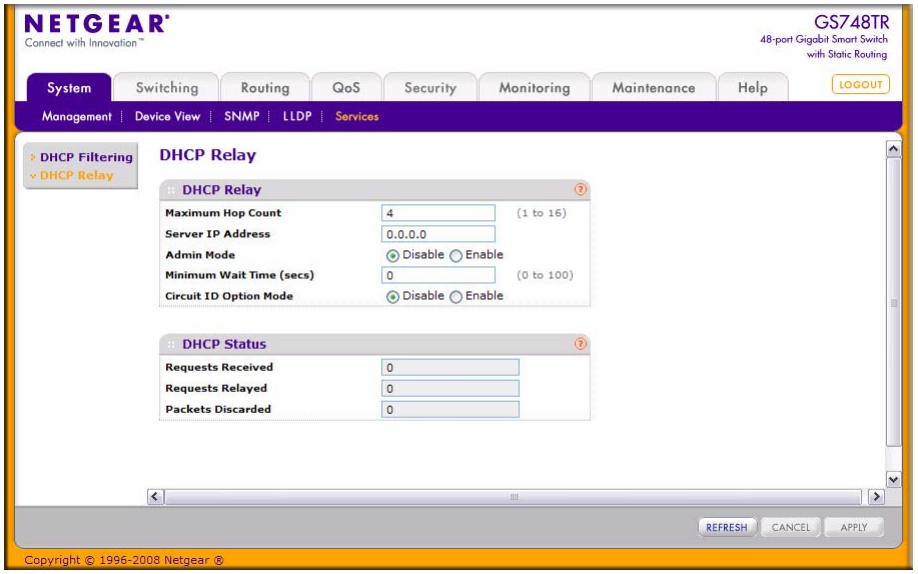


Figure 2-30

Table 2-28. BOOTP/DHCP Relay Agent Configuration Fields

Field	Description
Maximum Hop Count	Enter the maximum number of hops a client request can take before being discarded.
Server IP Address	Enter either the IP address of the BOOTP/DHCP server or the IP address of the next BOOTP/DHCP Relay Agent.
Admin Mode	Select Enable or Disable. When you select Enable, BOOTP/DHCP requests are forwarded to the IP address you entered in the Server IP address field.

Table 2-28. BOOTP/DHCP Relay Agent Configuration Fields (continued)

Field	Description
Minimum Wait Time (secs)	Enter a time in seconds. This value is compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets are only forwarded when the time stamp exceeds the minimum wait time.
Circuit ID Option Mode	Select Enable or Disable from the dropdown menu. If you select Enable, the relay agent adds Option 82 header packets to the DHCP Request packets before forwarding them to the server, and strips them off while forwarding the responses to the client.

2. If you make any changes to the page, click **Apply** to apply the changes to the system.

BOOTP/DHCP Status

Use the BOOTP/DHCP Status page to display the BOOTP/DHCP Relay status information.

To display the page, click **System > Services > DHCP Relay** in the navigation tree.

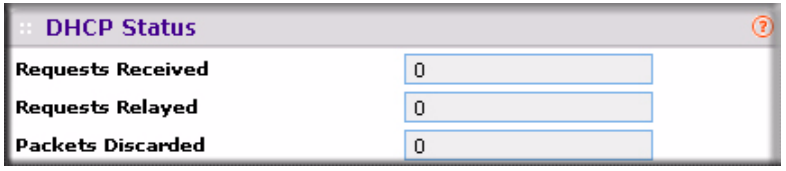


Figure 2-31

Table 2-29. BOOTP/DHCP Relay Status Fields

Field	Description
Requests Received	The total number of BOOTP/DHCP requests received from all clients since the last time the switch was reset.
Requests Relayed	The total number of BOOTP/DHCP requests forwarded to the server since the last time the switch was reset.
Packets Discarded	The total number of BOOTP/DHCP packets discarded by this Relay Agent since the last time the switch was reset.

Chapter 3
Configuring Switching Information

Configuring and Viewing Device Port Information

The pages on the Ports tab allows you to view and monitor the physical port information for the ports available on the switch. The Ports folder has links to the following features:

Port Configuration

Use the Port Configuration page to configure the physical interfaces on the switch.

To access the Port Configuration page:

1. Click **Switching > Ports > Port Configuration** in the navigation tree.

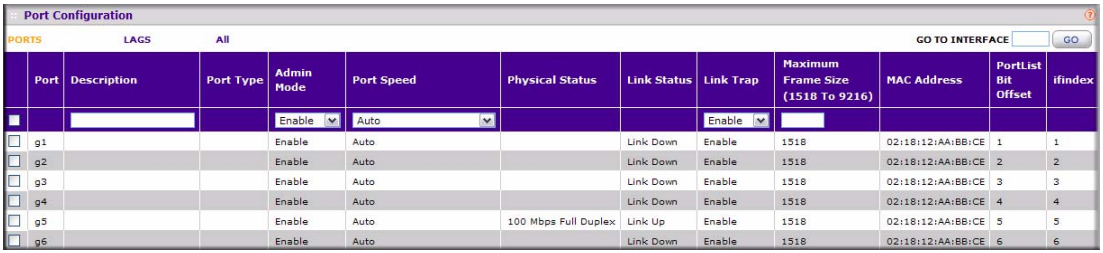


Figure 3-1

Table 3-1. Port Configuration Fields

Field	Description
Port	Select the port from the menu to display or configure data for that port. If you select **All**, the changes you make to the **Port Configuration** page apply to all physical ports on the system.
Description	Enter the description string to be attached to a port. The string can be up to 64 characters in length.
Port Type	For most ports this field is blank. Otherwise the possible values are: • **MON:** Indicates that the port is a monitoring port. For more information about port monitoring see Chapter 7, “Monitoring the System”. • **LAG:** Indicates that the port is a member of a Link Aggregation trunk. For more information see “LAG Membership” on page 3-6.
Admin Mode	Use the menu to select the port control administration state, which can be one of the following: • **Enable:** The port can participate in the network (default). • **Disable:** The port is administratively down and does not participate in the network.
Port Speed	Use the menu to select the port’s speed and duplex mode. If you select **Auto**, the duplex mode and speed will be set by the auto-negotiation process. Note that the port’s maximum capability (full duplex and 1000 Mbps) will be advertised. Otherwise, your selection will determine the port’s duplex mode and transmission rate. The factory default is **Auto**.
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the Link is up or down.

Table 3-1. Port Configuration Fields (continued)

Field	Description
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled: • **Enable:** Specifies that the system sends a trap when the link status changes. • **Disable:** Specifies that the system does not send a trap when the link status changes.
Maximum Frame Size	Indicates the maximum Ethernet frame size the interface supports or is configured to support. The frame size includes the Ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.
MAC Address	Displays the physical address of the specified interface.
PortList Bit Offset	Display the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.
ifIndex	The ifIndex of the interface table entry associated with this port. If the interface field is set to **All**, this field is blank.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any changes to the page, click **Apply** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Flow Control

IEEE 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss. When 802.3x flow control is enabled, lower speed switches can communicate with higher speed switches by requesting that the higher speed switch refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

To display the Flow Control page:

1. Click **Switching > Ports**, and then click the **Flow Control** link.

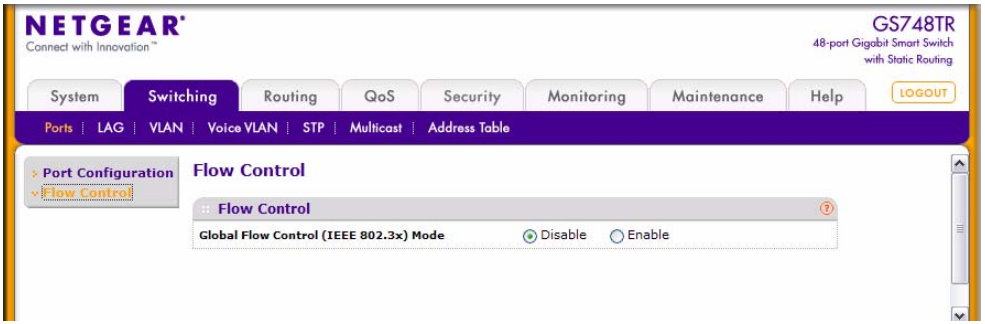


Figure 3-2

Table 3-2. Switch Configuration Fields

Field	Description
Global Flow Control (IEEE 802.3x) Mode	Enables or disables IEEE 802.3x flow control on the system. The factory default is disabled. • Select **Enable** so that the switch can communicate with higher speed switches. • Select **Disable** so that the switch does not send pause packets if the port buffers become full.

2. If you change the mode, click **Apply** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Creating LAGs

Link aggregation groups (LAGs), which are also known as port-channels, allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. You assign the LAG VLAN membership after you create a LAG. The LAG by default becomes a member of the management VLAN.

A LAG interface can be either static or dynamic, but not both. All members of a LAG must participate in the same protocols. A static port-channel interface does not require a partner system to be able to aggregate its member ports.

Note: The GS700TR switches support a maximum of six LAGs.

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LAGPDUs.

The LAG folder contains links to the following features:

- "LAG Configuration" on page 3-5
- "LAG Membership" on page 3-6
- "LACP Configuration" on page 3-7
- "LACP Port Configuration" on page 3-8

LAG Configuration

Use the LAG (Port Channel) Configuration page to group one or more full duplex Ethernet links to be aggregated together to form a link aggregation group, which is also known as a port-channel. The switch treats the LAG as if it were a single link.

To access the LAG Configuration page:

1. Click **Switching > LAG > Basic > LAG Configuration** in the navigation tree.

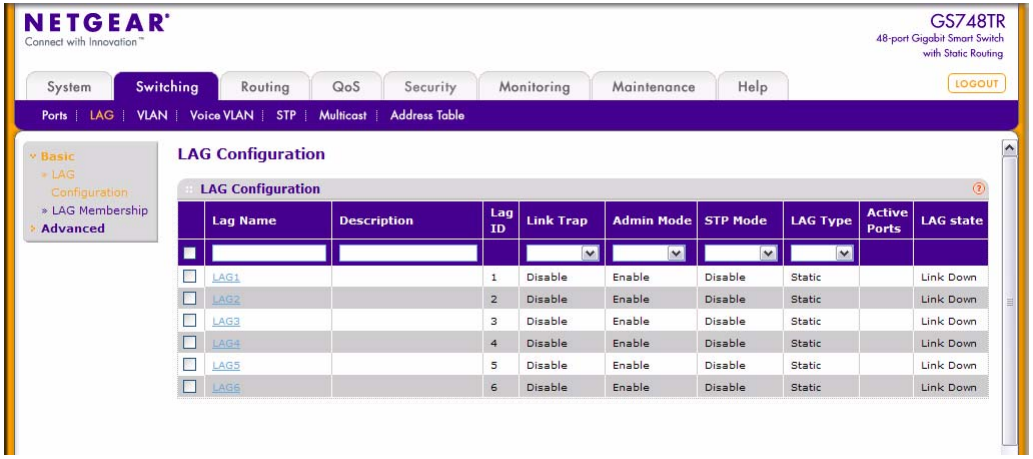


Figure 3-3

Table 3-3. LAG (Port Channel) Configuration Fields

Field	Description
LAG Name	Enter the name you want assigned to the LAG. You may enter any string of up to 15 alphanumeric characters. A valid name has to be specified in order to create the LAG
Description	Enter the Description string to be attached to a LAG. It can be up to 64 characters in length.
LAG ID	Identification of the LAG
Link Trap	Specify whether you want to have a trap sent when link status changes. The factory default is **Enable**, which will cause the trap to be sent.
Admin Mode	Select **Enable** or **Disable** from the menu. When the LAG (port channel) is disabled, no traffic will flow and LAGPDUs will be dropped, but the links that form the LAG (port channel) will not be released. The factory default is **Enable**.
STP Mode	The Spanning Tree Protocol Administrative Mode associated with the LAG. Possible values are **Enable** or **Disable**.
LAG Type	Select **Static** or **LACP**. When the LAG is enabled, it does not transmit or process received LAGPDUs, i.e. the member ports do not transmit LAGPDUs and all the LAGPDUs it may receive are dropped. The default is **Static**.
Active Ports	A listing of the ports that are actively participating members of this Port Channel. A maximum of 8 ports can be assigned to a port channel.
LAG State	Indicates whether the link is Up or Down.

2. Click **Add** to update the switch with the values on this screen. If you want the switch to retain the new values across a power cycle, you must perform a **Save**.
3. To remove a configured LAG (port channel), select it and click **Delete**. All ports that were members of this LAG are removed from the LAG and included in the default VLAN.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

LAG Membership

Use the LAG Membership page to group one or more full duplex Ethernet links to be aggregated together to form a link aggregation group (LAG), which is also known as a port-channel. The switch can treat the port-channel as if it were a single link.

To access the LAG Membership page:

1. Click **Switching** > **LAG** > **Basic** > **LAG Membership** in the navigation tree.

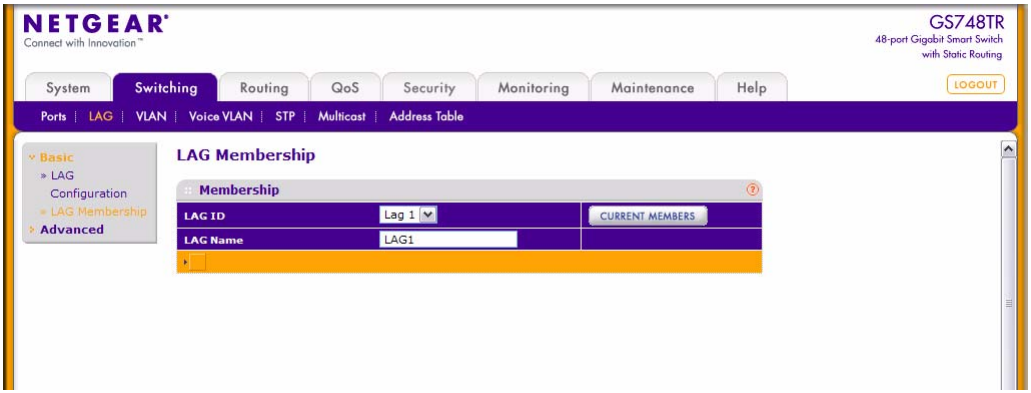


Figure 3-4

Table 3-4. LAG Membership Fields

Field	Description
LAG ID	Identifies the LAG (port channel) with the interface naming convention.
LAG Name	Enter the name you want assigned to the LAG. You may enter any string of up to 15 alphanumeric characters. A valid name has to be specified in order to create the LAG.
Port Selection Table	Select the ports as members of this LAG.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

LACP Configuration

To display the LACP Configuration page:

1. Click **Switching** > **LAG** > **Advanced** > **LACP Configuration** in the navigation tree.

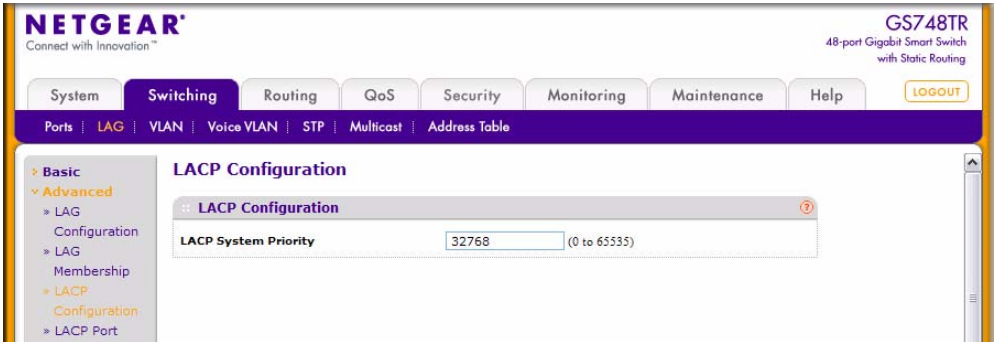


Figure 3-5

Table 3-5. LACP Configuration Fields

Field	Description
LACP System Priority	Specifies the device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. A higher value indicates a lower priority. You can change the value of the parameter globally by specifying a priority from 0 to 65535. The default value is 32768.

2. Click **Refresh** to reload the page and display the most current information.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

LACP Port Configuration

To display the LACP Port Configuration page:

1. Click **Switching > LAG > Advanced > LACP Port Configuration** in the navigation tree.

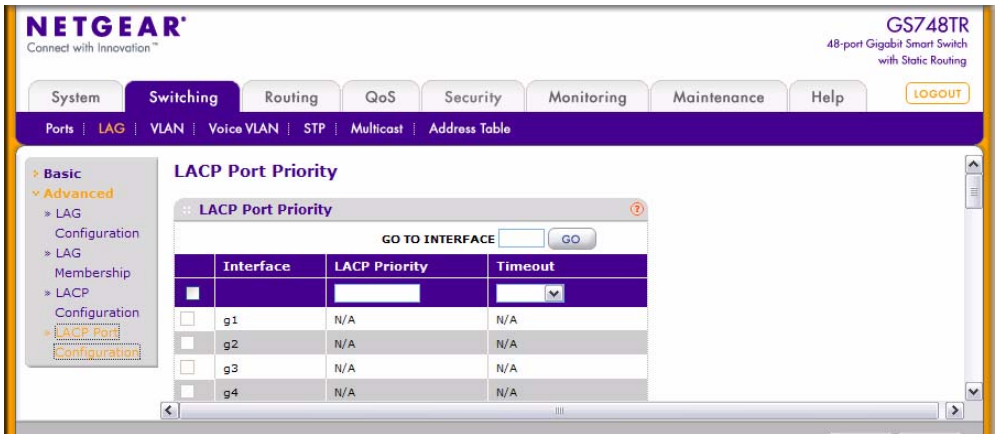


Figure 3-6

Table 3-6. LACP Port Configuration Fields

Field	Description
Interface	Select the interface for which data is to be displayed or configured.
LACP Priority	Specifies port priority value. The field range is 0 to 255. The default value is 128.
Timeout	Displays the administrative LACP timeout. The possible values are: • **Long**. Specifies a long timeout value. • **Short**. Specifies a short timeout value.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Managing VLANs

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You may have many reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

The VLAN folder contains links to the following features:

- "VLAN Configuration" on page 3-10
- "Configuring Spanning Tree Protocol" on page 3-18
- "Port VLAN ID Configuration" on page 3-13

VLAN Configuration

Use the VLAN Configuration page to define VLAN groups stored in the VLAN membership table. Your switch supports up to 255 VLANs. VLAN 1 is the default VLAN of which all ports are members.

To display the VLAN Configuration page:

1. Click **Switching > VLAN > Basic > VLAN Configuration** in the navigation tree.

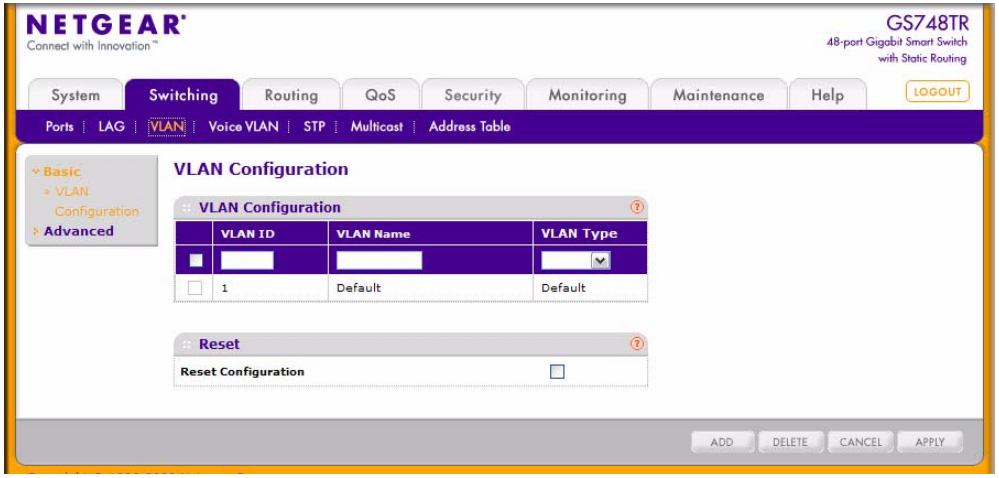


Figure 3-7

Table 3-7. VLAN Configuration Fields

Field	Description
VLAN ID	Specify the VLAN Identifier for the new VLAN. (You can only enter data in this field when you are creating a new VLAN.) The range of the VLAN ID is (1 to 4078).
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 is always named “Default.”
VLAN Type	This field identifies the type of the VLAN you are configuring. You cannot change the type of the default VLAN (VLAN ID = 1): it is always type “Default.” When you create a VLAN, using this screen, its type will always be “Static.” A VLAN that is created by GVRP registration initially has a type of “Dynamic.” You can use this menu to change its type to “Static.”

2. Click **Add** to add a new VLAN to the switch.
3. Click **Delete** to delete a selected VLAN from the switch.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

VLAN Membership Configuration

Use this page to configure VLAN Port Membership for a particular VLAN. You can select the Group operation through this page. Click the **Unit 1** link to see the ports to be configured.

To display the VLAN Membership Configuration page:

1. Click **Switching > VLAN > Advanced > VLAN Membership** in the navigation tree.

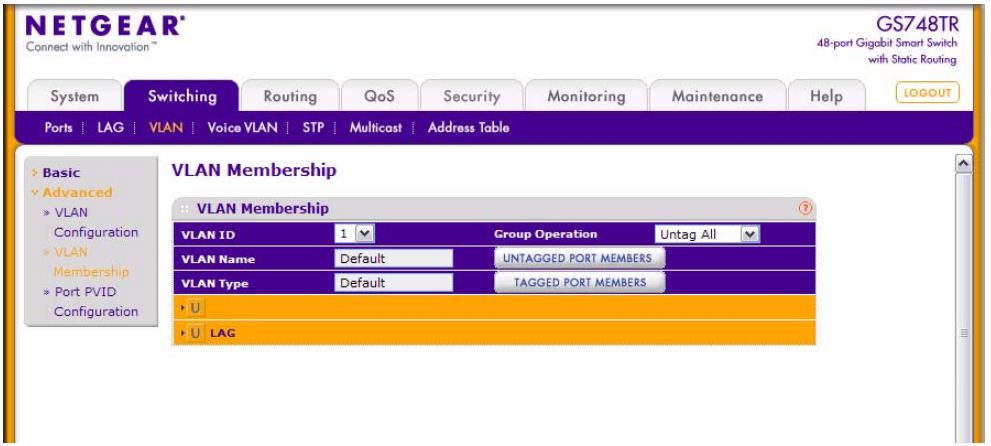


Figure 3-8

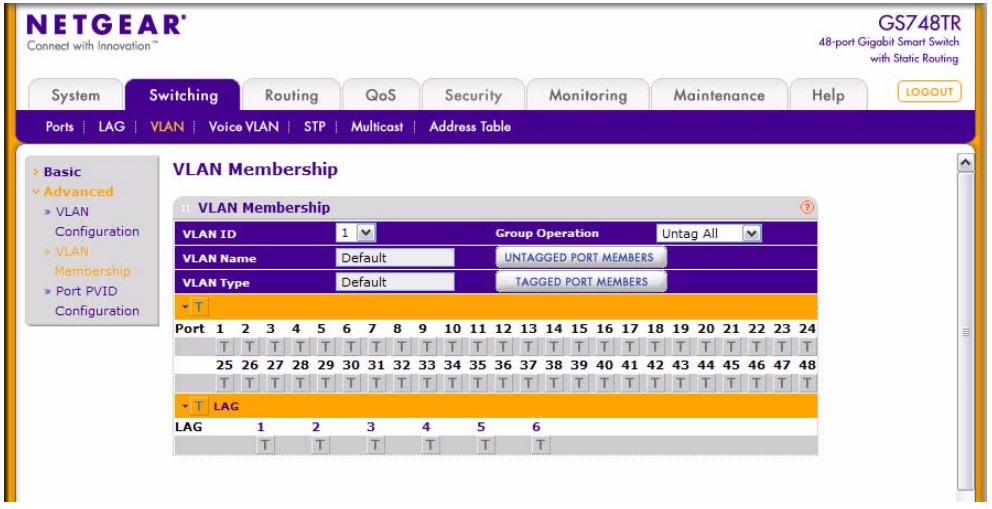


Figure 3-9

Table 3-8. VLAN Membership Configuration Fields

Field	Description
VLAN ID	Select the VLAN Identifier for which you want to display or configure data.
Group Operation	Use this field to select all the ports and configure them. Possible values are: • **Untag All**: Select all the ports on which all frames transmitted from this VLAN will be untagged. All the ports will be included in the VLAN. • **Tag All**: Select the ports on which all frames transmitted for this VLAN will be tagged. All the ports will be included in the VLAN. • **Remove All**: This selection has the effect of excluding all ports from the selected VLAN.
VLAN Name	This field identifies the name for the VLAN you selected. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 is always named “Default.”
Untagged/Tagged Port Members	Click Untagged Port Members or Tagged Port Members to see the port list and use it to add the ports you selected to this VLAN. Each port has three modes: • **Tagged:** Select the ports on which all frames transmitted for this VLAN will be tagged. The ports that are selected will be included in the VLAN. • **Untagged:** Select the ports on which all frames transmitted for this VLAN will be untagged. The ports that are selected will be included in the VLAN.
VLAN Type	This field identifies the type of the VLAN you selected. Possible values are: • **Default**: The default (VLAN ID = 1) is always present. • **Static**: A VLAN that you have configured using this screen.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

Port VLAN ID Configuration

Use the Port VLAN ID (PVID) Configuration page to configure a virtual LAN on a port.

To access the Port PVID Configuration page:

1. Click **Switching** > **VLAN** > **Advanced** > **Port PVID Configuration** in the navigation tree.

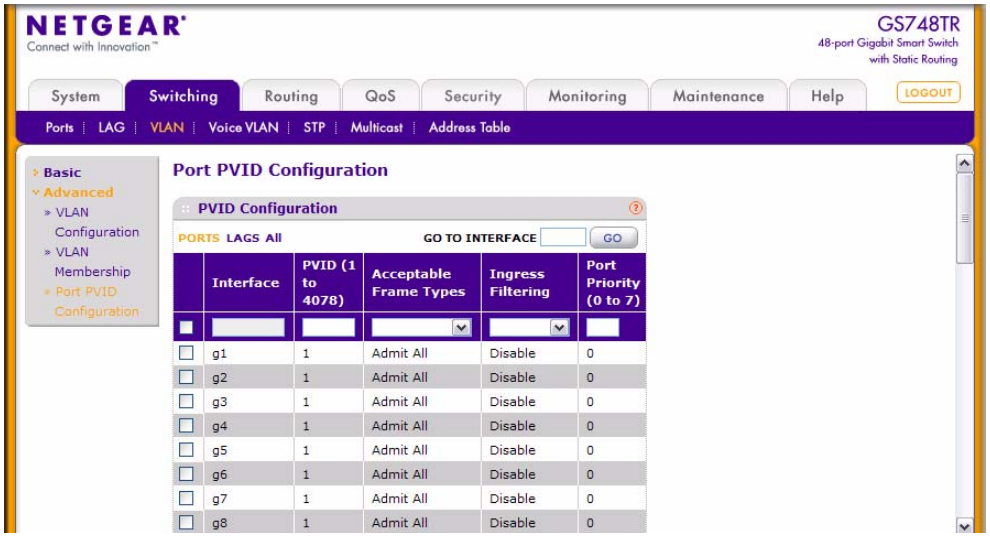


Figure 3-10

Table 3-9. Port VLAN ID Configuration Fields

Field	Description
Interface	Select the physical interface for which you want to display or configure data.
Port VLAN ID (PVID)	Specify the range of Port VLAN IDs you want assigned to untagged or priority tagged frames received on this port. The factory default is 1.
Acceptable Frame Types	Specify how you want the port to handle untagged and priority tagged frames. Whichever you select, VLAN tagged frames will be forwarded in accordance with the IEEE 802.1Q VLAN standard. The factory default is **Admit All**. • **VLAN Only:** The port will discard any untagged or priority tagged frames it receives. • **Admit All:** Untagged and priority tagged frames received on the port will be accepted and assigned the value of the Port VLAN ID for this port.

Table 3-9. Port VLAN ID Configuration Fields (continued)

Field	Description
Ingress Filtering	Specify how you want the port to handle tagged frames: • **Enable:** A tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. • **Disable:** All frames are forwarded in accordance with the IEEE 802.1Q VLAN standard. The factory default is **disable**.
Port Priority	Specify the default 802.1p priority assigned to untagged packets arriving at the port. Possible values are 0 to 7.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

Voice VLAN

Use this page to configure Voice VLAN. The Voice VLAN folder contains links to the following features:

- “Voice VLAN Properties” on page 3-15
- “Voice VLAN Port Setting” on page 3-16
- “Voice VLAN OUI” on page 3-17

Voice VLAN Properties

To display the Voice VLAN Properties page:

1. Click **Switching** > **Voice VLAN** > **Basic** > **Properties** in the navigation tree.

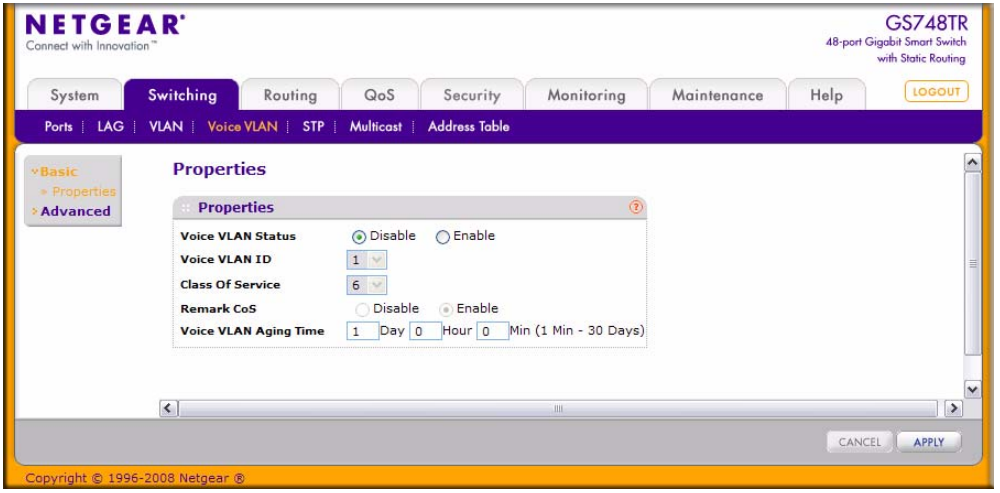


Figure 3-11

Table 3-10. Voice VLAN Properties Fields

Field	Description
Voice VLAN Status	Select to **Enable** or **Disable** Voice VLAN on the switch. The default is **Disable**.
Voice VLAN ID	Set the Voice VLAN Identifier to be used for voice traffic for the switch.
Class of Service	Set the CoS tag value to be reassigned for packets received on the Voice VLAN when Remark CoS is enabled.
Remark CoS	Select **Enable** or **Disable** reassigning the CoS tag value to packets received on the Voice VLAN.
Voice VLAN Aging TIme	Enter the amount of time after the last IP phone's OUI is aged out for a specific port. The port will age out after the bridge and voice aging time. The default time is 1 day.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. If you want the switch to retain the new values across a power cycle, you must perform a Save.

Voice VLAN Port Setting

To display the Voice VLAN Port Setting page:

1. Click **Switching** > **Voice VLAN** > **Advanced** > **Port Setting** in the navigation tree.

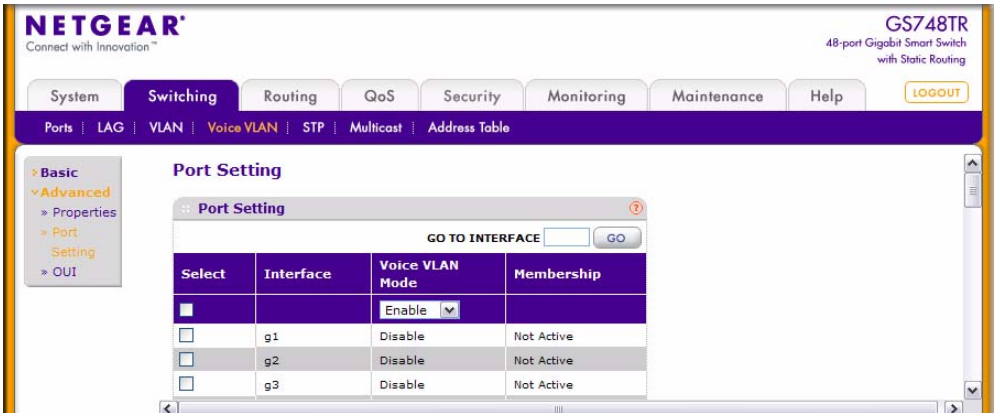


Figure 3-12

Table 3-11. Voice VLAN Port Setting Fields

Field	Description
Interface	Select the interface for which data is to be displayed or configured.
Voice VLAN Mode	Select to **Enable** or **Disable** Voice VLAN on the selected interface. The default is **Enable**.
Membership	Displays the current operational status of the Voice VLAN on the interface.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. If you want the switch to retain the new values across a power cycle, you must perform a Save.

Voice VLAN OUI

To display the Voice VLAN OUI page:

1. Click **Switching** > **Voice VLAN** > **Advanced** > **OUI** in the navigation tree.

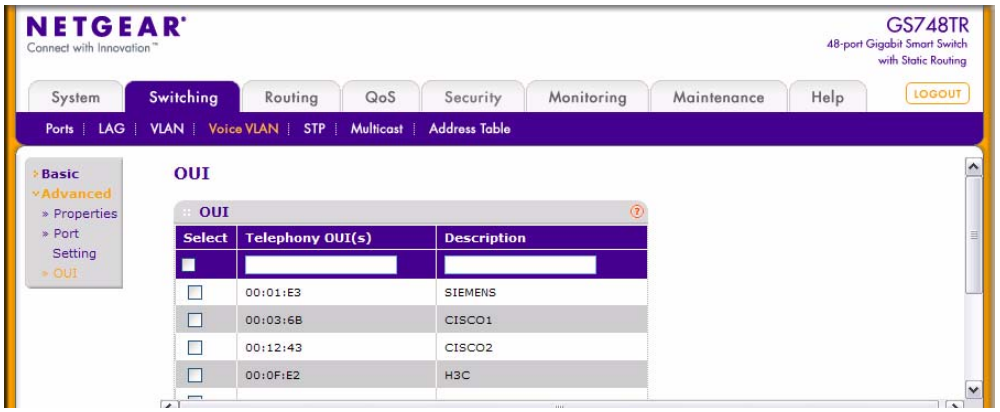


Figure 3-13

Table 3-12. Voice VLAN OUI Fields

Field	Description
Telephony OUI(s)	VOIP OUI prefix to be added in the format AA:BB:CC.
Description	Enter the description for the OUI.

2. Click **Add** to add a new Telephony OUI entry.
3. Click **Delete** to delete the selected entry.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. If you want the switch to retain the new values across a power cycle, you must perform a Save.
6. Click **Restore Defaults** to restore the default OUI's.

Configuring Spanning Tree Protocol

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops. Spanning tree versions supported include Common STP, Multiple STP, and Rapid STP.

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information on configuring Common STP, see "CST Port Configuration" on page 3-23.

Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (chief among the effects, is the rapid transitioning of the port to 'Forwarding'). The difference between the RSTP and the traditional STP (IEEE 802.1d) is the ability to configure and recognize full duplex connectivity and ports which are connected to end stations, resulting in rapid transitioning of the port to 'Forwarding' state and the suppression of Topology Change Notification. These features are represented by the parameters 'pointtopoint' and 'edgeport'. MSTP is compatible to both RSTP and STP. It behaves appropriately to STP and RSTP bridges. A MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge.

Note: For two bridges to be in the same region, the force version should be 802.1s and their configuration name, digest key, and revision level should match. For more information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

The Spanning Tree folder contains links to the following features:

STP Switch Configuration/Status

The Spanning Tree Switch Configuration/Status page contains fields for enabling STP on the switch.

To display the Spanning Tree Switch Configuration/Status page:

1. Click **Switching** > **STP** > **Basic > STP Configuration** in the navigation tree.

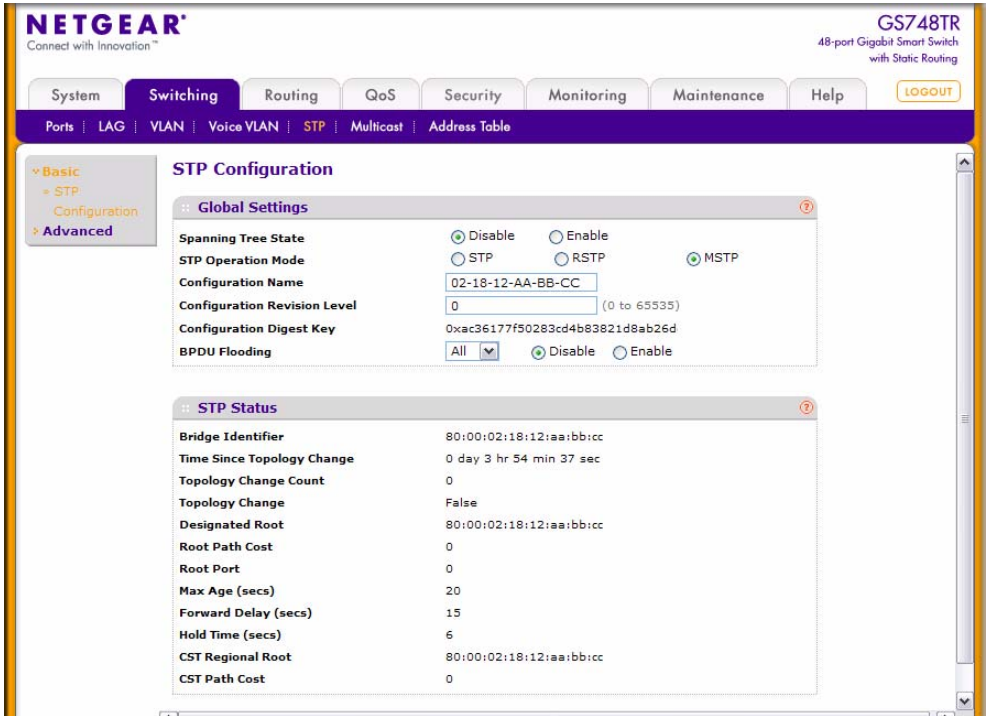


Figure 3-14

Table 3-13. Spanning Tree Switch Configuration/Status Fields

Field	Description
Spanning Tree State	Enables or disables Spanning Tree operation on the switch.
STP Operation Mode	Specifies the Force Protocol Version parameter for the switch. Options are: • **STP** (Spanning Tree Protocol): IEEE 802.1d • **RSTP** (Rapid Spanning Tree Protocol): IEEE 802.1w • **MSTP** (Multiple Spanning Tree Protocol): IEEE 802.1s
Configuration Name	Name used to identify the configuration currently being used. It may be up to 32 alphanumeric characters.
Configuration Revision Level	Number used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0.
Configuration Digest Key	Number used to identify the configuration currently being used.

Table 3-13. Spanning Tree Switch Configuration/Status Fields (continued)

Field	Description
BPDU Flooding	Enables or disables BPDU Flooding. When this feature is enabled, BPDU packets arriving at this port are flooded to other ports if STP is disabled.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time in seconds since the topology of the CST last changed.
Topology Change Count	The number of times the topology has changed for the CST.
Topology Change	The value of the topology change parameter for the switch indicating if a topology change is in progress on any port assigned to the CST. The value is either **True** or **False**.
Designated Root	The bridge identifier of the root bridge. Is made up from the bridge priority and the base MAC address of the bridge.
Root PathCost	Path Cost to the Designated Root for the CST.
Root Port	Port to access the Designated Root for the CST.
Max Age (secs)	Path Cost to the Designated Root for the CST.
Forward Delay (secs)	Derived value of the Root Port Bridge Forward Delay parameter.
Hold TIme (secs)	Minimum time between transmission of Configuration BPDUs.
CST Regional Root	Priority and base MAC address of the CST Regional Root.
CST Path Cost	Path Cost to the CST tree Regional Root.

2. Click **Refresh** to update the information on the screen with the most current data.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch
4. If you make any configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

CST Configuration

Use the Spanning Tree CST Configuration page to configure Common Spanning Tree (CST) and Internal Spanning Tree on the switch.

To display the Spanning Tree CST Configuration page:

1. Click **Switching** > **STP** > **Advanced > CST Configuration** in the navigation tree.

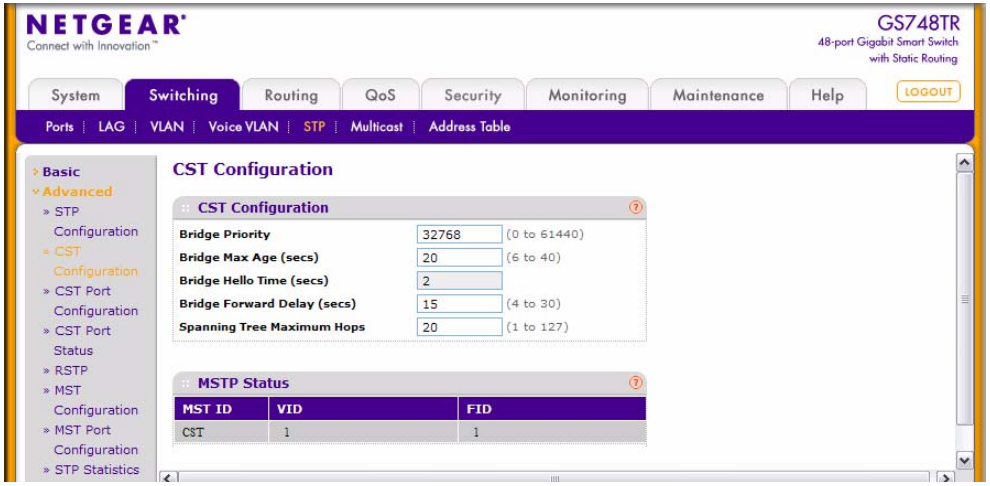


Figure 3-15

Table 3-14. Spanning Tree CST Configuration/Status Fields

Field	Description
Bridge Priority	When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. Specifies the bridge priority value for the Common and Internal Spanning Tree (CST). The valid range is 0-61440. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. The default priority is 32768.
Bridge Max Age (secs)	Specifies the bridge maximum age time for the Common and Internal Spanning Tree (CST), which indicates the amount of time in seconds a bridge waits before implementing a topological change. The valid range is 6-40, and the value must be less than or equal to (2 * Bridge Forward Delay) – 1 and greater than or equal to 2 * (Bridge Hello Time +1). The default value is 20.
Bridge Hello Time (secs)	Specifies the switch Hello time for the Common and Internal Spanning Tree (CST), which indicates the amount of time in seconds a root bridge waits between configuration messages. The valid range is 1-10, and the default value is 2. The value must be less than or equal to (Bridge Max Age / 2) – 1.

Table 3-14. Spanning Tree CST Configuration/Status Fields (continued)

Field	Description
Bridge Forward Delay (secs)	Specifies the switch forward delay time, which indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The value must be greater or equal to (Bridge Max Age / 2) + 1. The time range is from 4 seconds to 30 seconds. The default value is 15.
Spanning Tree Maximum Hops	Specifies the maximum number of bridge hops the information for a particular CST instance can travel before being discarded. The valid range is 1-127.

Displayed on the Spanning Tree CST Configuration page is the MSTP Status table.

Table 3-15. Spanning Tree MSTP Status Fields

Field	Description
MST ID	Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID	Table consisting of the VLAN IDs and the corresponding FID associated with each of them
FID	Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

2. Click **Refresh** to update the information on the screen with the most current data.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch
4. If you make any configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

CST Port Configuration

Use the Spanning Tree CST Port Configuration page to configure Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

To display the Spanning Tree CST Port Configuration page:

1. Click **Switching** > **STP** > **Advanced > CST Port Configuration** in the navigation tree.

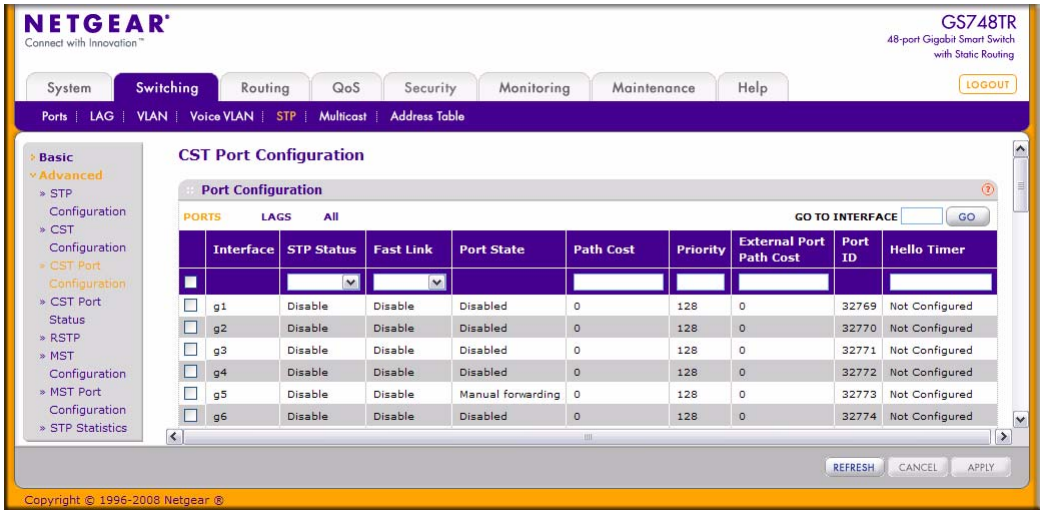


Figure 3-16

Table 3-16. Spanning Tree CST Port Configuration/Status Fields

Field	Description
Interface	Select one of the physical or port channel interfaces associated with the VLAN(s) associated with the CST.
STP Status	Spanning Tree Protocol Administrative Mode associated with the port or port channel. Possible values are **Enable** or **Disable**.
Fast Link	Specifies if the specified port is an Edge Port with the CST. Possible values are **Enable** or **Disable**. The default is **Disable**.
Port State	The Forwarding state of this port.
Path Cost	Set the Path Cost to a new value for the specified port in the common and internal spanning tree. It takes a value in the range of 1 to 200000000.
Priority	The priority for a particular port within the CST. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the priority is automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16.
External Port Path Cost	Set the External Path Cost to a new value for the specified port in the spanning tree. It takes a value in the range of 1 to 200000000.

Table 3-16. Spanning Tree CST Port Configuration/Status Fields (continued)

Field	Description
Port ID	The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
Hello Timer	Specifies the switch Hello time, which indicates the amount of time in seconds a port waits between configuration messages. The valid range is 1-10, and the default value is 2. The value must be less than or equal to (Bridge Max Age / 2) – 1. The default hello time value is 2.

2. Click **Refresh** to update the information on the screen with the most current data.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you make any configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

CST Port Status

Use the Spanning Tree CST Port Status page to display Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

To display the Spanning Tree CST Port Status page:

1. Click **Switching** > **STP** > **Advanced** > **CST Port Status** in the navigation tree.
2.

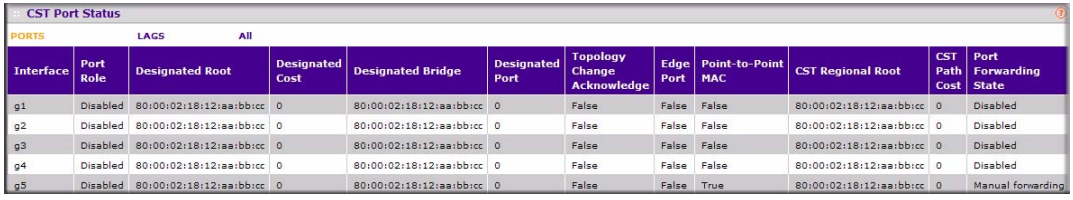


Figure 3-17

Table 3-17. Spanning Tree CST Port Status Fields

Field	Description
Interface	Select a physical or port channel interface to configure. The port is associated with the VLAN(s) associated with the CST.
Port Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: **Root Port, Designated Port**, **Alternate Port, Backup Port**, **Master Port** or **Disabled Port**.
Designated Root	Root Bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Topology Change Acknowledge	Identifies whether the next BPDU to be transmitted for this port would have the topology change acknowledgement flag set. It is either “True” or “False”.
Edge Port	Indicates whether the port is enabled as an edge port. Possible values are **Enabled** or **Disabled**.
Point-to-point MAC	Derived value of the point-to-point status.
CST Regional Root	Shows the bridge priority and base MAC address of the CST Regional Root.
CST Path Cost	Shows the path Cost to the CST tree Regional Root.
Port Forwarding State	Displays the Forwarding State of this port.

3. Click **Refresh** to update the information on the screen with the most current data.

Rapid STP Configuration

Use the Rapid Spanning Tree Configuration page to configure Rapid Spanning Tree (RSTP) on the switch.

To display the Rapid STP Configuration page:

1. Click **Switching** > **STP** > **Advanced** > **RSTP** in the navigation tree.

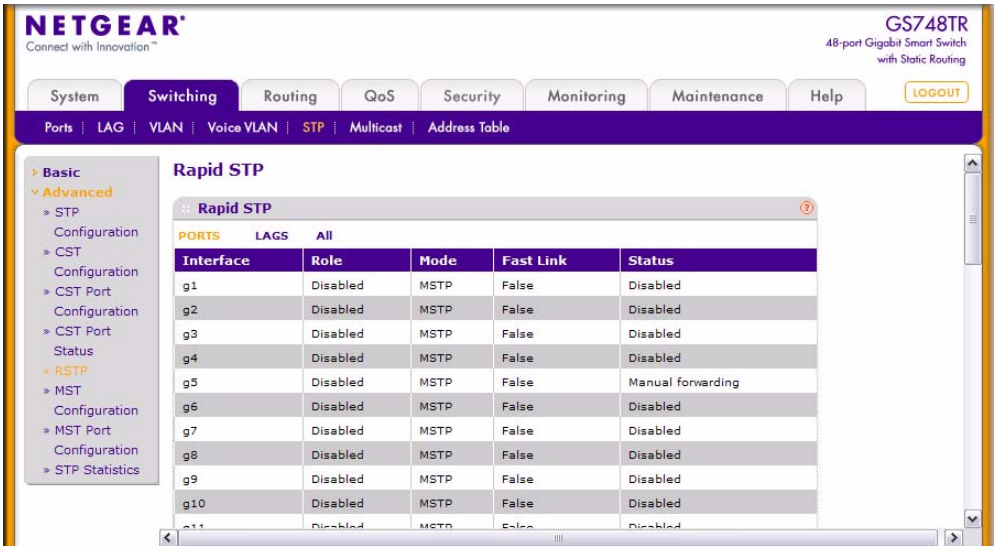


Figure 3-18

Table 3-18. Rapid STP

Field	Description
Interface	The physical or port channel interfaces associated with VLANs associated with the CST.
Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
Mode	Specifies the spanning tree operation mode. Different modes are: **STP**, **RSTP**, **MSTP**.
Fast Link	Indicates whether the port is enabled as an edge port.
Status	The Forwarding State of this port.

2. Click **Refresh** to update the information on the screen with the most current data.

MST Configuration

Use the Spanning Tree MST Configuration page to configure Multiple Spanning Tree (MST) on the switch.

To display the Spanning Tree MST Configuration page:

1. Click **Switching** > **STP** > **Advanced** > **MST Configuration** in the navigation tree. Use this page to create and configure a new MST or select an existing MST to display or configure.

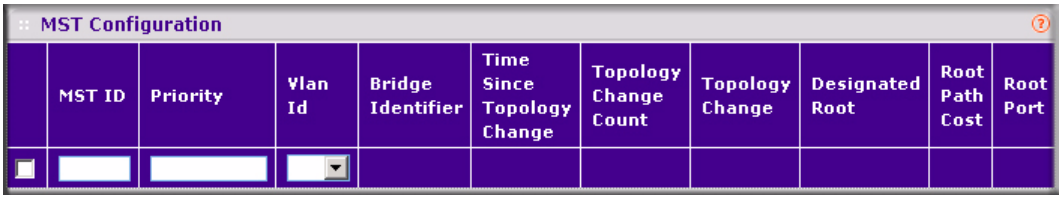


Figure 3-19

Table 3-19. Spanning Tree MST Configuration

Field	Description
MST ID	This is only visible when the select option of the MST ID select box is selected. The ID of the MST being created. Valid values for this are between 1 and 4094.
Priority	Specifies the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. The default priority is 32768.The valid range is 0-61440.
VLAN ID	This gives a list box of all VLANs on the switch. The VLANs associated with the MST instance which is selected are highlighted on the list. These can be selected or unselected for reconfiguring the association of VLANs to MST instances.
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Displays the total amount of time since the topology of the selected MST instance last changed. The time is displayed in hour/minute/second format, for example, 5 hours 10 minutes and 4 seconds.
Topology Change Count	Displays the total number of times topology has changed for the selected MST instance.
Topology Change	Indicates whether a topology change is in progress on any port assigned to the selected MST instance. The possible values are **True** or **False**.
Designated Root	Displays the bridge identifier of the root bridge, which is made up from the bridge priority and the base MAC address of the bridge.

Table 3-19. Spanning Tree MST Configuration (continued)

Field	Description
Root Path Cost	Displays the path cost to the Designated Root for this MST instance.
Root Port	Indicates the port to access the Designated Root for this MST instance.

2. Click **Add** to create a new MST which you have configured.
3. Click **Delete** to delete the selected MST instance. All VLANs associated with the instance are associated with the CST.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make any configuration changes, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

MST Port Configuration

Use the Spanning Tree MST Port Configuration page to display Multiple Spanning Tree (MST) on a specific port on the switch.

To display the Spanning Tree MST Port Status page:

1. Click **Switching > STP > Advanced > MST Port Configuration** in the navigation tree. The two figures below show the left and right portions of the web page.

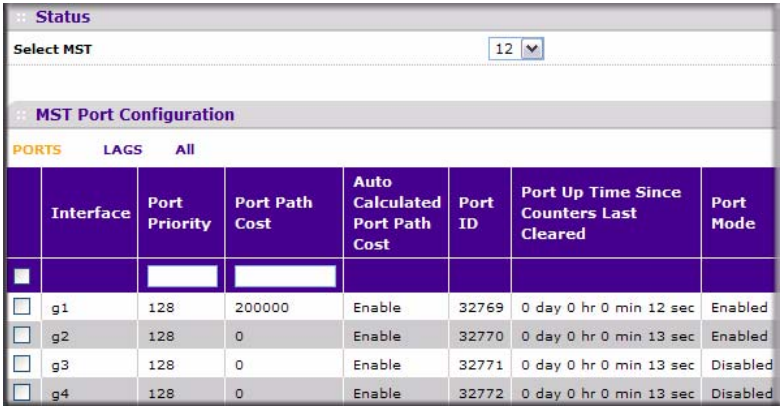
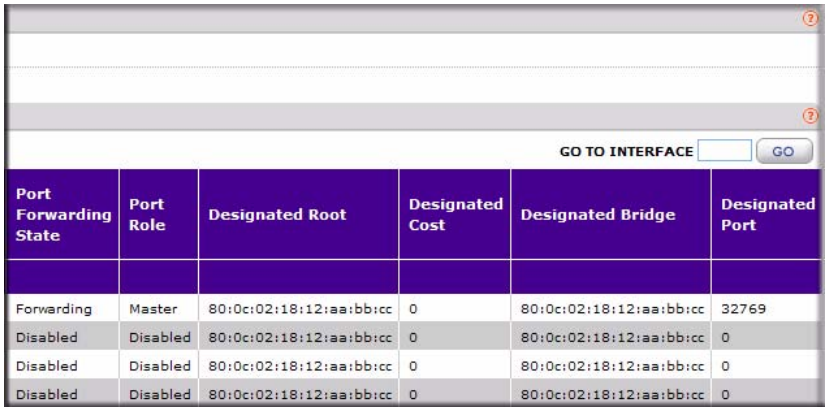


Figure 3-20



GO TO INTERFACE GO

Port Forwarding State	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port
Forwarding	Master	80:0c:02:18:12:aa:bb:cc	0	80:0c:02:18:12:aa:bb:cc	32769
Disabled	Disabled	80:0c:02:18:12:aa:bb:cc	0	80:0c:02:18:12:aa:bb:cc	0
Disabled	Disabled	80:0c:02:18:12:aa:bb:cc	0	80:0c:02:18:12:aa:bb:cc	0
Disabled	Disabled	80:0c:02:18:12:aa:bb:cc	0	80:0c:02:18:12:aa:bb:cc	0

Figure 3-21

Note: If no MST instances have been configured on the switch, the page displays a "No MSTs Available" message and does not display the fields shown in Table 3-20 on page 3-30.

Figure 3-22

Table 3-20. Spanning Tree MST Port Status Fields

Field	Description
Select MST	Select an existing MST instance from the pulldown list of MST IDs in the **Status** table at the top of the screen.
Interface	Select a physical or port channel interface to configure. The port is associated with the VLAN(s) associated with the selected MST instance.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the priority is automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16.

Table 3-20. Spanning Tree MST Port Status Fields (continued)

Field	Description
Port Path Cost	Set the Path Cost to a new value for the specified port in the selected MST instance. It takes a value in the range of 1 to 200000000.
Auto-calculated Port Path Cost	Displays whether the path cost is automatically calculated (**Enabled**) or not (**Disabled**). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
Port ID	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Up Time Since Counters Last Cleared	Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.
Port Mode	Spanning Tree Protocol Administrative Mode associated with the port or port channel. Possible values are **Enable** or **Disable**.
Port Forwarding State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are: • **Disabled:** STP is currently disabled on the port. The port forwards traffic while learning MAC addresses. • **Blocking:** The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. • **Listening:** The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses. • **Learning:** The port is currently in the learning mode. The port cannot forward traffic, however, it can learn new MAC addresses. • **Forwarding:** The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses
Port Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: **Root Port**, **Designated Port**, **Alternate Port**, **Backup Port**, **Master Port** or **Disabled Port**.
Designated Root	Root Bridge for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Refresh** to update the screen with the latest MST information.
4. If you make any configuration changes, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

STP Statistics

Use the Spanning Tree Statistics page to view information about the number and type of bridge protocol data units (BPDUs) transmitted and received on each port.

To display the Spanning Tree Statistics page:

1. Click **Switching > STP > Advanced > STP Statistics** in the navigation tree.

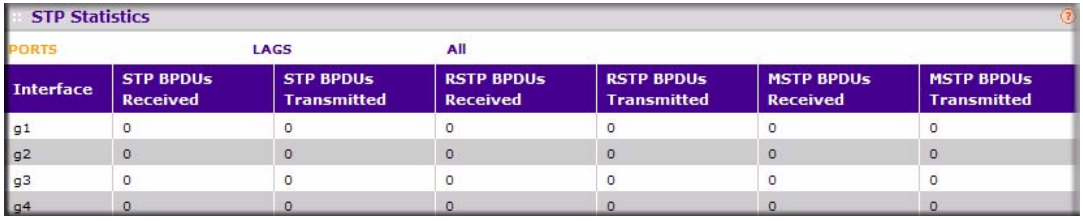


Figure 3-23

Table 3-21. Spanning Tree Statistics Fields

Field	Description
Interface	Select a physical or port channel interface to view its statistics.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.

2. Click **Refresh** to update the screen with the latest STP statistics information.

Configuring IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

A traditional Ethernet network may be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch will forward a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets will be flooded into network segments where no node has any interest in receiving the packet. While nodes will rarely incur any processing overhead to filter packets addressed to un-requested group addresses, they are unable to transmit new packets onto the shared media for the period of time that the multicast packet is flooded. The problem of wasting bandwidth is even worse when the LAN segment is not shared, for example in Full Duplex links.

Allowing switches to snoop IGMP packets is a creative effort to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments should receive packets directed to the group address.

The Multicast folder contains links to the following features:

- “Global Configuration” on page 3-33
- “IGMP Snooping Interface Configuration” on page 3-35

Global Configuration

Use the IGMP Snooping Configuration page to configure the parameters for IGMP snooping, which is used to build forwarding lists for multicast traffic.

To access the IGMP Snooping Configuration page:

1. Click **Switching** > **Multicast** > **IGMP Snooping** > **IGMP Snooping Configuration** in the navigation tree.

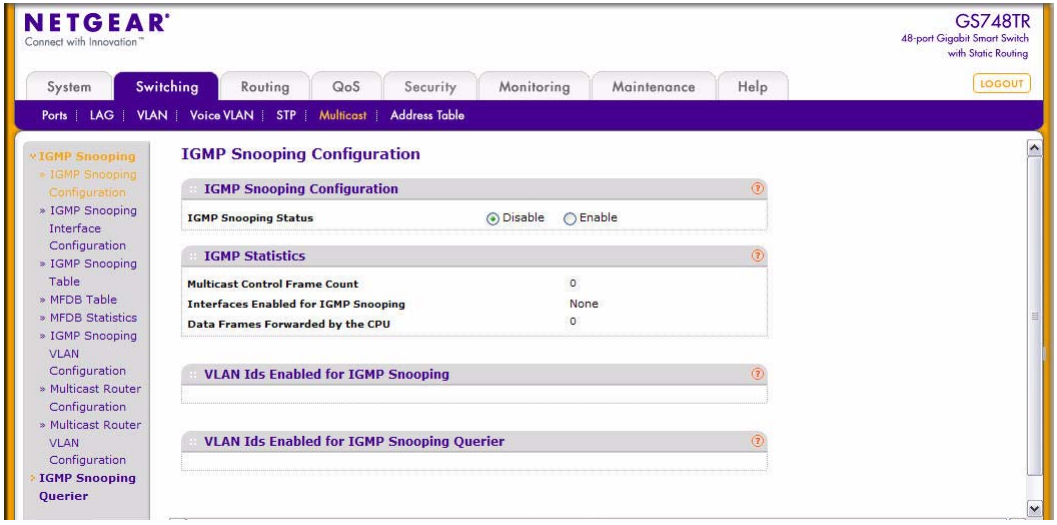


Figure 3-24

Table 3-22. IGMP Snooping Configuration Fields

Field	Description
IGMP Snooping Status	Select the administrative mode for IGMP Snooping for the switch. The default is **Disable**.
Multicast Control Frame Count	Shows the number of multicast control frames that have been processed by the CPU.
Interfaces Enabled for IGMP Snooping	Lists the interfaces currently enabled for IGMP Snooping. To enable interfaces for IGMP snooping, see “IGMP Snooping Interface Configuration” on page 3-35.
Data Frames Forwarded by the CPU	Shows the number of data frames forwarded by the CPU.
VLAN Ids Enabled For IGMP Snooping	Displays VLAN IDs enabled for IGMP snooping. To enable VLANs for IGMP snooping, see “IGMP Snooping VLAN Configuration” on page 3-40.
VLAN Ids Enabled For IGMP Snooping Querier	Displays VLAN IDs enabled for IGMP snooping querier.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any configuration changes, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

IGMP Snooping Interface Configuration

Use the IGMP Snooping Interface Configuration page to configure IGMP snooping settings on specific interfaces.

To access the IGMP Snooping Interface Configuration page:

1. Click **Switching > Multicast > IGMP Snooping > IGMP Snooping Interface Configuration** in the navigation tree.

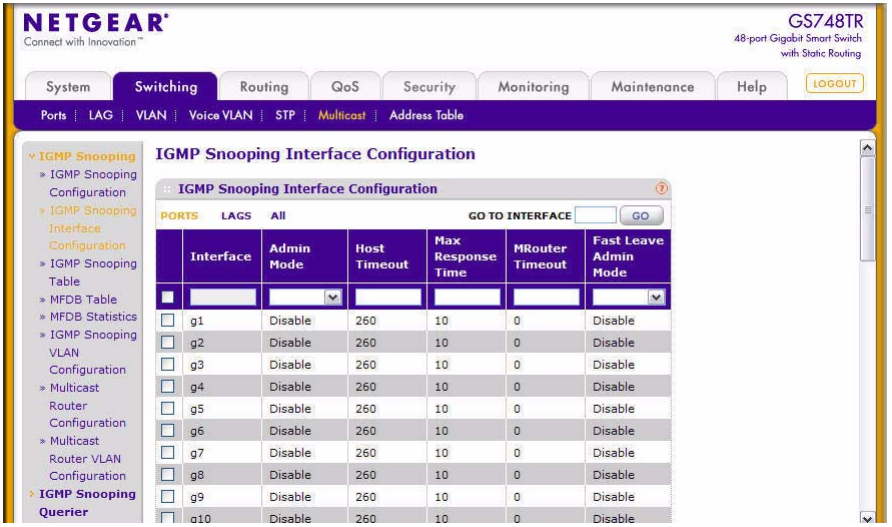


Figure 3-25

Table 3-23. IGMP Snooping Interface Configuration Fields

Field	Description
Interface	Lists all physical, VLAN, and LAG interfaces. Select the interface you want to configure.
Admin Mode	Select the interface mode for the selected interface for IGMP Snooping for the switch from the menu. The default is **Disable**.

Table 3-23. IGMP Snooping Interface Configuration Fields (continued)

Field	Description
Host TImeout	Specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group. Enter a value between 1 and 3600 seconds. The default is 260 seconds.
Max Response Time	Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds. The default is 10 seconds. The configured value must be less than the Group Membership Interval.
MRouter Timeout	Specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite timeout; i.e., no expiration.
Fast Leave Admin Mode	Select the Fast Leave mode for a particular interface from the menu. The default is **Disable**.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any configuration changes, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

Viewing Multicast Forwarding Database Information

The Layer 2 Multicast Forwarding Database (MFDB) is used by the switch to make forwarding decisions for packets that arrive with a multicast destination MAC address. By limiting multicasts to only certain ports in the switch, traffic is prevented from going to parts of the network where that traffic is unnecessary.

When a packet enters the switch, the destination MAC address is combined with the VLAN ID and a search is performed in the Layer 2 Multicast Forwarding Database. If no match is found, then the packet is either flooded to all ports in the VLAN or discarded, depending on the switch configuration. If a match is found, then the packet is forwarded only to the ports that are members of that multicast group.

The **Switching > Multicast** folder contains links to the following pages:

IGMP Snooping Table

Use the IGMP Snooping Table page to view all of the entries in the Multicast Forwarding Database that were created for IGMP snooping.

To access the IGMP Snooping Table page:

1. Click **Switching** > **Multicast** > **IGMP Snooping** > **IGMP Snooping Table** in the navigation tree.

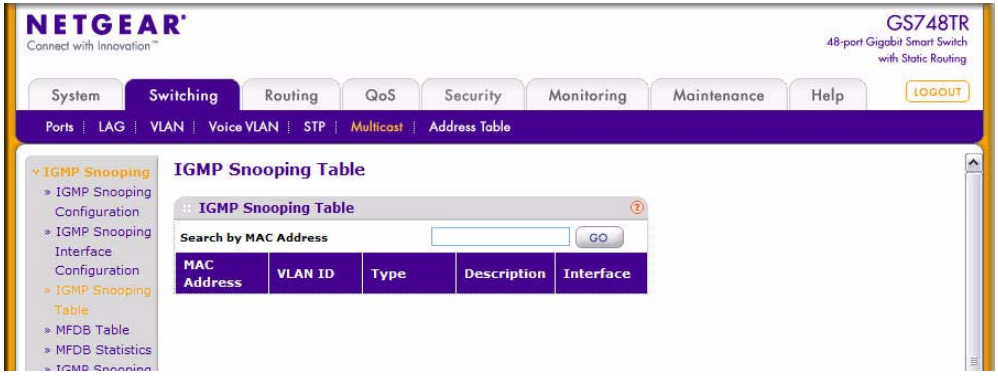


Figure 3-26

Table 3-24. MFDB IGMP Snooping Table Fields

Field	Description
MAC Address	A multicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example, 01:00:5e:45:67:89.
VLAN ID	A VLAN ID for which the switch has forwarding and or filtering information.

Table 3-24. MFDB IGMP Snooping Table Fields (continued)

Field	Description
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry. Possible values are **Management Configured**, **Network Configured** and **Network Assisted**.
Interface	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address.

2. Click **Clear** to clear one or all of the IGMP Snooping entries.
3. Click **Refresh** to reload the page and display the most current information.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

MFDB Table

Use the MFDB Table page to view the port membership information for all active multicast address entries. The key for an entry consists of a MAC address. Entries may contain data for more than one protocol.

To access the MFDB Table page:

1. Click **Switching** > **Multicast** > **IGMP Snooping** > **MFDB Table** in the navigation tree.
2.

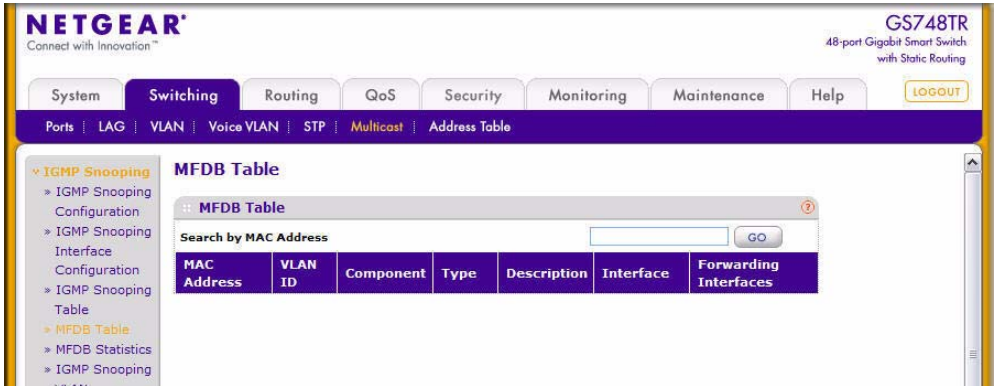


Figure 3-27

Table 3-25. MFDB Table Fields

Field	Description
MAC Address	The MAC Address to which the multicast MAC address is related. To search by MAC address, enter the address with the MFDB table entry you want displayed. Enter six two-digit hexadecimal numbers separated by colons, for example 00:0f:43:67:89:AB. Then click **Go**. If the address exists, that entry will be displayed. An exact match is required.
VLAN ID	The VLAN ID to which the multicast MAC address is related.
Component	This is the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are **IGMP Snooping** or **Static Filtering**.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry. Possible values are **Management Configured**, **Network Configured** and **Network Assisted**.
Interface	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the selected address.
Forwarding Interfaces	The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

3. Click **Refresh** to update the information on the screen with the most current data.

MFDB Statistics

Use the multicast forwarding database Statistics page to view statistical information about the MFDB table.

To access the Stats page:

1. Click **Switching** > **Multicast** > **IGMP Snooping** > **MFDB Statistics** in the navigation tree.

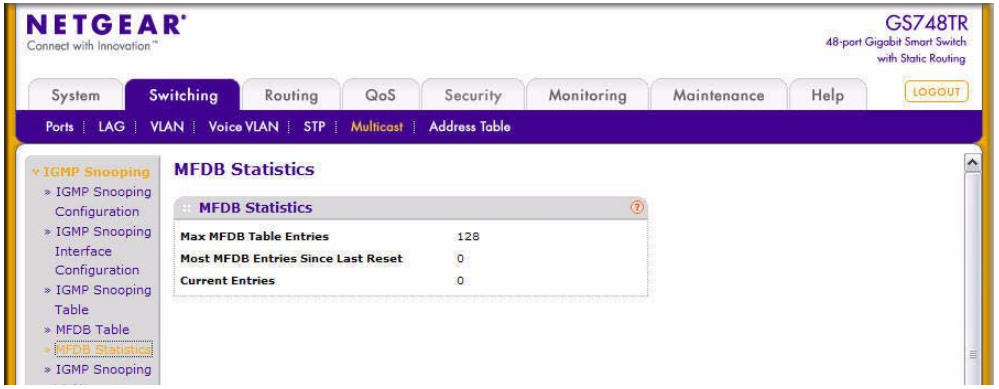


Figure 3-28

Table 3-26. Multicast Forwarding Database Statistics Fields

Field	Description
Max MFDB Table Entries	Shows the maximum number of entries that the Multicast Forwarding Database table can hold.
Most MFDB Entries Since Last Reset	The largest number of entries that have been present in the Multicast Forwarding Database table since the system was last reset. This value is also known as the MFDB high-water mark.
Current Entries	Shows the current number of entries in the Multicast Forwarding Database table.

2. Click **Refresh** to update the information on the screen with the most current data.

IGMP Snooping VLAN Configuration

Use the IGMP Snooping VLAN Configuration page to configure IGMP snooping settings for VLANs on the system.

To access the IGMP Snooping VLAN Configuration page:

1. Click **Switching** > **Multicast** > **IGMP Snooping** > **IGMP Snooping VLAN Configuration** in the navigation tree.

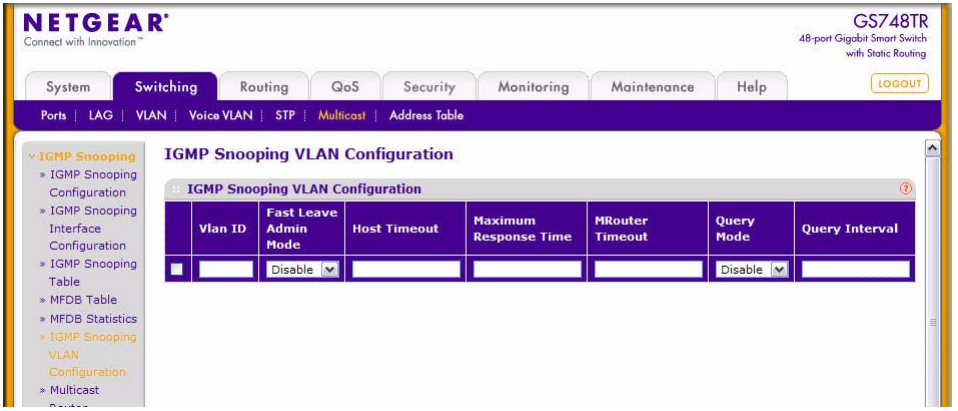


Figure 3-29

Table 3-27. IGMP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	List of VLAN IDs for which IGMP Snooping is enabled.
Fast Leave Admin Mode	Enable or disable the IGMP Snooping Fast Leave Mode for the specified VLAN ID. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface. You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.
Host Timeout	Sets the value for group membership interval of IGMP snooping for the specified VLAN ID. The valid range is (Maximum Response Time + 1) to 3600 seconds.

Table 3-27. IGMP Snooping VLAN Configuration Fields (continued)

Field	Description
Maximum Response Time	Enter the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to (Group Membership Interval -1) seconds. Its value should be greater than the Group Membership Interval value.
MRouter Timeout	Sets the value for multicast router expiry time of IGMP Snooping for the specified VLAN ID. The valid range is 0 to 3600 seconds.
Query Mode	Enable or disable the IGMP Querier Mode for the specified VLAN ID.
Query Interval	Enter the value for IGMP Query Interval for the specified VLAN ID. Valid range is 1 to 18000.

2. Click **Add** to enable IGMP snooping on the specified VLAN.
3. Click **Delete** to disable IGMP snooping on the specified VLAN.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make any configuration changes, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

Multicast Router Configuration

Use the IGMP Snooping Multicast Router Configuration page to configure an interface as a static multicast router interface. All IGMP packets snooped by the switch will be forwarded to the multicast router reachable from this interface. The configuration is not needed most of the time since the switch will automatically detect the presence of multicast router and forward IGMP packets accordingly. It is only needed when you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

To access the IGMP Snooping Multicast Router Configuration page:

1. Click **Switching** > **Multicast** > **IGMP Snooping** > **Multicast Router Configuration** in the navigation tree.

2.

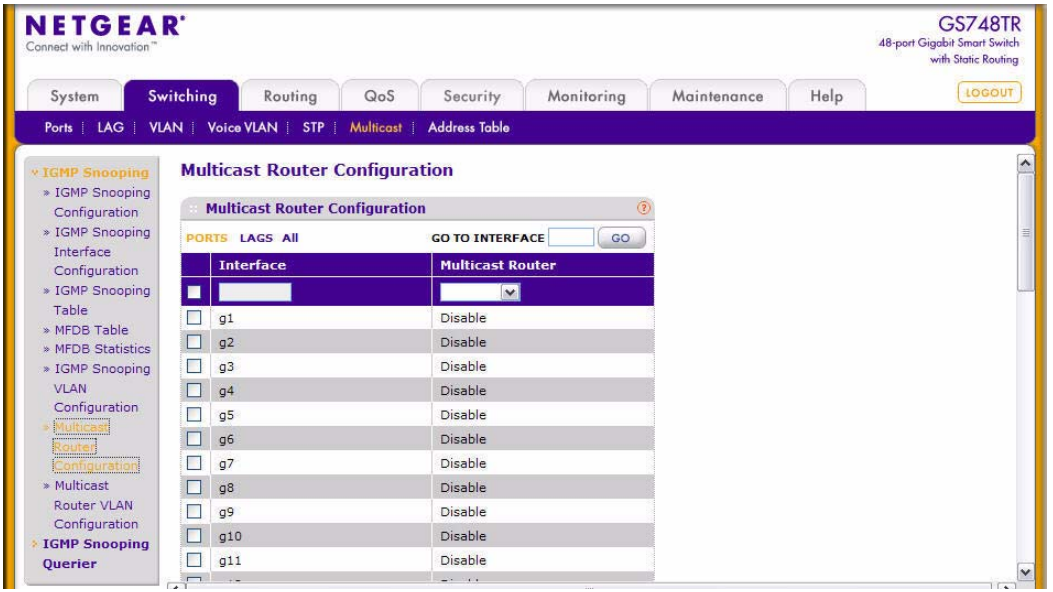


Figure 3-30

Table 3-28. Multicast Router Configuration Fields

Field	Description
Interface	This lists all physical interfaces. Select the interface for which you want Multicast Router to be enabled.
Multicast Router	Enable or disable Multicast Router on the selected interfaces. • **Enable:** The port is a multicast router interface. • **Disable:** The port does not have a multicast router configured.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. If you enable or disable multicast router configuration on an interface, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

Multicast Router VLAN Configuration

Use the IGMP Snooping Multicast Router VLAN Configuration page to configure multicast router settings for VLANs on an interface.

To access the IGMP Snooping Multicast Router VLAN Configuration page:

1. Click **Switching** > **Multicast** > **IGMP Snooping** > **Multicast Router VLAN Configuration** in the navigation tree.

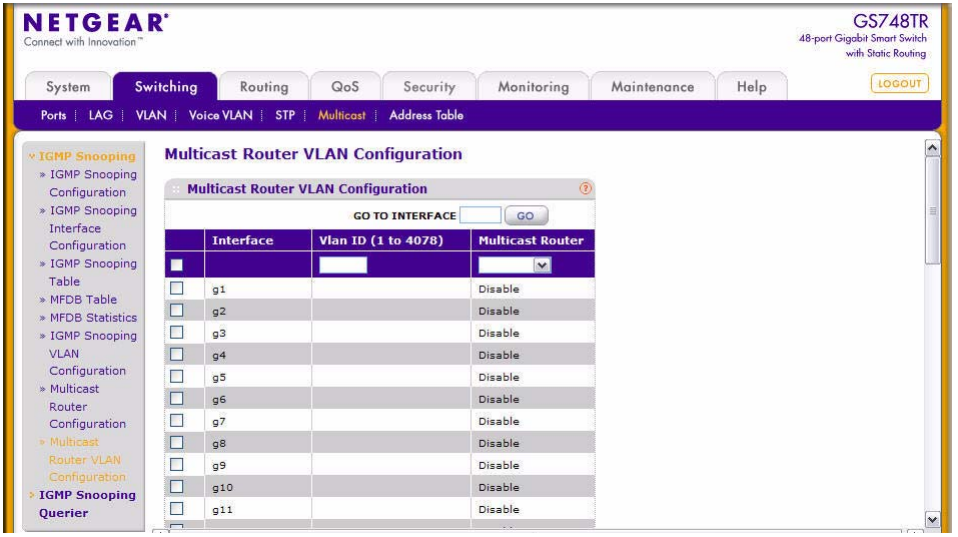


Figure 3-31

Table 3-29. Multicast Router VLAN Configuration Fields

Field	Description
Interface	Select the physical or LAG interface for which you want Multicast Router to be enabled.
VLAN ID	Enter the VLAN ID to configure as enabled or disabled for multicast routing. The valid range is 1 to 4078.
Multicast Router	Select **Enable** or **Disable** from the menu to change the multicast router mode of the VLAN associated with this interface.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. If you make any configuration changes, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

Configuring IGMP Snooping Queriers

IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the 'IGMP querier'. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

These pages enable you to configure and display information on IGMP snooping queriers on the network and, separately, on VLANs.

The IGMP Snooping Querier folder contains links to the following features:

- “IGMP Snooping Querier Configuration” on page 3-45
- “IGMP Snooping Querier VLAN Configuration” on page 3-46
- “IGMP Snooping Querier VLAN Status” on page 3-48

IGMP Snooping Querier Configuration

Use this page to enable or disable the IGMP Snooping Querier feature, specify the IP address of the router to perform the querying, and configure related parameters.

To access this page:

1. Click **Switching** > **Multicast** > **IGMP Snooping Querier** > **IGMP Snooping** > **Querier Configuration** in the navigation tree.

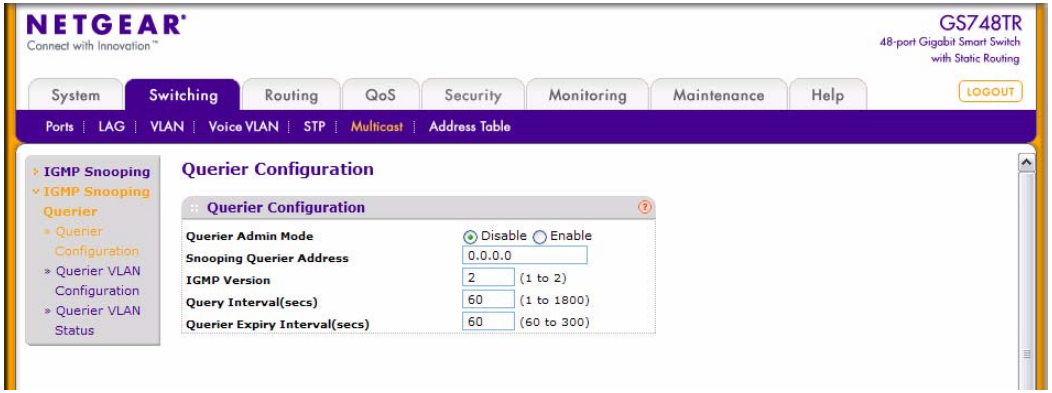


Figure 3-32

Table 3-30. IGMP Snooping Querier Configuration Fields

Field	Description
Querier Admin Mode	Select the administrative mode for IGMP Snooping for the switch from the menu. The default is **Disable**.
Snooping Querier Address	Specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which the query is being sent.
IGMP Version	Specify the IGMP protocol version used in periodic IGMP queries.
Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

2. Click **Refresh** to redisplay the page with the latest information from the switch.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you configure an IGMP snooping querier, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

IGMP Snooping Querier VLAN Configuration

Use this page to configure IGMP queriers for use with VLANs on the network.

To access this page:

1. Click **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration** in the navigation tree.

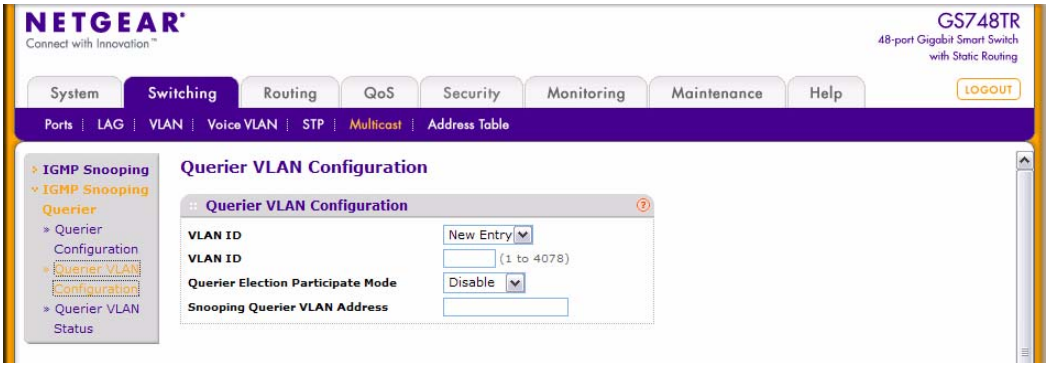


Figure 3-33

Table 3-31. IGMP Snooping Querier VLAN Configuration Fields

Field	Description
VLAN ID	Specifies VLAN ID for which the IGMP Snooping Querier is to be enabled. Select **New Entry** to create a new VLAN ID for IGMP Snooping. You can also set pre-configurable Snooping Querier parameters.
Querier Election Participate Mode	Enable or disable Querier Participate Mode. When this mode is disabled, upon seeing another querier of same version in the VLAN, the snooping querier moves to non-querier state. When enabled, the snooping querier participates in querier election, in which the least IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
Snooping Querier VLAN Address	Specify the Snooping Querier Address to be used as the source address in periodic IGMP queries sent on the specified VLAN.

2. Click **Refresh** to redisplay the page with the latest information from the switch.
3. Click **Delete** to disable Snooping Querier on the selected VLAN. This button is not visible when a VLAN is not selected.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you configure a snooping querier for a VLAN, click **Apply** to apply the new settings to the switch.

IGMP Snooping Querier VLAN Status

Use this page to view the operational state and other information for IGMP snooping queriers for VLANs on the network.

To access this page:

1. Click **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status** in the navigation tree.

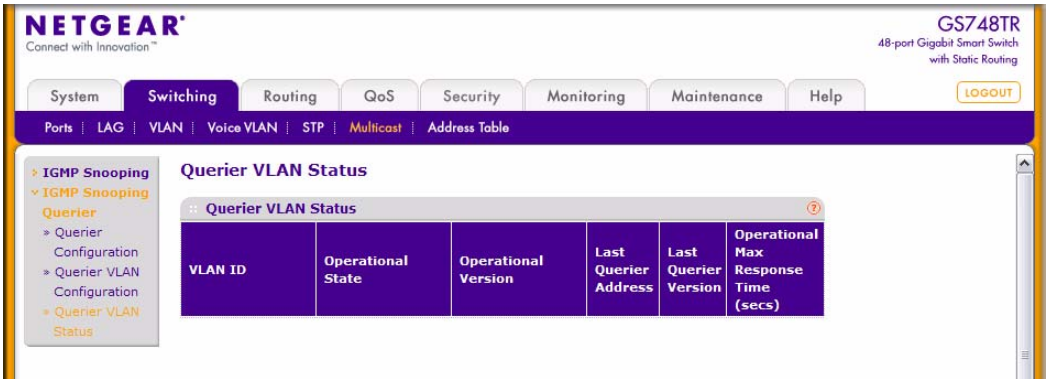


Figure 3-34

Table 3-32. IGMP Snooping Querier VLAN Status Fields

Field	Description
VLAN ID	Specifies the VLAN ID on which the IGMP Snooping Querier is administratively enabled and for which VLAN exists in the VLAN database.
Operational State	Specifies the operational state of the IGMP Snooping Querier on a VLAN: • **Querier**: The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode. • **Non-Querier**: The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. • **Disabled**: The snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when IGMP snooping is not operational on the VLAN, when the querier address is not configured, or the network management address is not configured.
Operational Version	Displays the IGMP protocol version of the operational querier.
Last Querier Address	Displays the IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	Displays the IGMP protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	Displays the maximum response time to be used in the queries that are sent by the snooping querier.

2. Click **Refresh** to redisplay the page with the latest information from the switch.

Searching and Configuring the Forwarding Database

The forwarding database maintains a list of MAC addresses after having received a packet from this MAC address. The transparent bridging function uses the forwarding database entries to determine how to forward a received frame.

The **Address Table** folder contains links to the following features:

- “Searching the MAC Address Table” on page 3-50
- “Dynamic Address Configuration” on page 3-52

- "MAC Address Table" on page 3-53
- "Static MAC Address" on page 3-55

Searching the MAC Address Table

Use the search function of the MAC Address Table page to display information about unicast entries for which the switch has forwarding and/or filtering information.

To access this page:

1. Click **Switching > Address Table > Basic > Address Table** in the navigation tree.
2. Use the "Search By" field to search for MAC Addresses by **MAC Address**, **VLAN ID**, or **Interface**.
    - **MAC Address**: Select **MAC Address** from the menu and enter a six-byte hexadecimal MAC address in two-digit groups separated by colons. Then click **Go**. If the address exists, that entry will be displayed. An exact match is required.
    - **VLAN ID**: Select **VLAN ID** from the menu, enter the VLAN ID, for example 100. Then click **Go**. If any entries with that VLAN ID exist they are displayed.

- **Interface**: Select **Interface** from the menu, enter the interface ID in g1, g2... format. Then click **Go**. If any entries with learned on that interface exist, they are displayed.

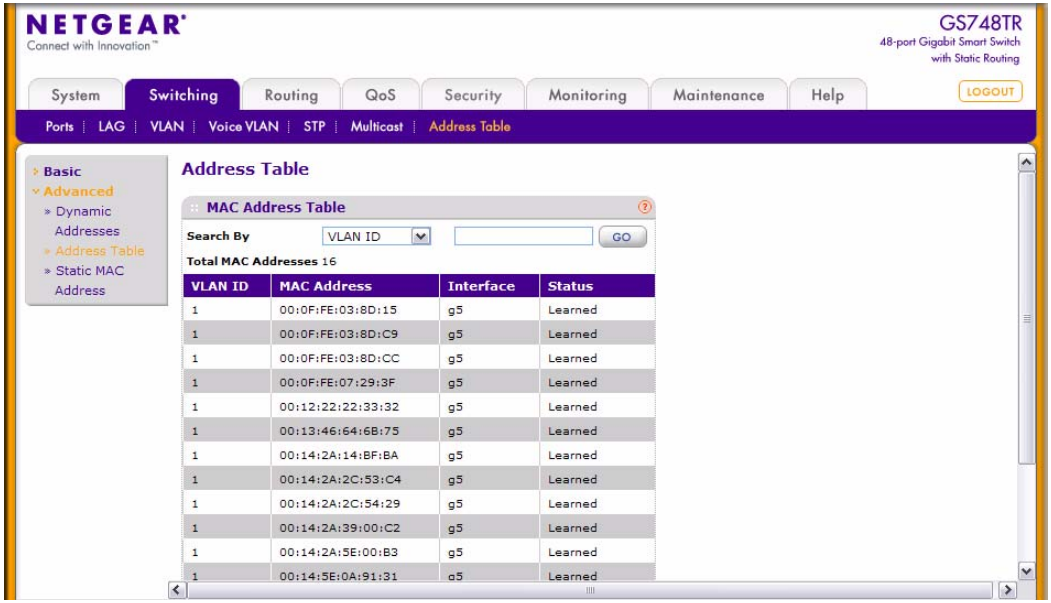


Figure 3-35

Table 3-33. MAC Address Table Fields

Field	Description
VLAN ID	Specifies the VLAN ID on which the IGMP Snooping Querier is administratively enabled and for which VLAN exists in the VLAN database.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six byte MAC address with each byte separated by colons. For example: 00:0F:89:AB:CD:EF.
Interface	The port where this address was learned. In other words, this field shows the port through which the MAC address can be reached.
Status	The status of this entry. The possible values are: • **Static:** The entry was added when a static MAC filter was defined. • **Learned:** The entry was learned by observing the source MAC addresses of incoming traffic, and is currently in use. • **Management:** The system MAC address, which is identified with interface c1.

3. Click **Clear** to clear Dynamic MAC Addresses in the table.
4. Click **Refresh** to redisplay the page to show the latest MAC Addresses.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Dynamic Address Configuration

Use the **Advanced > Dynamic Addresses** page to set the amount of time to keep a learned MAC address entry in the forwarding database. The forwarding database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time.

To access the Configuration page:

1. Click **Switching > Address Table > Advanced > Dynamic Addresses** in the navigation tree.

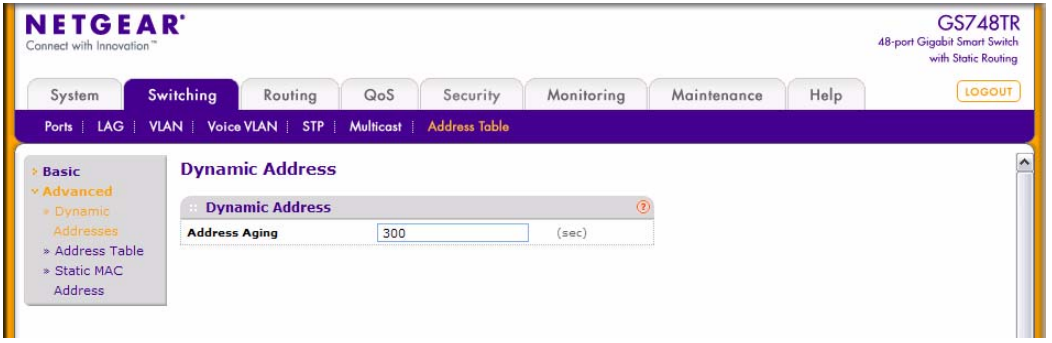


Figure 3-36

Table 3-34. Dynamic Address Configuration Fields

Field	Description
Address Aging	Specify the number of seconds the forwarding database should wait before deleting a learned entry that has not been updated. 802.1d-1990 recommends a default of 300 seconds. You may enter any number of seconds between 10 and 1000000. The factory default is 300.

	**Note:** IEEE 802.1d recommends a default of 300 seconds, which is the factory default.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Apply** to apply to send the updated configuration to the switch. Configuration changes take effect immediately.

MAC Address Table

The MAC Address Table contains information about unicast entries for which the switch has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

To access the MAC Address Table page:

1. Click **Switching > Address Table > Advanced > Address Table** in the navigation tree.

   You can search for MAC Addresses by VLAN ID, MAC Address, or interface:

   - Search by VLAN ID. Select **VLAN ID** from the menu, and enter the VLAN ID, for example, 100. Then click the **Go** button. If the address exists, the entry will be displayed as the first entry, followed by the remaining (greater) MAC addresses.
   - Search by MAC Address. Select **MAC Address** from the menu and enter a six-byte hexadecimal MAC address in two-digit groups separated by colons. Then click **Go**. If the address exists, that entry will be displayed. An exact match is required.
   - Search by Interface. Select **Interface** from the menu, enter the interface ID in g1, g2... format. Then click **Go**. If any entries with learned on that interface exist, they are displayed.

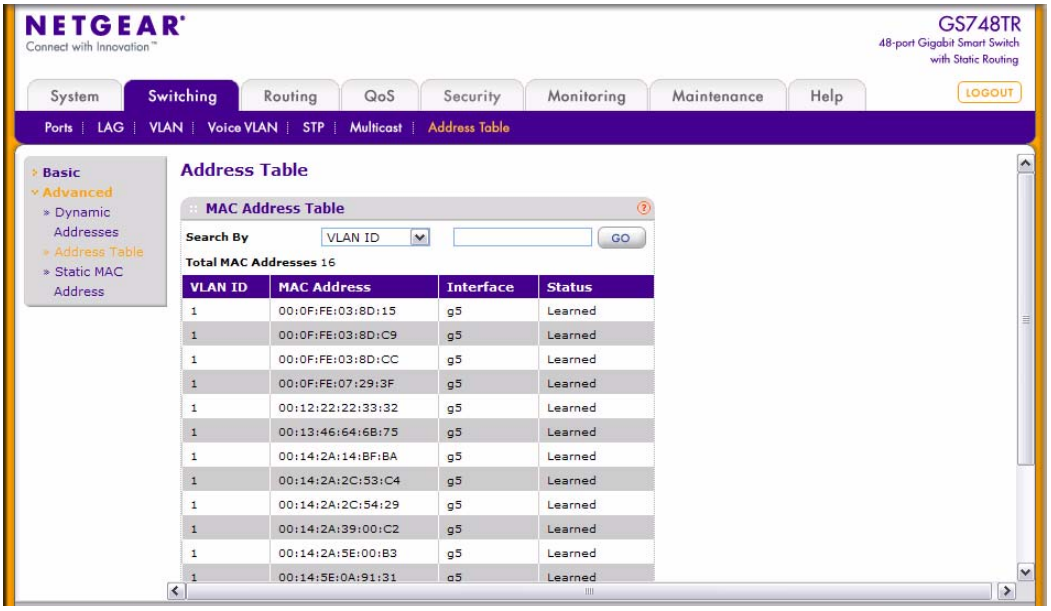


Figure 3-37

Table 3-35. MAC Address Table Fields

Field	Description
VLAN ID	The VLAN ID associated with the MAC Address.
MAC Address	A unicast MAC Address for which the switch has forwarding and/or filtering information. The MAC address is in the format of 6 two-digit hexadecimal numbers that are separated by colons. For example, 00:0f:5e:45:67:89 is the MAC Address.
Interface	The port upon which this address was learned.
Status	The status of this entry. Possible values are: • **Learned**. The value of the corresponding instance was learned, and is being used. • **Management**. The value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress. • **Static**.THe value of the corresponding instance was added by the system or a user and cannot be relearned.

2. Click **Clear** to clear the entries.
3. Click **Refresh** to reload the page and display the latest MAC address learned on a specific port.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Static MAC Address

Use the Static MAC Address Configuration page to view static MAC addresses configured on an interface.

To access the Static MAC Address Configuration page:

1. Click **Switching > Address Table > Advanced > Static MAC Address** in the navigation tree.

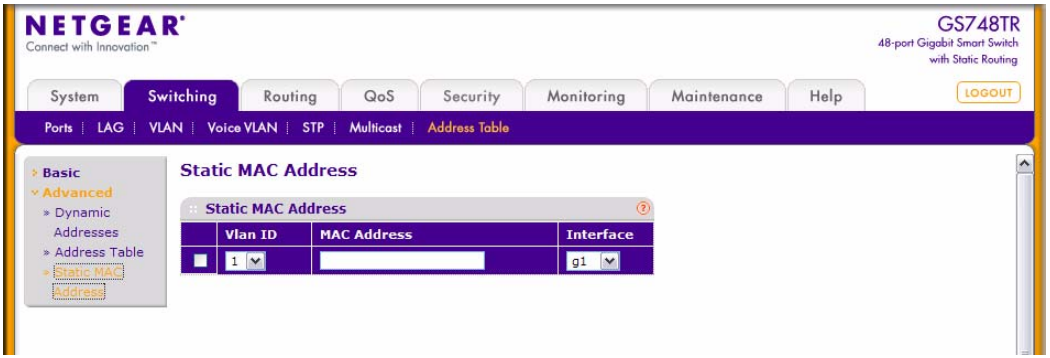


Figure 3-38

Table 3-36. Static MAC Address Fields

Field	Description
VLAN ID	Select the VLAN ID corresponding to the MAC address being added.
Static MAC Address	Only packets with source address matching this MAC Address will be admitted, otherwise it will be discarded.
Interface	Select the physical interface for which you want to display data.

2. Click **Refresh** to reload the page and display the latest MAC address learned on a specific port.
3. Enter a new static MAC address in the field, select the VLAN ID corresponding to the MAC address being added, then click **Add** to add the static MAC address to the switch.

4. After you enter the MAC address and VLAN ID of the statically configured MAC address to delete, click **Delete** to remove the MAC address from the port and apply the new settings to the system. The screen refreshes, and the MAC address no longer appears in the table on the page.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. If you make any changes to the page, click **Apply** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Chapter 4
Configuring Routing

GS700TR Smart Switch supports IP routing. Use the links in the Routing navigation tree folder to manage routing on the system. This section contains the following information:

When a packet enters the switch, the destination MAC address is checked to see if it matches any of the configured routing interfaces. If it does, then the silicon searches the host table for a matching destination IP address. If an entry is found, then the packet is routed to the host. If there is not a matching entry, then the switch performs a longest prefix match on the destination IP address. If an entry is found, then the packet is routed to the next hop. If there is no match, then the packet is routed to the next hop specified in the default route. If there is no default route configured, then the packet is passed to the software to be handled appropriately.

The routing table can have entries added either statically by the administrator or dynamically via a routing protocol. The host table can have entries added either statically by the administrator or dynamically via ARP.

Configuring IP Settings

Use the following web pages to configure and display IP routing data:

IP Configuration

Use the IP Configuration page to configure routing parameters for the switch.

To access the IP Configuration page:

1. Click **Routing** > **IP** > **IP Configuration** in the navigation tree.

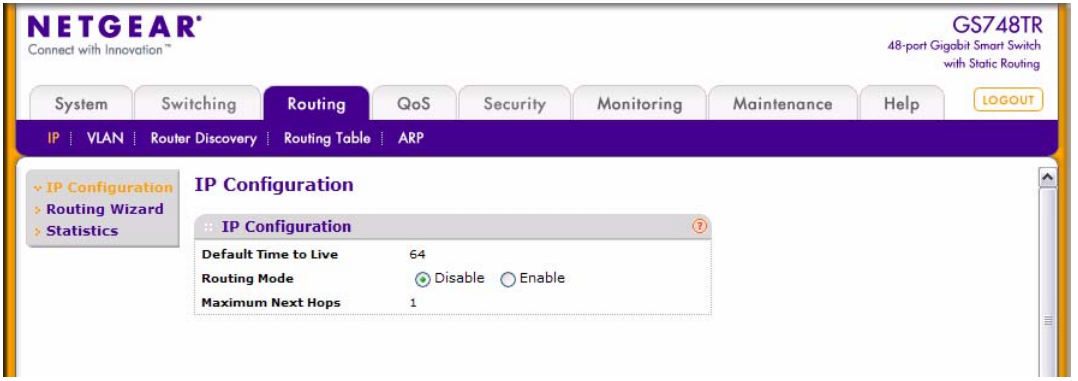


Figure 4-1

Table 4-1. IP Configuration Fields

Field	Description
Default Time to Live	The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol.
Routing Mode	Select either the Enable or the Disable radio button. You must enable routing for the switch before you can route through any of the interfaces. Routing is also enabled or disabled per VLAN interface. The default value is Disable.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a read-only value.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any changes to the page, click **Apply** to apply the changes to the system.

VLAN Routing Wizard

Use the VLAN Routing Wizard page to configure VLAN Routing interfaces on the system.]

To access the VLAN Routing Wizard page:

1. Click **Routing** > **IP** > **Routing Wizard** in the navigation tree.

Figure 4-2 shows the VLAN Routing Wizard page with the Unit and LAG fields expanded to show the ports. The page does not show the ports until you click the Unit or LAG link.

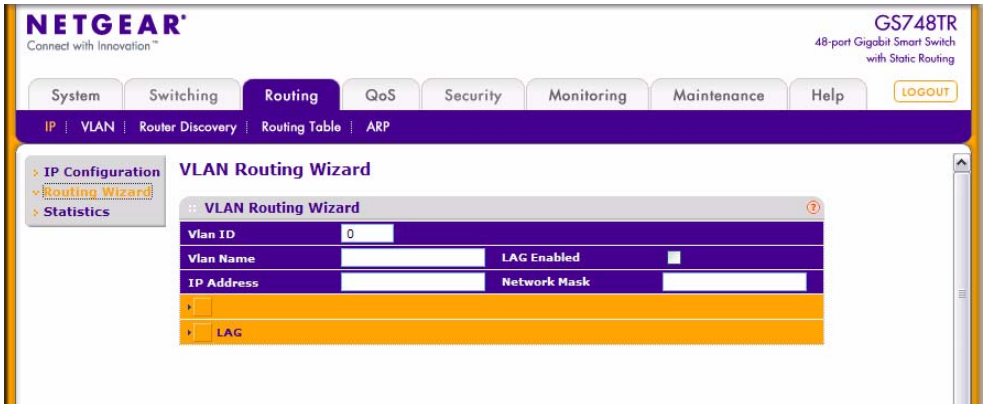


Figure 4-2

Table 4-2. VLAN Routing Configuration Fields

Field	Description
VLAN ID	Enter the ID of a VLAN to configure for VLAN Routing.The range of the VLAN ID is (1 to 4078).
VLAN Name	A unique name for the VLAN.
LAG Enabled	Select the check box to allow the ability to add selected ports to the VLAN as a LAG. The default is No.
IP Address	Enter an IP Address for the VLAN Routing Interface.
Network Mask	Enter a Subnet Mask for the VLAN Routing Interface.
Unit 1	Click **Unit 1** to display the ports on the switch. For each port, you can click its associated box to add the port to the VLAN as a tagged (T) or untagged (U) interface.
LAG	Click **LAG** to view the available LAGs on the switch. Click the box associated with the port to add the LAG to the VLAN as a tagged (T) or untagged (U) interface.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

IP Statistics

The statistics reported on the IP Statistics page are as specified in RFC 1213.

To display the page:

1. Click **Routing** > **IP** > **Statistics** in the navigation tree.

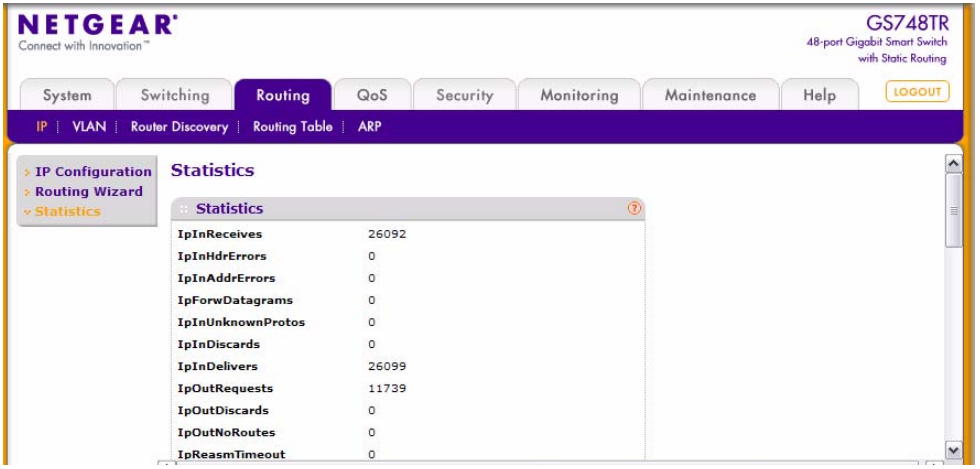


Figure 4-3

Note: Figure 4-3 shows some, but not all, of the fields on the page.

Table 4-3. IP Statistics Fields

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

Table 4-3. IP Statistics Fields (continued)

Field	Description
IpInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter includes only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.

Table 4-3. IP Statistics Fields (continued)

Field	Description
IpReasmOKs	The number of IP datagrams successfully re-assembled.
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
IcmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
IcmpInErrors	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
IcmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
IcmpInTimeExcds	The number of ICMP Time Exceeded messages received.
IcmpInParmProbs	The number of ICMP Parameter Problem messages received.
IcmpInSrcQuenchs	The number of ICMP Source Quench messages received.
IcmpInRedirects	The number of ICMP Redirect messages received.
IcmpInEchos	The number of ICMP Echo (request) messages received.
IcmpInEchoReps	The number of ICMP Echo Reply messages received.
IcmpInTimestamps	The number of ICMP Timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.

Table 4-3. IP Statistics Fields (continued)

Field	Description
IcmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object is always zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
IcmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

2. Click **Refresh** to update the page with the most current data.

Configuring VLAN Routing

You can configure GS700TR Smart Switch software with some ports supporting VLANs and some supporting routing. You can also configure the software to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC Destination Address (MAC DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN, and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, plus the internal bridge-router interface, if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required. This section shows how to configure GS700TR Smart Switch software to support VLAN routing. A port can be either a VLAN port or a router port, but not both. However, a VLAN port may be part of a VLAN that is itself a router port.

VLAN Routing Configuration

Use the VLAN Routing Configuration page to view information about the VLAN routing interfaces configured on the system or to assign an IP address and subnet mask to VLANs on the system.

To display the page:

1. Click the **Routing** > **VLAN** tab.

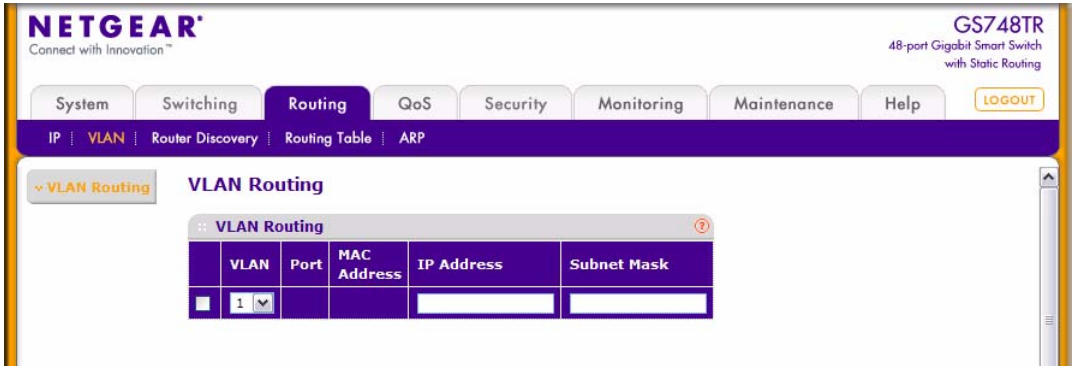


Figure 4-4

Table 4-4. VLAN Routing Configuration Fields

Field	Description
VLAN ID	Select a VLAN ID from the menu to configure VLAN routing properties. VLANs that are already configured for routing appear in the table. To perform the same configuration on all VLAN routing interfaces, select the check box in the heading row. To change the configuration for a single interface, select the check box next to the VLAN ID.
Port	The logical slot and port number assigned to the VLAN Routing Interface.

Table 4-4. VLAN Routing Configuration Fields (continued)

Field	Description
MAC Address	The MAC Address assigned to the VLAN Routing Interface.
IP Address	Enter an IP Address of the VLAN Routing Interface.
Subnet Mask	Enter a Subnet Mask for the VLAN Routing Interface.

Configuring Router Discovery

The Router Discovery protocol is used by hosts to identify operational routers on the subnet. Router Discovery messages are of two types: “Router Advertisements” and “Router Solicitations.” The protocol mandates that every router periodically advertise the IP Addresses it is associated with. Hosts listen for these advertisements and discover the IP Addresses of neighboring routers.

Router Discovery Configuration

Use the Router Discovery Configuration page to enter or change Router Discovery parameters.

To display the page:

1. Click the **Routing > Router Discovery** tab.

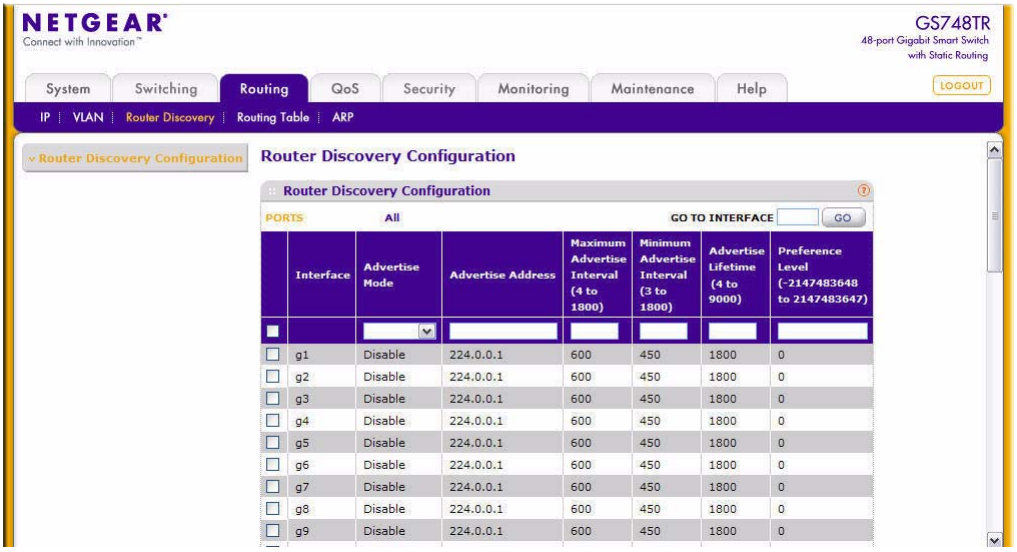


Figure 4-5

Table 4-5. Router Discovery Configuration Fields

Field	Description
Interface	Select the router interface for which data is to be configured. To perform the same configuration on all interfaces, select the check box in the heading row. To configure a single interface, select the check box associated with the interface. The interface number appears in the **Interface** field in the table heading row.
Advertise Mode	Select Enable or Disable from the dropdown menu. If you select Enable, Router Advertisements are transmitted from the selected interface.
Advertise Address	Enter the IP Address to be used to advertise the router.
Maximum Advertise Interval (secs)	Enter the maximum time (in seconds) allowed between router advertisements sent from the interface. The allowed range for this field is 4 to 1800.
Minimum Advertise Interval (secs)	Enter the minimum time (in seconds) allowed between router advertisements sent from the interface. The allowed range for this field is 3 to 1800.
Advertise Lifetime (secs)	Enter the value (in seconds) to be used as the lifetime field in router advertisements sent from the interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts. The allowed range for this field is 4 to 9000, i.e. the configured “Maximum Advertise Interval” to 9000.
Preference Level	Specify the preference level of the router as a default router relative to other routers on the same subnet. Higher numbered addresses are preferred. You must enter an integer.

2. If you make any changes to the page, click **Apply** to apply the changes to the system.

Configuring and Viewing Routes

From the **Routing Table** page, you can configure static and default routes and view the routes that the GS700TR has already learned. To display the page:

1. Click the **Routing > Routing Table** tab.

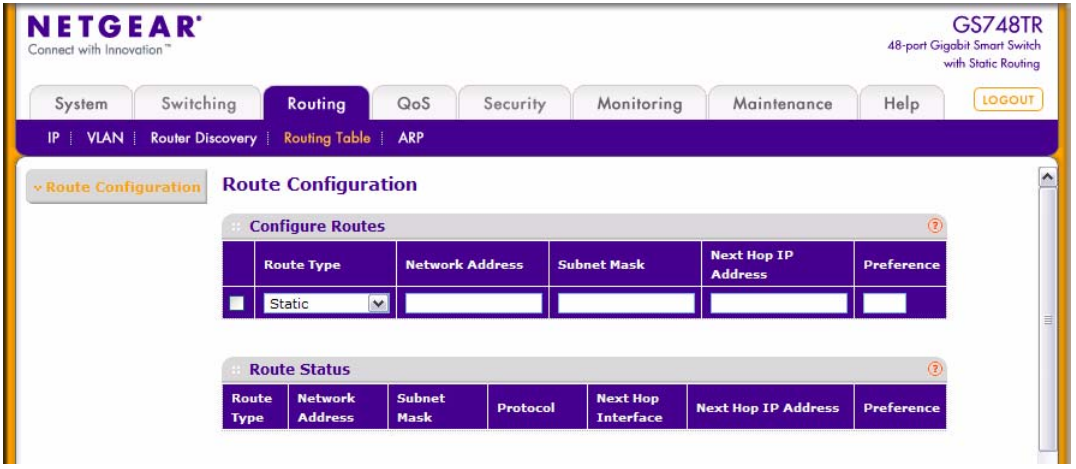


Figure 4-6

Table 4-6. Route Configuration Fields

Field	Description
Route Type	Specifies whether the route is to be a Default route or a Static route. If creating a default route, all you need to specify is the next hop IP address, otherwise you need to specify each field.
Network Address	Specify the IP route prefix for the destination. In order to create a route, a valid routing interface must exist and the next hop IP Address must be on the same network as the routing interface.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP address that identifies the attached network.

Table 4-6. Route Configuration Fields

Field	Description
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network. When creating a route, the next hop IP must be on the same network as the routing interface. Valid next hop IP Addresses can be seen on the 'Route Table' page.
Preference	Specifies a preference value for the configured next hop. The preference is an integer value from 1 to 255. You can specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, the user controls whether a static route is more or less preferred. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

2. To add a route, enter the route information into the appropriate fields and click **Add**.
3. To delete a route, select the check box next to the route and click **Delete**.

The **Route Status** table provides information about the routes the GS700TR already has in its routing table.

Table 4-7. Route Status Fields

Field	Description
Route Type	Indicates whether the learned route is a static or default route.
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are one of the following: • Local • Static
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.

Table 4-7. Route Status Fields (continued)

Field	Description
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
Preference	Shows the preference value for the configured next hop.

Configuring ARP

The address resolution protocol (ARP) associates a layer 2 MAC address with a layer 3 IPv4 address. GS700TR Smart Switch software features both dynamic and manual ARP configuration. With manual ARP configuration, you can statically add entries into the ARP table.

ARP is a necessary part of the internet protocol (IP) and is used to translate an IP address to a media (MAC) address, defined by a local area network (LAN) such as Ethernet. A station needing to send an IP packet must learn the MAC address of the IP destination, or of the next hop router, if the destination is not on the same subnet. This is achieved by broadcasting an ARP request packet, to which the intended recipient responds by unicasting an ARP reply containing its MAC address. Once learned, the MAC address is used in the destination address field of the layer 2 header prepended to the IP packet.

The ARP cache is a table maintained locally in each station on a network. ARP cache entries are learned by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), every recipient has the opportunity to store the sender’s IP and MAC address in their respective ARP cache. The ARP response, being unicast, is normally seen only by the requestor, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The GS700TR switches support 480 ARP entries.

Devices can be moved in a network, which means the IP address that was at one time associated with a certain MAC address is now found using a different MAC, or may have disappeared from the network altogether (i.e., it has been reconfigured, disconnected, or powered off). This leads to stale information in the ARP cache unless entries are updated in reaction to new information seen

on the network, periodically refreshed to determine if an address still exists, or removed from the cache if the entry has not been identified as a sender of an ARP packet during the course of an ageout interval, usually specified via configuration.

Use the following web pages to configure and display ARP detail:

- “ARP Cache” on page 4-15
- “Global ARP Configuration” on page 4-16
- “ARP Entry Configuration” on page 4-17
- “ARP Entry Management” on page 4-19

ARP Cache

Use the ARP Cache page to view entries in the ARP table, a table of the remote connections most recently seen by this switch.

To display the page:

1. Click the **Routing** > **ARP** > **Basic** > **ARP Cache** tab.

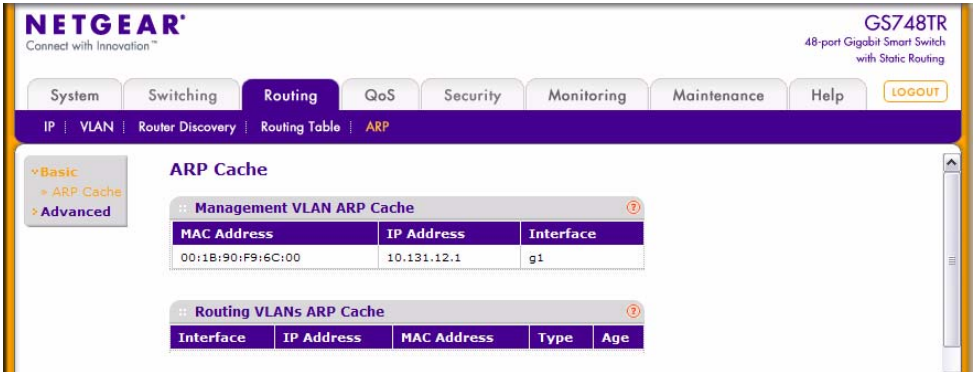


Figure 4-7

Table 4-8. Management VLAN ARP Cache Fields

Field	Description
MAC Address	Displays the MAC address of the device.
IP Address	Displays the associated IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
Interface	Shows the associated interface of the connection.

Table 4-9. Routing VLANs ARP Cache

Field	Description
Interface	The routing interface associated with the ARP entry.
IP Address	Displays the associated IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
MAC Address	Displays the unicast MAC address of the device.
Type	The type of the ARP entry. Possible values are: • Local. An ARP entry associated with one of the switch's routing interface's MAC addresses. • Gateway. A dynamic ARP entry whose IP address is that of a router. • Static. An ARP entry configured by the user. • Dynamic. An ARP entry which has been learned by the router.
Age	Age since the entry was last refreshed in the ARP Table. The format is hh:mm:ss.

2. Click **Refresh** to refresh the page with the most current data from the switch.

Global ARP Configuration

Use the **Global ARP Configuration** page to display and change the configuration parameters of the ARP table.

To display the page:

1. Click the **Advanced** > **Global ARP Configuration** link from the **Routing** > **ARP** tab.

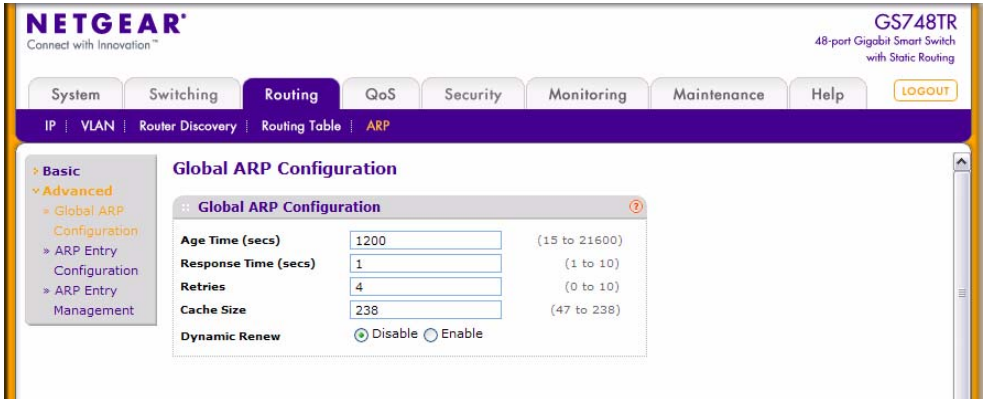


Figure 4-8

Table 4-10. Global ARP Configuration Fields

Field	Description
Age Time (secs)	Enter the value you want the switch to use for the ARP entry ageout time. You must enter a valid integer, which represents the number of seconds it will take for an ARP entry to age out. The range is 15 to 21600 seconds. The default value is 1200 seconds.
Response Time (secs)	Enter the value you want the switch to use for the ARP response timeout. You must enter a valid integer, which represents the number of seconds the switch will wait for a response to an ARP request. The range is 1 to 10 seconds. The default value is 1 second.
Retries	Enter an integer which specifies the maximum number of times an ARP request will be retried. The range for this field is 0 to 10. The default value is 4.
Cache Size	Enter an integer which specifies the maximum number of entries for the ARP cache. The range is 47 to 238. The default value is 238.
Dynamic Renew	This controls whether the ARP component automatically attempts to renew ARP entries of type Dynamic when they age out. The default setting is **Enable**.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately

ARP Entry Configuration

Use this page to add an entry to the ARP table. To display the page:

4. Click the **Advanced** > **ARP Entry Configuration** link from the **Routing** > **ARP** tab.

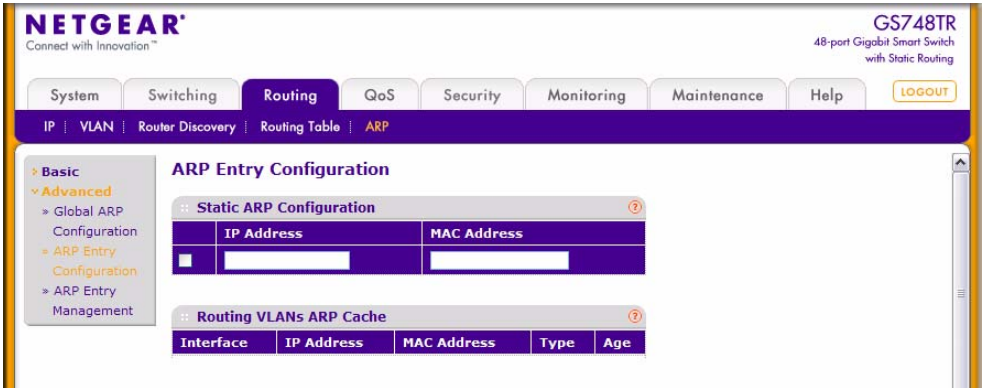


Figure 4-9

Table 4-11. Static ARP Configuration

Field	Description
IP Address	Enter the IP address that you want to add. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
MAC Address	The unicast MAC address of the device. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

Table 4-12. Routing VLANs ARP Cache Fields

Field	Description
Interface	The routing interface associated with the ARP entry.
IP Address	The IP address of a device on a subnet attached to one of the switch's routing interfaces.
MAC Address	The unicast MAC address for the device. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
Type	The type of the ARP entry, which can be one of the following: • Local - An ARP entry associated with one of the switch's routing interface's MAC addresses • Gateway - A dynamic ARP entry whose IP address is that of a router • Static - An ARP entry configured by the user • Dynamic - An ARP entry which has been learned by the router
Age	Age since the entry was last refreshed in the ARP Table. The format is hh:mm:ss

5. Click **Refresh** to refresh the page with the most current data from the switch.

6. Click **Add** to add an ARP Entry.
7. Click **Delete** to delete an ARP Entry.
8. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
9. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

ARP Entry Management

Use this page to remove certain entries from the ARP Table.

To display the page:

1. Click the **Routing > ARP > Advanced > ARP Entry Management** in the navigation tree.

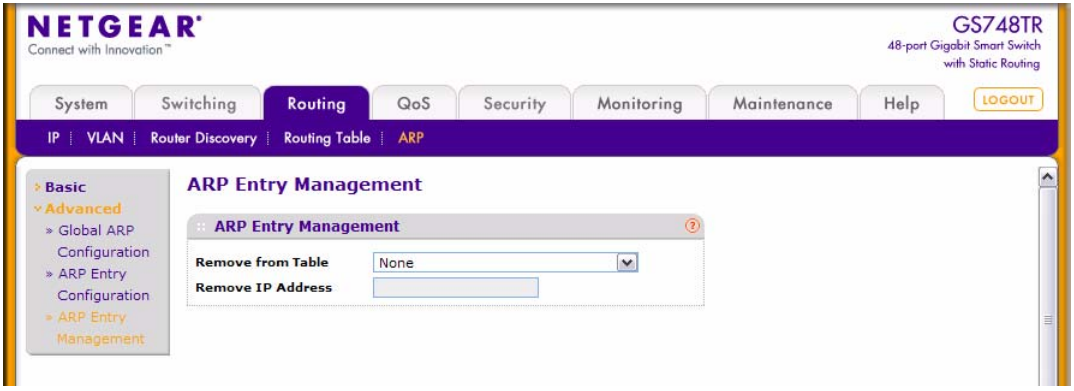


Figure 4-10

Table 4-13. ARP Entry Management Fields

Field	Description
Remove from Table	Allows you to remove certain entries from the ARP Table. The choices listed specify the type of ARP Entry to be deleted: • **All Dynamic Entries** • **All Dynamic and Gateway Entries** • **Specific Dynamic / Gateway Entry**. Selecting this allows you to specify the required IP address. • **Specific Static Entry**. • **None**. Select if you do not want to delete any entry from the ARP Table.
Remove IP Address	If you select **Specific Dynamic/Gateway Entry** or **Specific Static Entry** in the **Remove from Table** list, you can enter the IP address of an entry to remove from the ARP table.

Chapter 5
Configuring Quality of Service

This section gives an overview of Quality of Service (QoS) and explains the QoS features available from the Quality of Service navigation tree menu. This section contains the following subsections:

In a typical switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets have no place to be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given "special treatment" in a QoS capable network. With this in mind, all elements of the network must be QoS-capable. The presence of at least one node which is not QoS-capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

Note: Some of the features described in this section may not be supported in GS700TR Smart Switch software releases for particular hardware platforms.

Configuring Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be

used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, transmission rate shaping, etc., are user-configurable at the queue (or port) level.

Eight queues per port are supported.

The Class of Service folder contains links to the following features:

Basic CoS Configuration

Use the Trust Mode Configuration page to set the class of service trust mode of an interface. Each port in the switch can be configured to trust one of the packet fields (802.1p or IP DSCP), or to not trust any packet's priority designation (untrusted mode). If the port is set to a trusted mode, it uses a mapping table appropriate for the trusted field being used. This mapping table indicates the CoS queue to which the packet should be forwarded on the appropriate egress port(s). Of course, the trusted field must exist in the packet for the mapping table to be of any use, so there are default actions performed when this is not the case. These actions involve directing the packet to a specific CoS level configured for the ingress port as a whole, based on the existing port default priority as mapped to a traffic class by the current 802.1p mapping table.

Alternatively, when a port is configured as untrusted, it does not trust any incoming packet priority designation and uses the port default priority value instead. All packets arriving at the ingress of an untrusted port are directed to a specific CoS queue on the appropriate egress port(s), in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping is unable to be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

To display the Basic CoS Configuration page:

1. Click the **QoS > Basic > CoS Configuration** in the navigation tree.

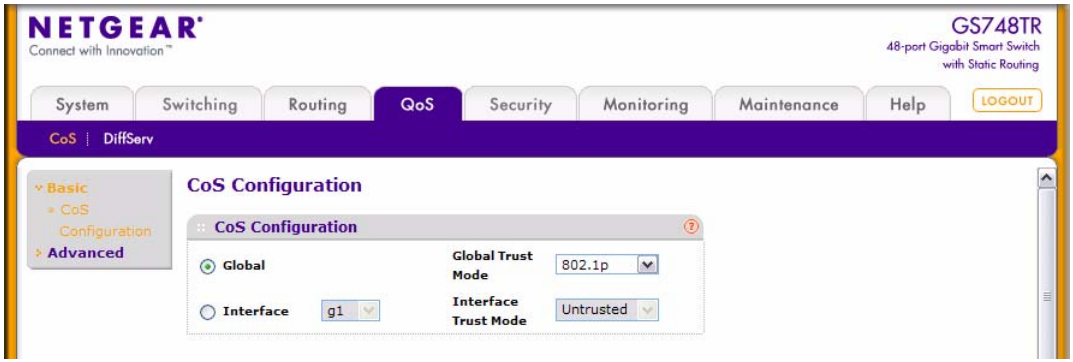


Figure 5-1

Table 5-1. Basic CoS Configuration Fields

Field	Description
Global	Select the Global option to apply the same trust mode to all CoS configurable interfaces.
Global Trust Mode	Specifies whether or not all interfaces trust a particular packet marking when the packet enters the port. The default value is trust 802.1p. The mode can only be one of the following: • Untrusted • 802.1p • DSCP
Interface	The menu contains all CoS configurable interfaces. Select an individual interface from the menu to override the global settings on a per-interface basis.
Interface Trust Mode	Specifies whether or not an interface trusts a particular packet marking when the packet enters the port. The default value is trust 802.1p. The mode can only be one of the following: • Untrusted • 802.1p • DSCP

CoS Interface Configuration

Use the CoS Interface Configuration page to apply an interface shaping rate to all ports or to a specific port.

To display the CoS Interface Configuration page:

1. Click the **QoS** > **CoS** tab, and then click the **Advanced** > **CoS Interface Configuration** link.

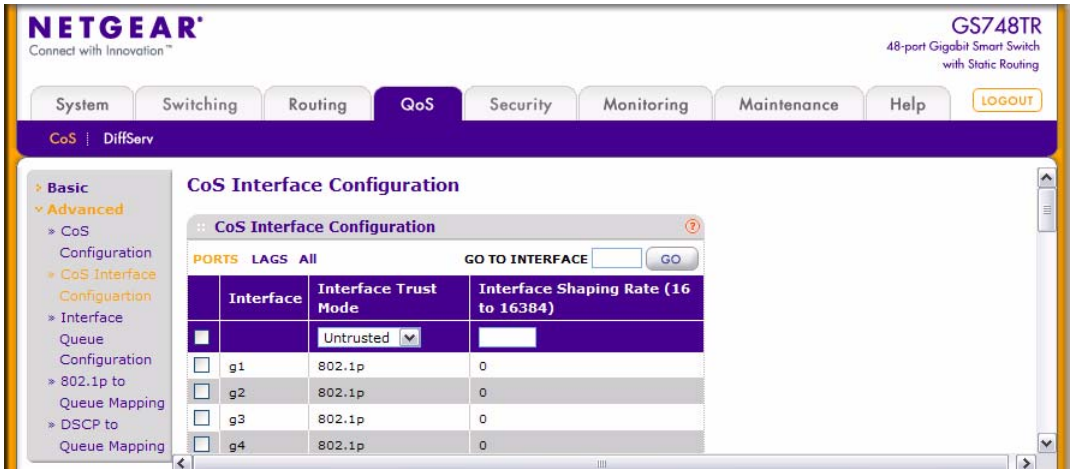


Figure 5-2

Table 5-2. Interface Configuration Fields

Field	Description
Interface	Indicates the interface to be affected by the Interface Shaping Rate. Select the check box in the heading row to apply a trust mode or rate to all interfaces. Select the check box next to an individual port to apply a trust mode or rate to a specific interface.
Interface Trust Mode	Specifies whether or not an interface (or all interfaces if all interfaces are selected) trust a particular packet marking when the packet enters the port. The default value is trust 802.1p. The mode can only be one of the following: • Untrusted • 802.1p • DSCP
Interface Shaping Rate	Specifies the maximum bandwidth allowed, typically used to shape the outbound transmission rate in increments of 64 kbps in the range of 16-16384. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. The default value is 0, in increments of 16. A value of 0 means the maximum is unlimited.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. If you make changes to the page, click **Apply** to apply the changes to the system.

Interface Queue Configuration

Use the Interface Queue Configuration page to define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port. Each port has its own CoS queue-related configuration.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally or per-port. A global configuration change is automatically applied to all ports in the system.

To display the Interface Queue Configuration page:

1. Click the **QoS** > **CoS** tab, and then click the **Advanced** > **Interface Queue Configuration** link.

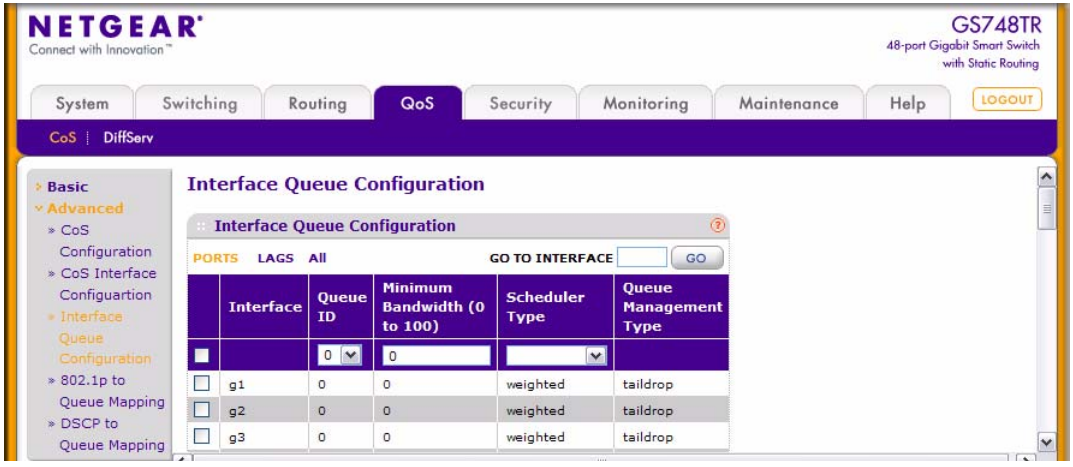


Figure 5-3

Table 5-3. Interface Queue Configuration Fields

Field	Description
Interface	Indicates the interface to configure. Select the check box in the heading row to apply a trust mode or rate to all interfaces. Select the check box next to an individual port to apply a trust mode or rate to a specific interface.
Queue ID	Use the menu to select the queue to be configured.

Table 5-3. Interface Queue Configuration Fields (continued)

Field	Description
Minimum Bandwidth	Enter a percentage of the maximum negotiated bandwidth for the selected queue on the interface. Specify a percentage from 0 to 100, in increments of 5.
Scheduler Type	Selects the type of queue processing from the dropdown menu. Options are **Weighted** and **Strict**. Defining on a per-queue basis allows the user to create the desired service characteristics for different types of traffic. • **Weighted**: Weighted round robin associates a weight to each queue. This is the default. The HW queues are mapped to the following weight proportions: 1:3:5:7:8:10:12:15. • **Strict**: Strict priority services traffic with the highest priority on a queue first.
Queue Management Type	Displays the type of packet management used for all packets, which is Taildrop. All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.

2. If you make changes to the page, click **Apply** to apply the changes to the system.

802.1p to Queue Mapping

The 802.1p to Queue Mapping page also displays the Current 802.1p Priority Mapping table. To display the 801.p to Queue Mapping page:

1. Click **QoS** > **CoS** > **Advanced** > **802.1p to Queue Mapping** to display the page.

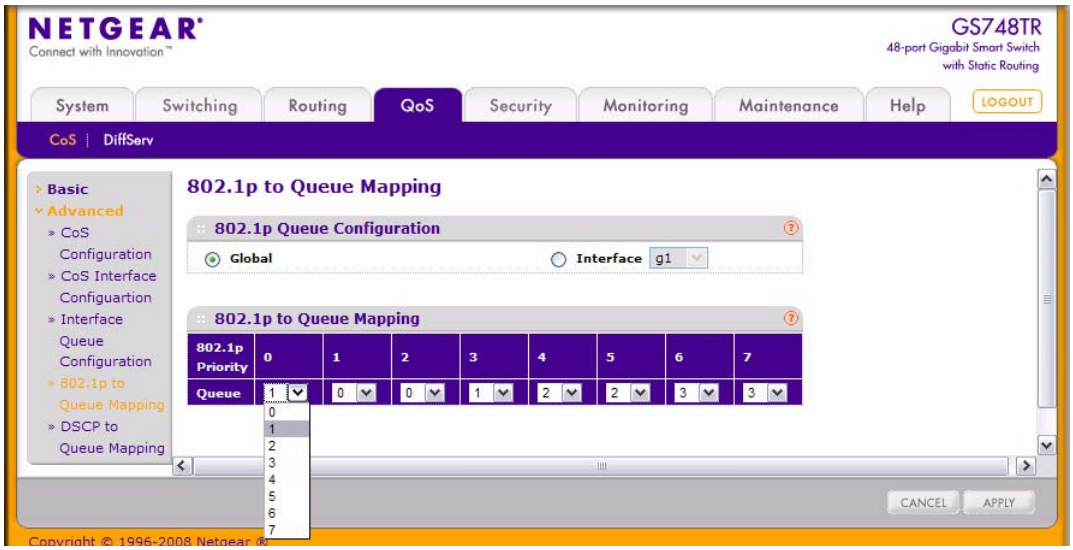


Figure 5-4

Table 5-4. Current 802.1p Priority Mapping Table Fields

Field	Description
Global	Select the Global option to apply the same 802.1p priority mapping to all CoS configurable interfaces.
Interface	The menu contains all CoS configurable interfaces. Select an individual interface from the menu to override the global settings for 802.1p priority mapping on a per-interface basis.
802.1p Priority	This row contains traffic class selectors for each of the eight 802.1p priorities to be mapped. The priority goes from low (0) to high (7). For example, traffic with a priority of 0 is for most data traffic and is sent using “best effort.” Traffic with a higher priority, such as 6, might be time-sensitive traffic, such as voice or video. The values in each dropdown menu represent the traffic class. The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent.

2. If you make changes to the page, click **Apply** to apply the changes to the system.

DSCP to Queue Mapping

Use the DSCP to Queue Mapping page to specify which internal traffic class to map the corresponding DSCP value.

To display the IP DSCP Mapping page:

1. Click the **QoS > CoS** tab, and then click the **Advanced > DSCP to Queue Mapping** link.

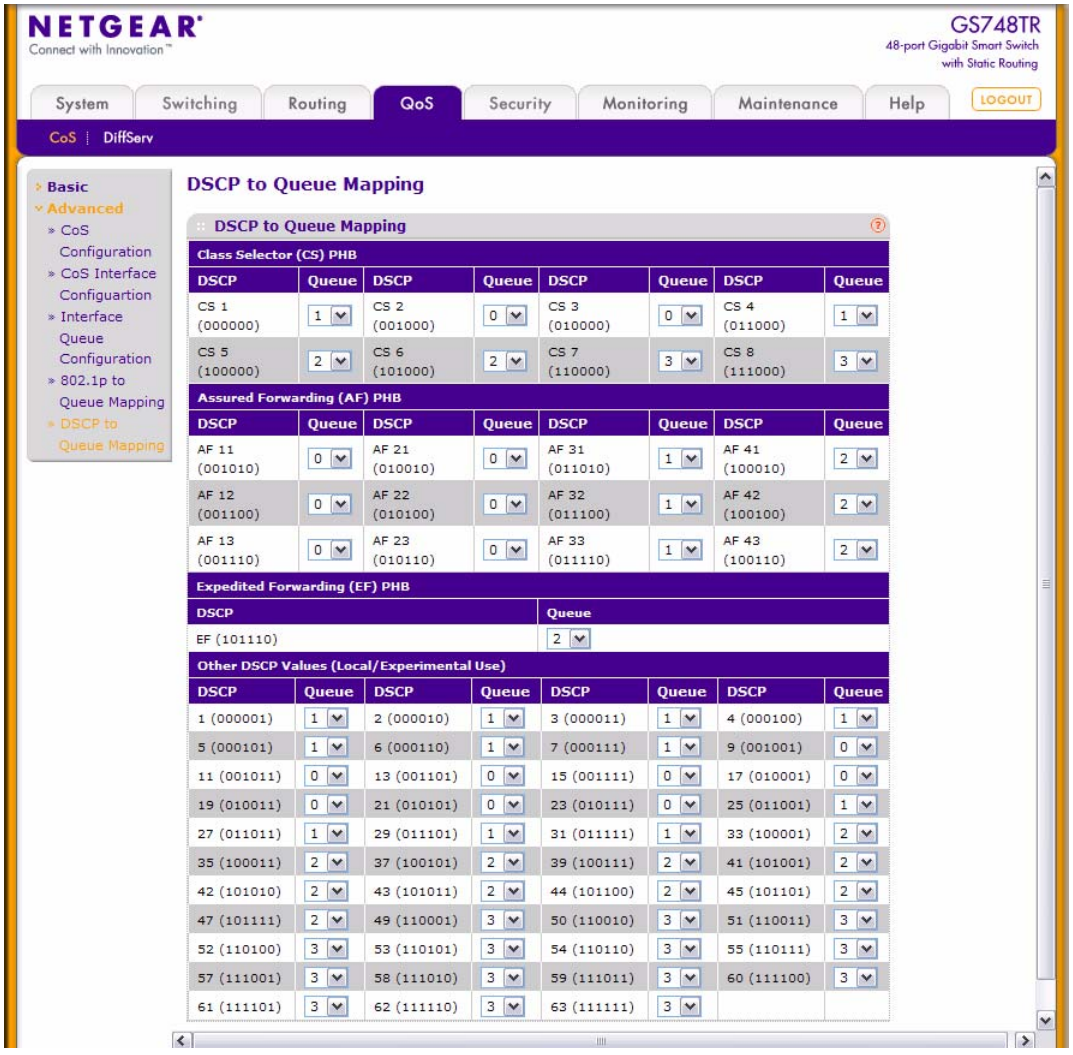


Figure 5-5

Table 5-5. IP DSCP Mapping Configuration Fields

Field	Description
DSCP	Lists the DSCP values to which you can map an internal traffic class. The values range from 0-63.
Queue	The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent. Valid range is 0-7.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make changes to the page, click **Apply** to apply the changes to the system.

Configuring Differentiated Services

The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Standard IP-based networks are designed to provide “best effort” data delivery service. “Best effort” service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications, such as e-mail and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. Conversely, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Defining DiffServ

To use DiffServ for QoS, the web pages accessible from the Differentiated Services menu page must first be used to define the following categories and their criteria:

1. Class: Create classes and define class criteria.
2. Policy: Create policies, associate classes with policies, and define policy statements.
3. Service: Add a policy to an inbound interface

Packets are classified and processed based on defined criteria. The classification criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

Packet processing begins by testing the class match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

The Differentiated Services menu page contains links to the various Diffserv configuration and display features.

To display the page, click **QoS > DiffServ** in the navigation menu. The Differentiated Services menu page contains links to the following features:

- "Diffserv Configuration"
- "Class Configuration"
- "Policy Configuration"
- "Service Configuration"
- "Service Statistics"

Diffserv Configuration

Use the Diffserv Configuration page to display DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables.

To display the page:

1. Click the **QoS > DiffServ > Basic > Diffserv Configuration** in the navigation tree.

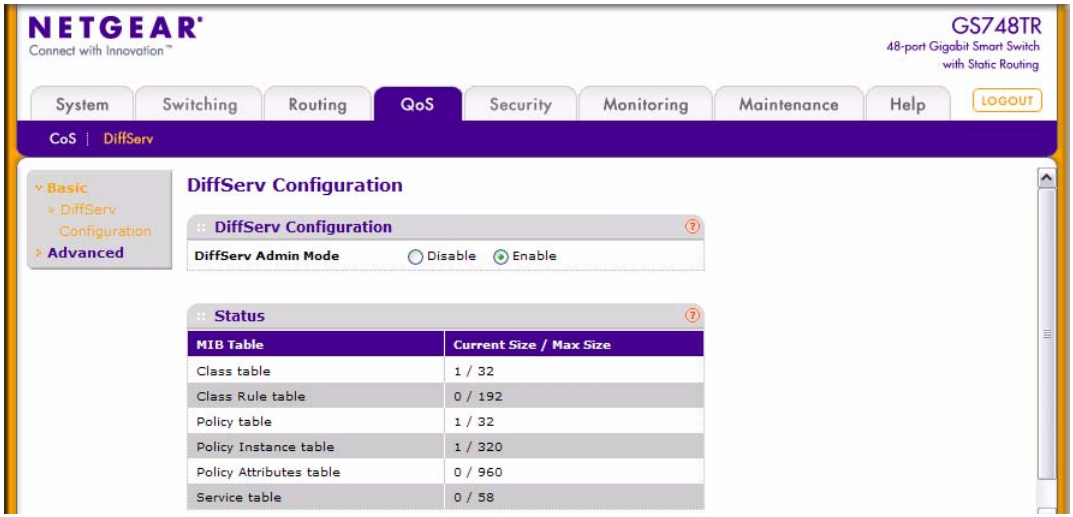


Figure 5-6

Table 5-6. DiffServ Configuration Fields

Field	Description
DiffServ Admin Mode	Turns admin mode on and off. While disabled, the DiffServ configuration is retained and can be changed, but it is not active. While enabled, Differentiated Services are active.
Status Field	
Class Table	Displays the current and maximum number of rows of the class table.
Class Rule Table	Displays the current and maximum number of rows of the class rule table.
Policy Table	Displays the current and maximum number of rows of the policy table.
Policy Instance Table	Displays the current and maximum number of rows of the policy instance table.
Policy Attributes Table	Displays the current and maximum number of rows of the policy attributes table.
Service Table	Displays the current and maximum number of rows of the service table.

2. If you change the DiffServ admin mode, click **Apply** to apply the change to the system.

Class Configuration

Use the Class Configuration page to add a new Diffserv class name, or to rename or delete an existing class. The page also allows you to define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can have multiple match criteria in a class. The logic is a Boolean “logical-and” for this criteria.

To display the page:

1. Click the **QoS > DiffServ** tab and then click the **Advanced > Class Configuration** link.

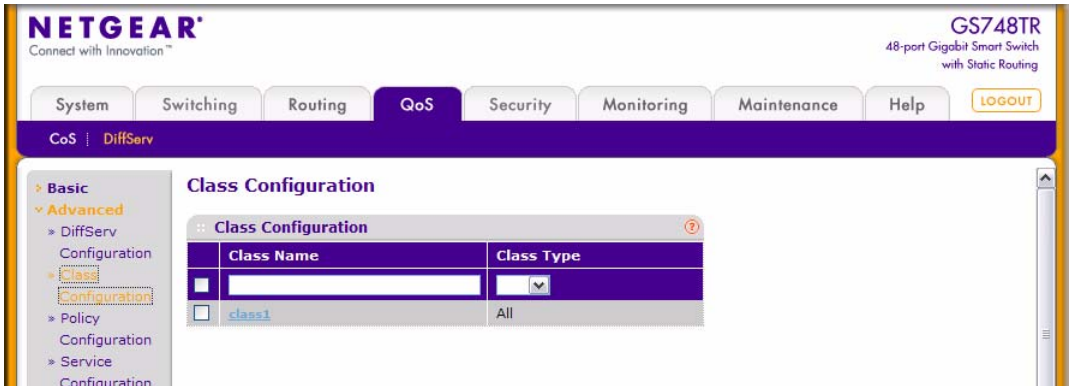


Figure 5-7

Table 5-7. DiffServ Class Creation Fields

Field	Description
Class Name	Enter a class name. To create a new class, select the class type and click **Add**. To rename an existing class, click **Apply** after you enter the class name.
Class Type	Currently the hardware supports only the **Class Type** value **All**, which means all the various match criteria defined for the class should be satisfied for a packet match. **All** signifies the logical **AND** of all the match criteria.

2. Click **Refresh** to refresh the page with the most current data from the switch.
3. To delete a Class Name, click the check box beside the Class Name, then click **Delete** to remove the Class Name.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

To configure the class match criteria:

1. Click the class link.

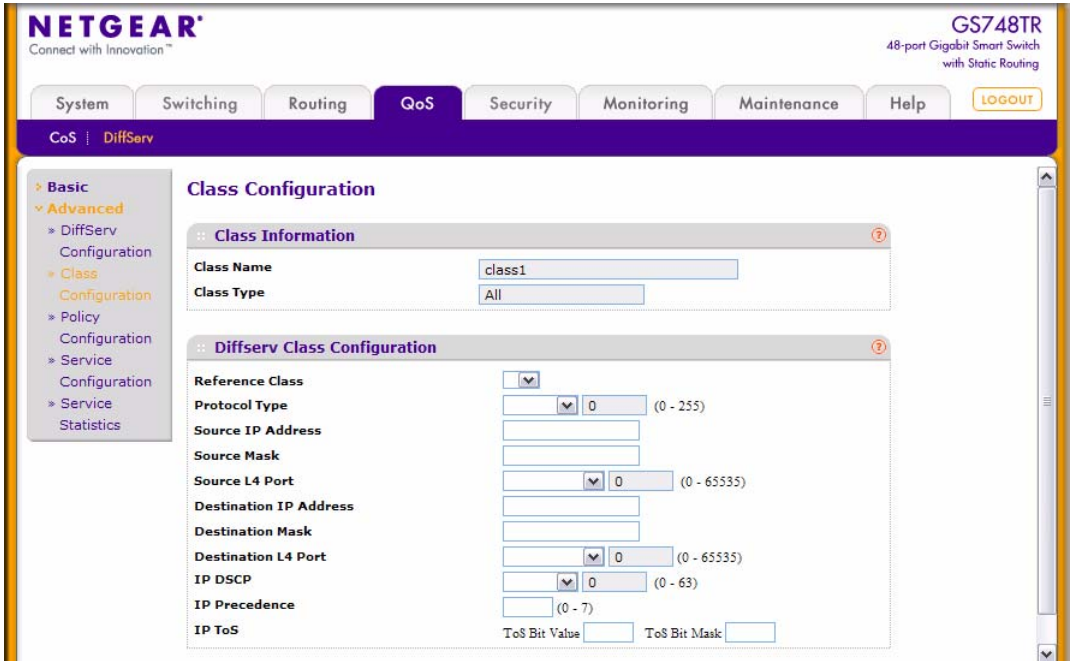


Figure 5-8

Table 5-8. Diffserv Class Configuration Fields

Field	Description
Reference Class	Selects a class to start referencing for criteria. If the specified class references another class, the Reference Class match criterion disappears from the match list to prevent you adding another class reference, since a specified class can reference at most one other class of the same type. Additionally, a **Remove Class Reference** button appears on the screen. Click the button to remove the current class reference.
Protocol Type	Requires a packet's layer 4 protocol to match the protocol you select. If you select Other, enter a protocol number in the field that appears. The valid range is 0-255.

Table 5-8. Diffserv Class Configuration Fields

Field	Description
Source IP Address	Requires a packet's source port IP address to match the address listed here. In the **IP Address** field, enter a valid source IP address in dotted decimal format.
Source Mask	Enter a valid subnet mask to determine which bits in the IP address are significant. Note that this is *not* a wildcard mask.
Source L4 Port	Requires a packet's TCP/UDP source port to match the port you select. Select the desired L4 keyword from the list on which the rule can be based. If you select Other, the screen refreshes and a Port ID field appears. Enter a user-defined Port ID by which packets are matched to the rule.
Destination IP Address	Requires a packet's destination port IP address to match the address listed here. In the **IP Address** field, enter a valid destination IP address in dotted decimal format.
Destination Mask	Enter a valid subnet mask to determine which bits in the IP address are significant. Note that this is *not* a wildcard mask.
Destination L4 Port	Requires a packet's TCP/UDP destination port to match the port you select. Select the desired L4 keyword from the list on which the rule can be based. If you select Other, the screen refreshes and a Port ID field appears. Enter a user-defined Port ID by which packets are matched to the rule.
IP DSCP	Matches the packet's DSCP to the class criteria's when selected. Select the DSCP type from the dropdown menu. or enter a DSCP value to match. If you select Other, enter a custom value in the **DSCP Value** field that appears.
IP Precedence	Matches the packet's IP Precedence value to the class criteria's when Enter a value in the range of 0-7.
IP TOS	Matches the packet's Type of Service bits in the IP header to the class criteria's when selected and a value is entered. In the **TOS Bits** field, enter a two-digit hexadecimal number to match the bits in a packet's TOS field. In the **TOS Mask** field, specify the bit positions that are used for comparison against the IP TOS field in a packet.

2. Click **Refresh** to refresh the page with the most current data from the switch.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Policy Configuration

Use the Policy Configuration page to associate a collection of classes with one or more policy statements.

To display the page:

1. Click **QoS > DiffServ** tab and then click the **Advanced > Policy Configuration** link.

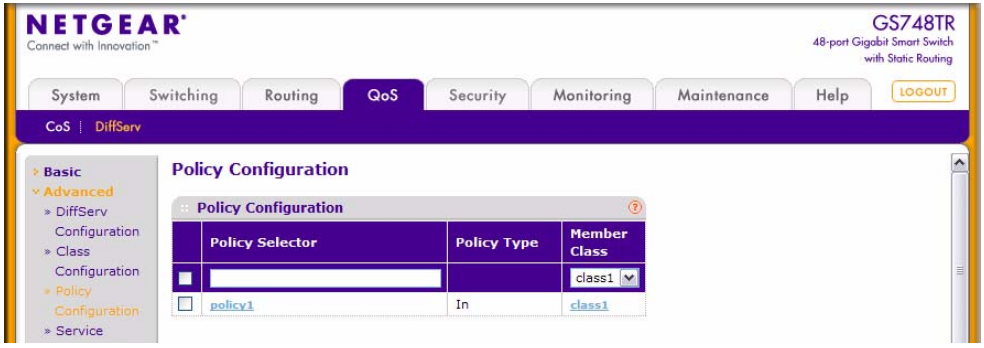


Figure 5-9

Table 5-9. Policy Configuration Fields

Field	Description
Policy Selector	To create a new policy, enter a policy name into the Policy Selector field and click **Add**. To modify or delete a policy, select the check box associated with the policy and either modify the fields and click **Apply** or click **Delete** to remove the policy.
Policy Type	The available policy type is *In*, which indicates the type is specific to inbound traffic. This field is not configurable.
Member Class	The menu lists all DiffServ classes that have been added to the policy names. To remove a DiffServ class from a policy, select the name of the class from the list, and then click **Delete**.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

To configure the policy attributes:

1. Click the name of the policy.

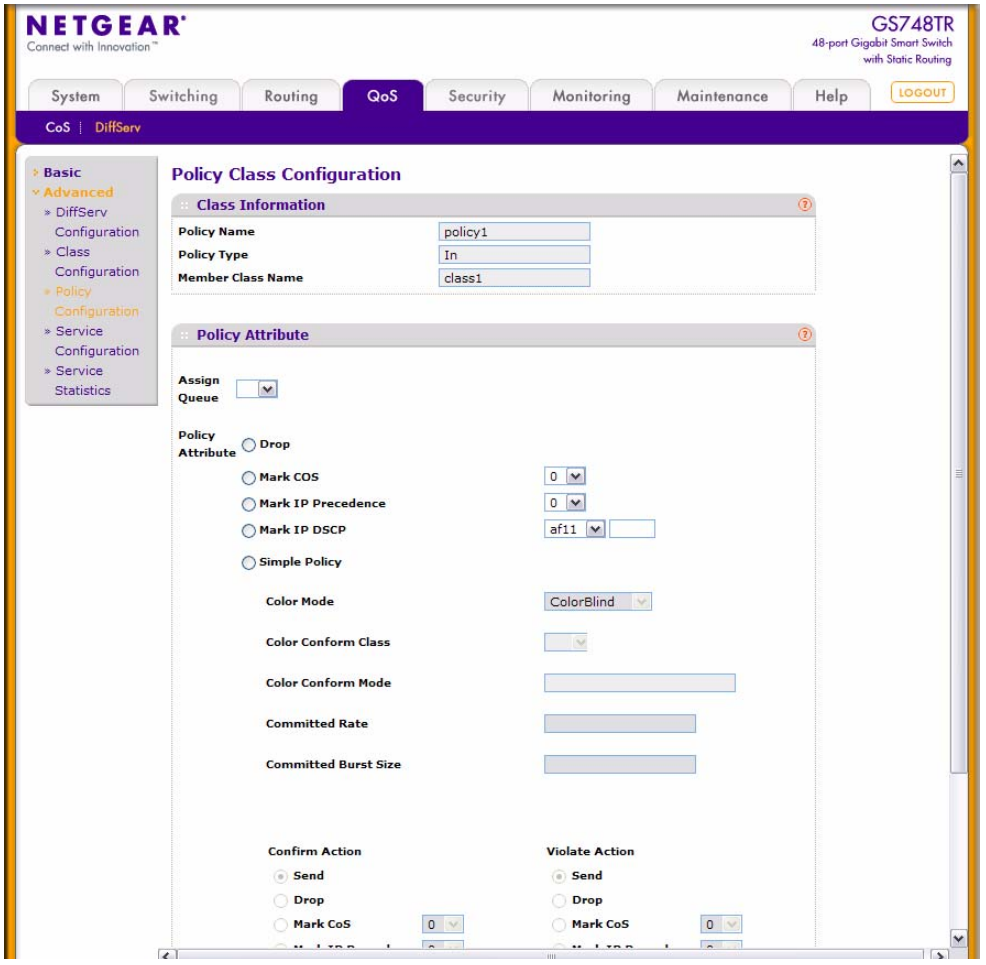


Figure 5-10

Table 5-10. Policy Attributes Fields

Field	Description
Assign Queue	• Assigns the packets of this policy-class to a queue. Enter an integer from 0-7 in the **Queue Id Value** field.
Policy Attribute	Select a policy attribute, which can be one of the following: • **Drop**: Select this field to drop packets for this policy-class. There are no fields to configure. • **Mark CoS**: Enter the specified Class of Service queue number to mark all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7. • **Mark IP Precedence**: Use this attribute to mark all packets for the associated traffic stream with the IP Precedence value you enter in the **IP Precedence Value** field. • **Mark IP DSCP**: Use this attribute to mark all packets for the associated traffic stream with IP DSCP value you choose from the menu. • **Simple Policy:** The next row describes the Simple Policy and its associated fields.

Table 5-10. Policy Attributes Fields (continued)

Field	Description
Simple Policy	Use this attribute to establish the traffic policing style for the specified class. The simple form of the policy command uses a single data rate and burst size, resulting in two outcomes: confirm and violate. The Simple Policy attribute configuration page has the following configurable fields: • **Color Mode**: Color Aware mode requires the existence of one or more color classes that are valid for use with this policy instance; otherwise, the color mode is color blind, which is the default. • **Color Conform Class**: A valid color class contains a single, non-excluded match criterion for one of the following fields (provided the field does not conflict with the classifier of the policy instance itself): - CoS - IP DSCP - IP Precedence - Secondary CoS • **Color Conform Mode:** The match-criteria of the color Conform class. • **Committed Rate:** The committed rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. • **Committed Burst Size:** The committed burst size is specified in kilobytes (KB) and is an integer from 1 to 128. -

Table 5-10. Policy Attributes Fields (continued)

Field	Description
	• **Conform Action**: Determines what happens to packets that are considered conforming (below the police rate). Select one of the following actions: - **Send**: (default) These packets are presented unmodified by DiffServ to the system forwarding element. - **Drop**: These packets are immediately dropped. - **Mark CoS**: These packets are marked by DiffServ with the specified CoS value before being presented to the system forwarding element. This selection requires that the Mark CoS value field be set. - **Mark IP Precedence**: These packets are marked by DiffServ with the specified IP Precedence value before being presented to the system forwarding element. This selection requires that the Mark IP Precedence value field be set. - **Mark IP DSCP**: These packets are marked by DiffServ with the specified DSCP value before being presented to the system forwarding element. This selection requires that the DSCP value field be set. • **Violate Action:** Determines what happens to packets that are considered non-conforming (above the police rate). Select one of the following actions: - **Send**: (default) These packets are presented unmodified by DiffServ to the system forwarding element. - **Drop**: (default) These packets are immediately dropped. - **Mark CoS**: These packets are marked by DiffServ with the specified CoS value before being presented to the system forwarding element. This selection requires that the Mark CoS value field be set. - **Mark IP Precedence**: These packets are marked by DiffServ with the specified IP Precedence value before being presented to the system forwarding element. This selection requires that the Mark IP Precedence value field be set. - **Mark IP DSCP**: These packets are marked by DiffServ with the specified DSCP value before being presented to the system forwarding element. This selection requires that the DSCP value field be set.

2. Click **Refresh** to refresh the page with the most current data from the switch.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Service Configuration

Use the Service Configuration page to activate a policy on a port.

To display the page:

1. Click the **QoS** > **DiffServ** tab and then click the **Advanced** > **Service Configuration** link.

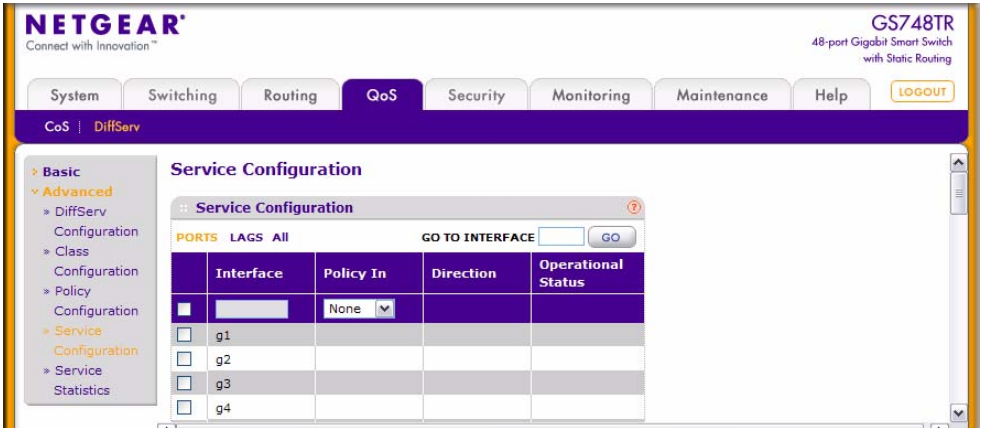


Figure 5-11

Table 5-11. Service Configuration Fields

Field	Description
Interface	Selects the interface (physical, LAG, or All) to be affected from dropdown menus. Select the check box in the heading row to configure all interfaces with the same setting. Select the check box next to an individual port to configure a single interface
Policy In	Selects the policy to be associated with the port from a dropdown menu.
Direction	Shows that the traffic direction of this service interface, which is always *In*.
Operational Status	Shows the operational status of this service interface, which is either Up or Down.

2. To activate a policy on an interface, select the interface and the policy, and then click **Apply**.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. To display the list of Ports, click PORTS as shown in Figure 5-11.
5. To display the list of LAGs, click **LAGS** as shown in Figure 5-12.

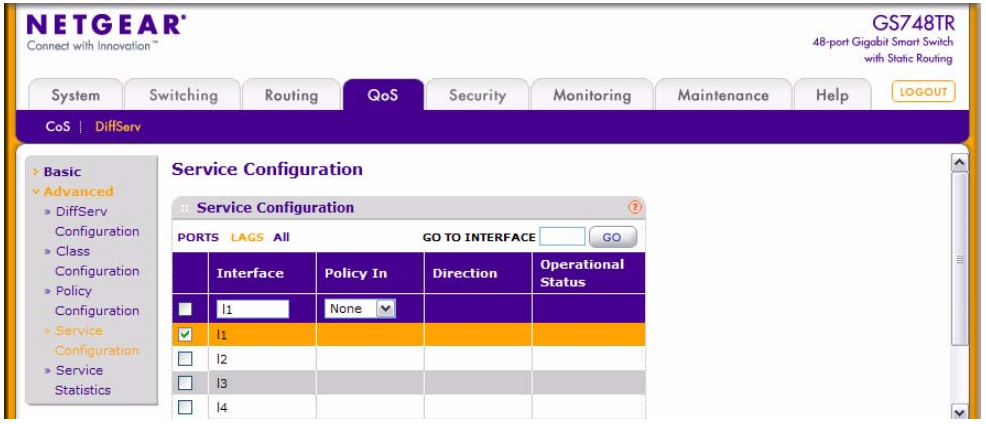


Figure 5-12

To go to an interface in the list:

1. Type the interface number in the **Go To Interface** field and click **Go** as shown in Figure 5-13.

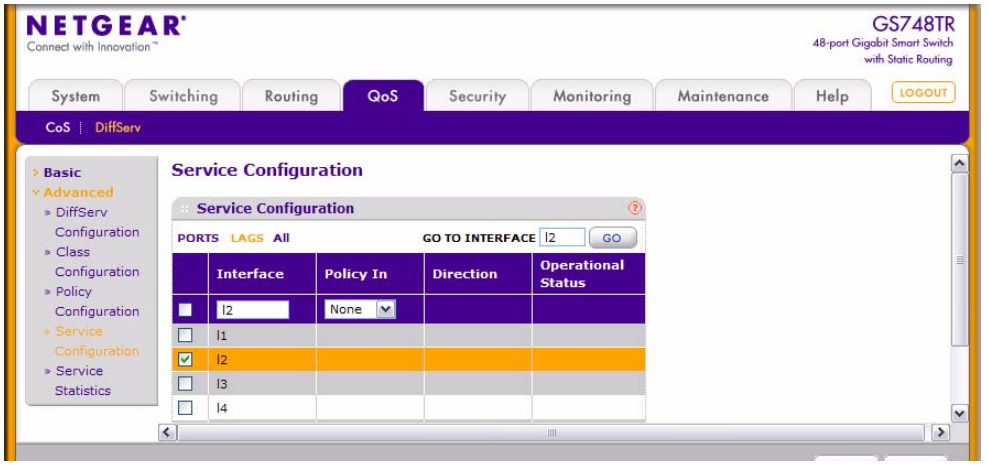


Figure 5-13

Service Statistics

Use the Service Statistics page to display service-level statistical information about all interfaces that have DiffServ policies attached.

To display the page:

1. Click the **QoS** > **DiffServ** tab and then click the **Advanced** > **Service Statistics** link.

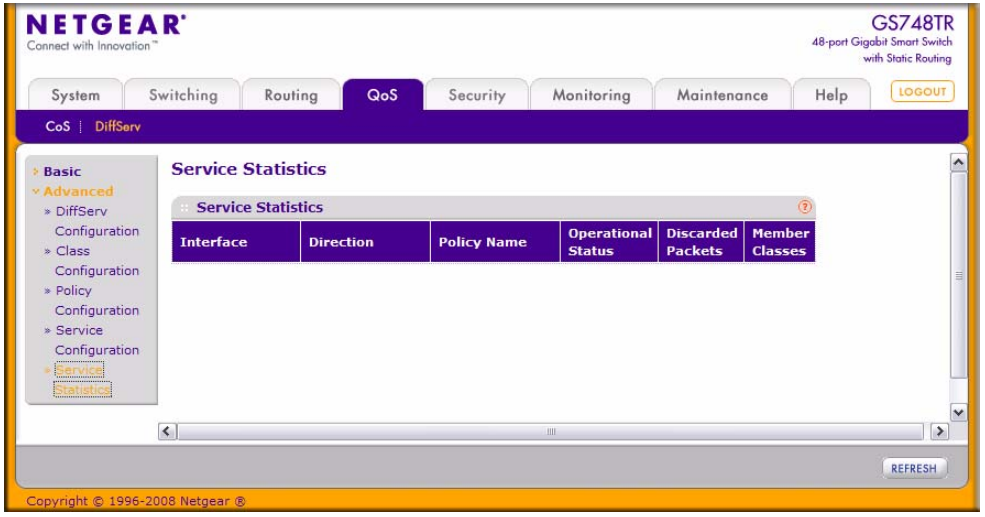


Figure 5-14

Table 5-12. Service Statistics Fields

Field	Description
Interface	Shows the interface for which service statistics are to display.
Direction	Shows the direction of packets for which service statistics display, which is always *In*.
Policy Name	Displays the policy associated with the selected interface.
Operational Status	Shows the operational status of this service interface, which is either Up or Down.
Discarded Packets	Shows the total number of packets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.
Member Classes	Selects the member class for which octet statistics are to display.

2. Click **Refresh** to update the page with the most current information.

Chapter 6
Managing Device Security

Use the features available from the Security tab to set management security parameters for port, user, and server security.

The Security folder contains links to the following features:

- "Management Security Settings"
- "Configuring Management Access"
- "Port Authentication"
- "Traffic Control"
- "Configuring Access Control Lists"

Management Security Settings

From the **Management Security Settings** page, you can configure the login password, Remote Authorization Dial-In User Service (RADIUS) settings, Terminal Access Controller Access Control System (TACACS+) settings, and authentication lists.

To display the page, click the **Security > Management Security** tab. The Management Security folder contains links to the following features:

- "Change Password" on page 6-1
- "RADIUS Configuration" on page 6-2
- "Configuring TACACS+" on page 6-10
- "Authentication List Configuration" on page 6-13

Change Password

Use the page to change the login password. To display the page:

1. click **Security > Management Security > User Configuration > Change Password** in the navigation tree.

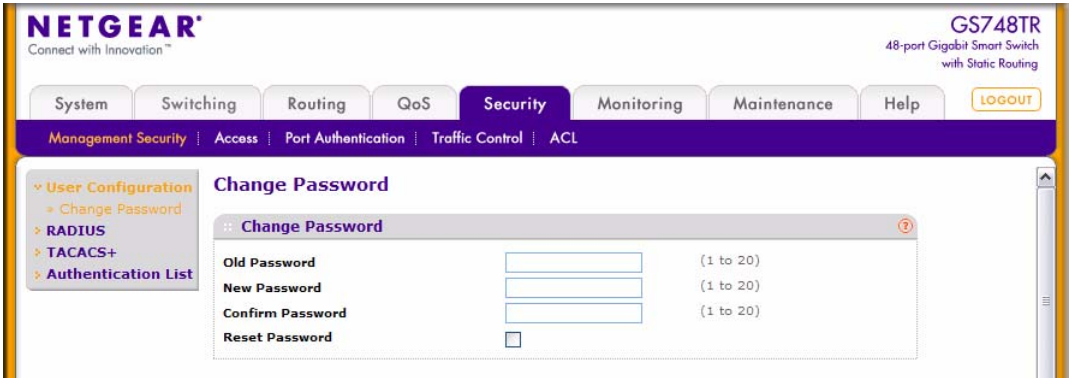


Figure 6-1

Table 6-1. User Accounts Fields

Field	Description
Old Password	Specify the current password for the account created by the user. The entered password will be displayed in asterisks (*). Passwords are one to 20 alphanumeric characters in length and are case sensitive.
New Password	Enter the optional new or changed password for the account. It will not display as it is typed, and only asterisks (*) will show on the screen. Passwords are one to 20 alphanumeric characters in length and are case sensitive.
Confirm Password	Enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (*)
Reset Password	Use this field to reset the password to the default value.

Note: In the case of a lost password, the user has to reset the button on the front panel for more than one second to restore the factory default.

RADIUS Configuration

RADIUS servers provide additional security for networks. The RADIUS server maintains a user database, which contains per-user authentication information. RADIUS servers provide a centralized authentication method for:

- Web Access

- Access Control Port (802.1X)

The RADIUS folder contains links to the following features:

- “Global Configuration” on page 6-3
- “Server Configuration” on page 6-5
- “Accounting Server Configuration” on page 6-7

Global Configuration

Use the RADIUS Configuration page to add information about one or more RADIUS servers on the network.

To access the RADIUS Configuration page:

1. Click **Security > Management Security**, and then click the **RADIUS > Global Configuration** in the navigation tree.

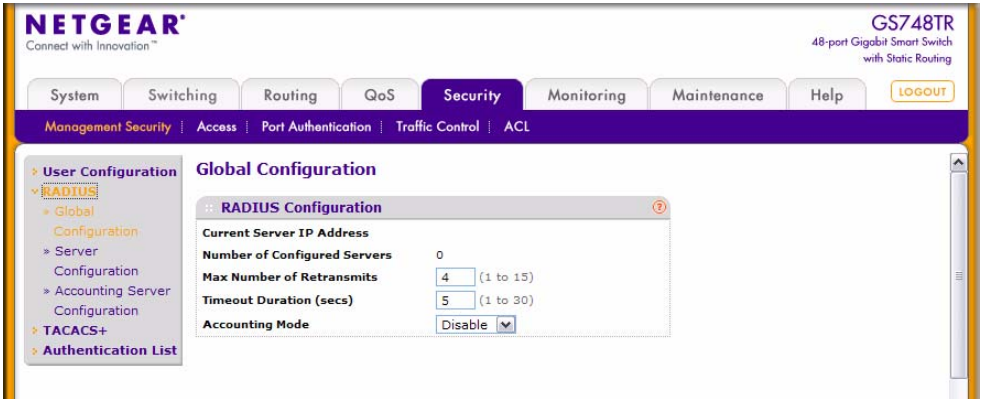


Figure 6-2

Table 6-2. RADIUS Configuration Fields

Field	Description
Current Server IP Address	Shows the IP address of the current server. This field is blank if no servers are configured. If more than one RADIUS servers are configured, the current server is the server configured as the primary server. If no servers are configured as the primary server, the current server is the most recently added RADIUS server.
Number of Configured Servers	The number of RADIUS servers that have been configured. This value will be in the range of 0 and 3.
Max Number of Retransmits	The value of the maximum number of times a request packet is retransmitted. The valid range is 1-15. Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.
Timeout Duration (secs)	The timeout value, in seconds, for request retransmissions. The valid range is 1 - 30. Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.
Accounting Mode	Use the dropdown menu to select whether the RADIUS accounting mode is enabled or disabled on the current server.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make changes to the page, click **Apply** to apply the changes to the system.

Server Configuration

Use the RADIUS Server Configuration page to view and configure various settings for the current RADIUS server configured on the system.

To access the RADIUS Server Configuration page:

1. Click **Security > Management Security**, and then click the **RADIUS** > **Server Configuration** link.

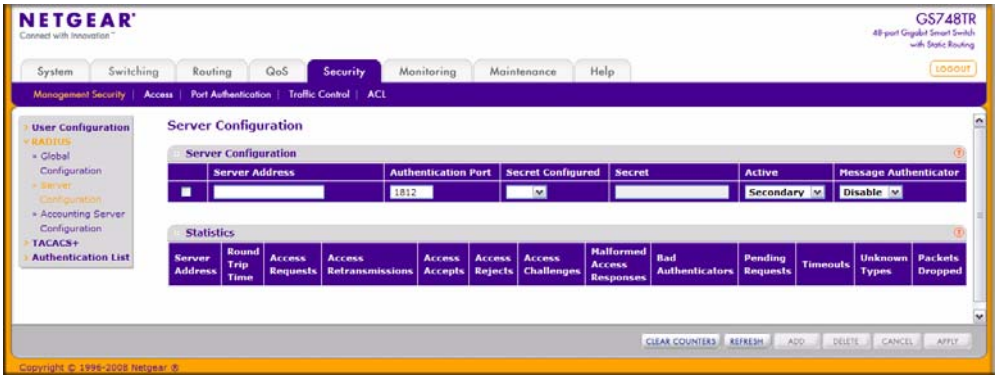


Figure 6-3

Table 6-3. RADIUS Server Configuration Fields

Field	Description
Server Address	Enter the IP address of the RADIUS server to add. To modify settings for a RADIUS server that is already configured on the switch, select the check box next to the server address.
Authentication Port	Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port, and the valid range is 0-65535.
Secret Configured	You can only enter a RADIUS secret if you select Yes from the menu. After you add the RADIUS server, this field indicates whether the shared secret for this server has been configured.
Secret	Shared secret text string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This secret must match the RADIUS encryption.
Active	Sets the selected server to the **Primary** or **Secondary** server.
Message Authenticator	**Enable** or **disable** the message authenticator attribute for the selected server.

2. Click **Refresh** to update the page with the most current information.
3. To add a RADIUS server, enter information about the server into the appropriate fields and click **Add**.
4. To delete a configured RADIUS server, select the check box next to the server address, and then click **Delete**.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. If you make changes to the page, click **Apply** to apply the changes to the system.

Table 6-4. RADIUS Server Statistics Fields

Field	Description
Server Address	Use the dropdown menu to select the IP address of the RADIUS server for which to display statistics.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access-responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.

Table 6-4. RADIUS Server Statistics Fields (continued)

Field	Description
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

7. Click **Clear Counters** to clear the authentication server and RADIUS statistics to their default values.
8. Click **Refresh** to refresh the page with the most current data from the switch.

Accounting Server Configuration

Use the RADIUS Accounting Server Configuration page to view and configure various settings for one or more RADIUS accounting servers on the network.

To access the RADIUS Accounting Server Configuration page:

1. Click **Security > Management Security**, and then click the **RADIUS** > **Accounting Server Configuration** in the navigation tree.

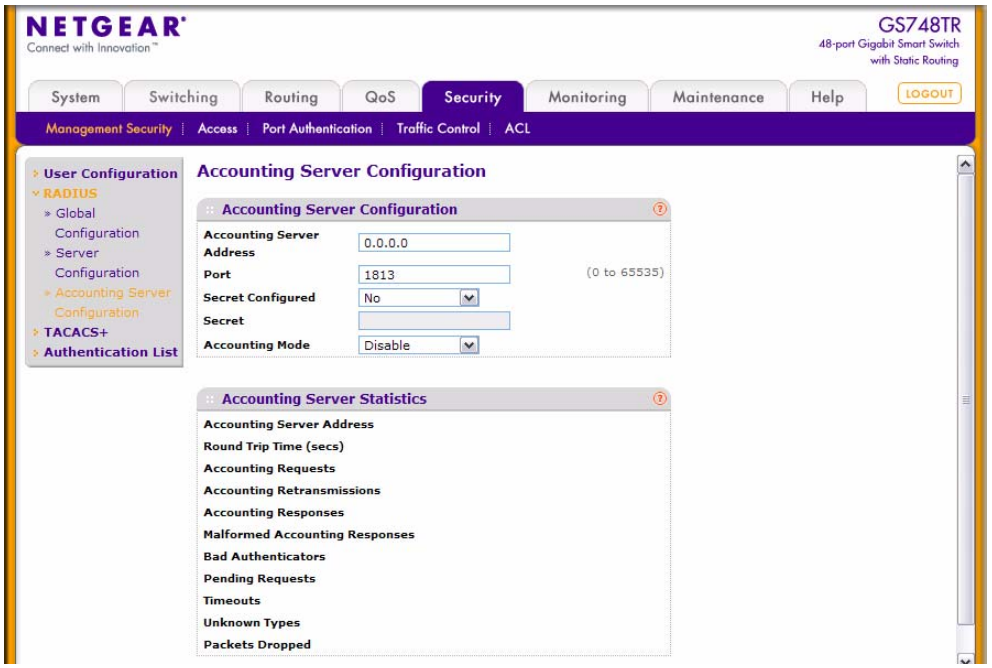


Figure 6-4

Table 6-5. RADIUS Accounting Server Configuration Fields

Field	Description
Accounting Server Address	Enter the IP address of the RADIUS accounting server to add.
Port	Identifies the authentication port the server uses to verify the RADIUS accounting server authentication. The port is a UDP port, and the valid range is 0-65535.
Secret Configured	Indicates whether the shared secret for this server has been configured. The Secret field is only available if you select Yes.
Secret	Specifies the shared secret to use with the specified accounting server. This field is only displayed if the user has READWRITE access.
Accounting Mode	Use the menu to enable or disable the RADIUS accounting mode.

2. Click **Refresh** to update the page with the most current information.
3. To delete a configured RADIUS Accounting server, click **Delete**.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

To add a RADIUS Accounting server:

1. Enter information about the server into the appropriate fields and click **Apply**.

Table 6-6. RADIUS Accounting Server Fields

Field	Description
Accounting Server Address	Select the IP address of the RADIUS accounting server for which to display statistics.
Round Trip Time (secs)	Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Accounting Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Accounting Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this server.
Accounting Responses	Displays the number of RADIUS packets received on the accounting port from this server.
Malformed Accounting Responses	Displays the number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	Displays the number of RADIUS Accounting-Response packets that contained invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

2. Click **Clear Counters** to reset all statistics to their default value.
3. Click **Refresh** to update the page with the most current information.

Configuring TACACS+

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

- **Authentication**: Provides authentication during login and via user names and user-defined passwords.
- **Authorization**: Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS+ server checks the user privileges.

The TACACS+ protocol ensures network security through encrypted protocol exchanges between the device and TACACS+ server.

The TACACS+ folder contains links to the following features:

- "Configuring TACACS+" on page 6-10
- "Server Configuration" on page 6-11

TACACS+ Configuration

The TACACS+ Configuration page contains the TACACS+ settings for communication between the switch and the TACACS+ server you configure via the inband management port.

To display the TACACS+ Configuration page:

1. Click **Security > Management Security**, and then click the **TACACS+** > **TACACS+ Configuration** link.

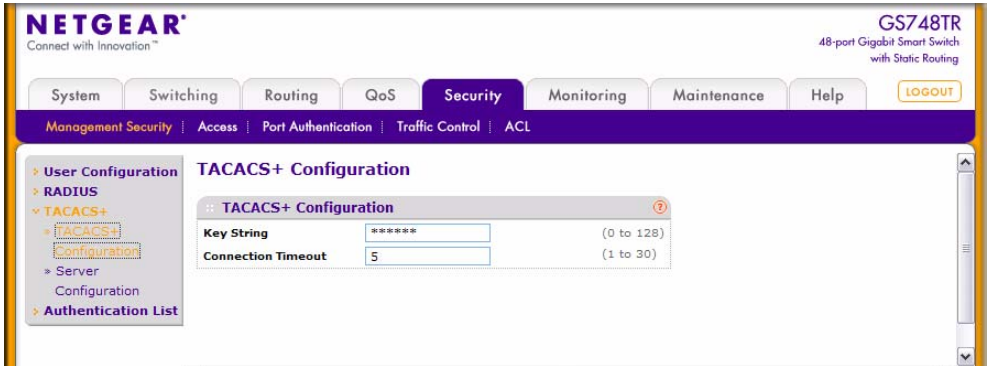


Figure 6-5

Table 6-7. TACACS+ Configuration Fields

Field	Description
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The valid range is 0-128 characters. The key must match the key configured on the TACACS+ server.
Connection Timeout	The maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server. The valid range is 1 -30.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make any changes to the page, click **Apply** to apply the new settings to the system.

Server Configuration

Use the TACACS+ Server Configuration page to configure up to five TACACS+ servers with which the switch can communicate.

To display the TACACS+ Server Configuration page:

1. Click **Security > Management Security**, and then click the **TACACS+** > **Server Configuration** link.

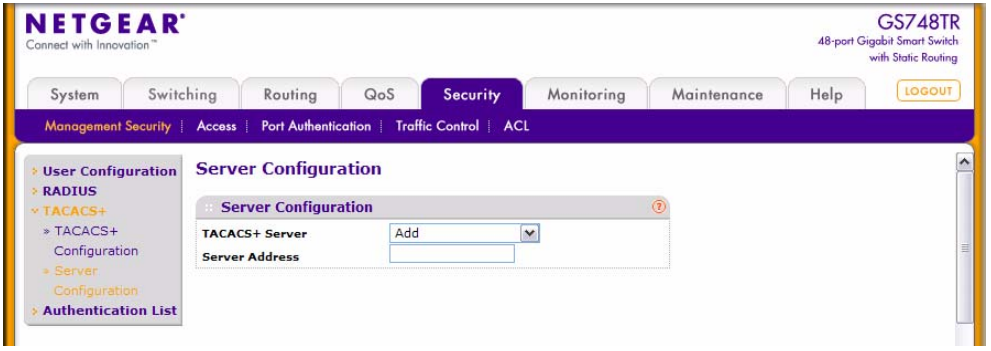


Figure 6-6

Table 6-8. TACACS+ Configuration Fields

Field	Description
TACACS+ Server	Use the dropdown menu to select the IP address of the TACACS+ server to view or configure. If fewer than five TACACS+ servers are configured on the system, the Add option is also available. Select Add to configure additional TACACS+ servers.
Server Address	Enter the IP address of the TACACS+ server to add. This field is only available when Add is selected in the **TACACS+ Server IP Address** field.

After you add one or more TACACS+ servers, additional fields appear on the **TACACS+** Server Configuration page.

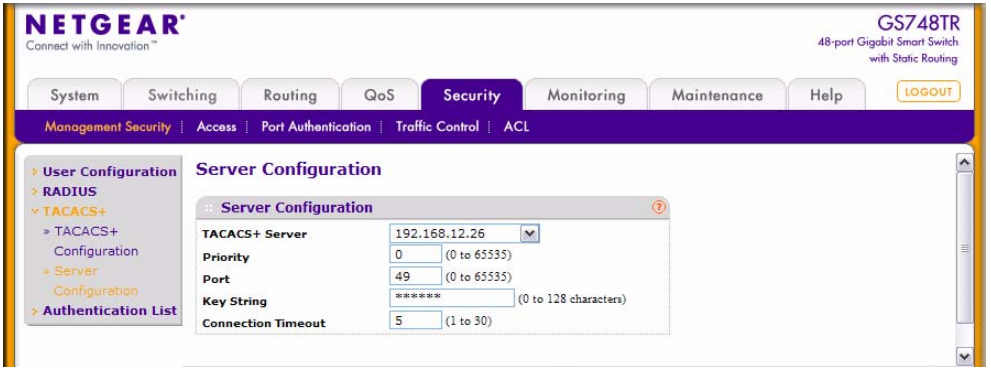


Figure 6-7

Table 6-9. TACACS+ Configuration Fields

Field	Description
TACACS+ Server	Use the dropdown menu to select the IP address of the TACACS+ server to view or configure. If fewer than five RADIUS servers are configured on the system, the Add option is also available. Select Add to configure additional RADIUS servers.
Priority	Specifies the order in which the TACACS+ servers are used. The valid range 0-65535.
Port	The authentication port number through which the TACACS+ session occurs. The default is port 49, and the range is 0-65535.

Table 6-9. TACACS+ Configuration Fields (continued)

Field	Description
Key String	Defines the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ server. The valid range is 0-128 characters.
Connection Timeout	The amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is from 1 to 30 seconds.

2. If you make changes to the page, or add a new entry, click **Apply** to apply the changes to the system.
3. To delete a configured TACACS+ server, select the IP address of the server from the **TACACS+ Server IP Address** dropdown menu, and then click **Delete**.

Authentication List Configuration

Use the Authentication List page to configure login lists. A login list specifies one or more authentication methods to validate switch or port access for the admin user.

Note: Admin is the only user on the system and is assigned to a pre-configured list named defaultList, which you cannot delete. You can add **admin** to other lists or configure the defaultList with other settings.

To access the Authentication List page:

1. Click **Security** > **Management Security**, and then click the **Authentication List** link.

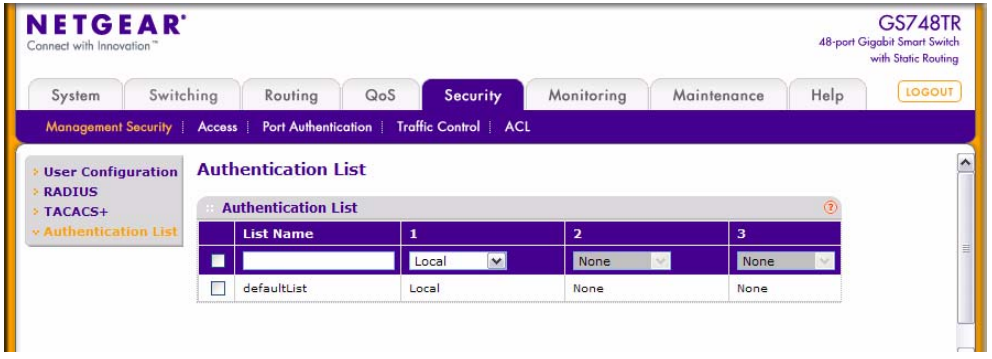


Figure 6-8

Table 6-10. Authentication Profile Fields

Field	Description
List Name	The menu allows you to select an existing list to view or configure. If you are creating a new login authentication list, enter the name you want to assign. The name can be up to 15 alphanumeric characters in length and is not case sensitive. Click **Apply** to create the new list name.
1	Use the dropdown menu to select the authentication method that should appear first in the selected authentication login list. If you select a method that does not time out as the first method, such as 'local', no other method will be tried, even if you have specified more than one method. Note that this parameter will not appear when you first create a new login list. User authentication occurs in the order the methods are selected. Possible methods are as follows: • **Local:** The user's locally stored ID and password will be used for authentication. Since the local method does not time out, if you select this option as the first method, no other method will be tried, even if you have specified more than one method. • **RADIUS:** The user's ID and password will be authenticated using the RADIUS server. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user. • **TACACS+:** The user's ID and password will be authenticated using the TACACS+ server. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2. • **None:** The authentication method is unspecified. This option is only available for Method 2 and Method 3.
2	Use the menu to select the authentication method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. Note that this parameter will not appear when you first create a new login list.
3	Use the menu to select the authentication method, if any, that should appear third in the selected authentication login list. Note that this parameter will not appear when you first create a new login list.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. If you make changes to the page, click **Apply** to apply the changes to the system.

Configuring Management Access

From the Access page, you can configure HTTP and Secure HTTP access to the GS700TR. You can also configure Access Control Profiles and Access Rules.

The **Security > Access** tab contains the following folders:

HTTP Configuration

Use the HTTP Configuration page to configure the HTTP server settings on the system.

To access the HTTP Configuration page:

1. Click the **Security** tab, then click **Access**, and then click the **HTTP > HTTP Configuration** link.

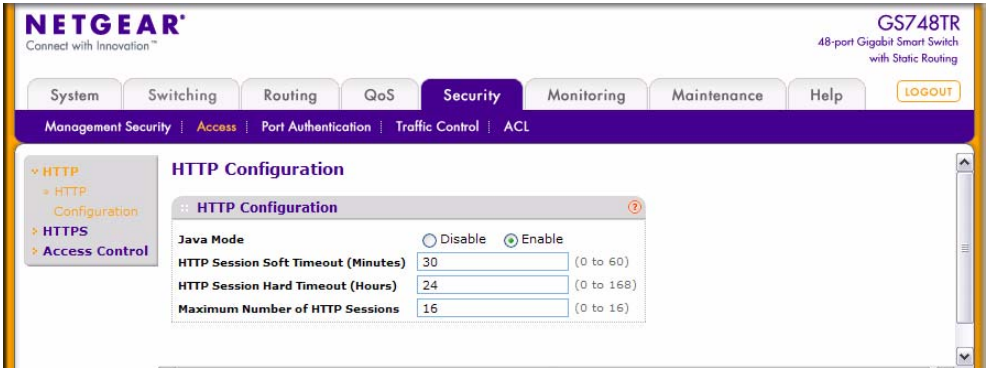


Figure 6-9

Table 6-11. HTTP Configuration Fields

Field	Description
Java Mode	This select field is used to **Enable** or **Disable** the web Java Mode. This applies to both secure and un-secure HTTP connections. The currently configured value is shown when the web page is displayed. The default value is Enable.
HTTP Session Soft Timeout	This field is used to set the inactivity timeout for HTTP sessions. The value must be in the range of (0 to 60) minutes. A value of zero corresponds to an infinite timeout. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.
HTTP Session Hard Timeout	This field is used to set the hard timeout for HTTP sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (0 to 168) hours. A value of zero corresponds to an infinite timeout. The default value is 24 hours. The currently configured value is shown when the web page is displayed.
Maximum Number of HTTP Sessions	This field is used to set the maximum allowable number of HTTP sessions. The value must be in the range of (0 to 16). The default value is 16. The currently configured value is shown when the web page is displayed.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make changes to the page, click **Apply** to apply the changes to the system.

Secure HTTP Configuration

Secure HTTP enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. When you manage the switch by using a Web interface, secure HTTP can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks.

Use the Secure HTTP Configuration page to configure the settings for HTTPS communication between the management station and the switch.

To display the Secure HTTP Configuration page:

1. Click **Security** > **Access**, and then click the **HTTPS** > **HTTPS Configuration** link.

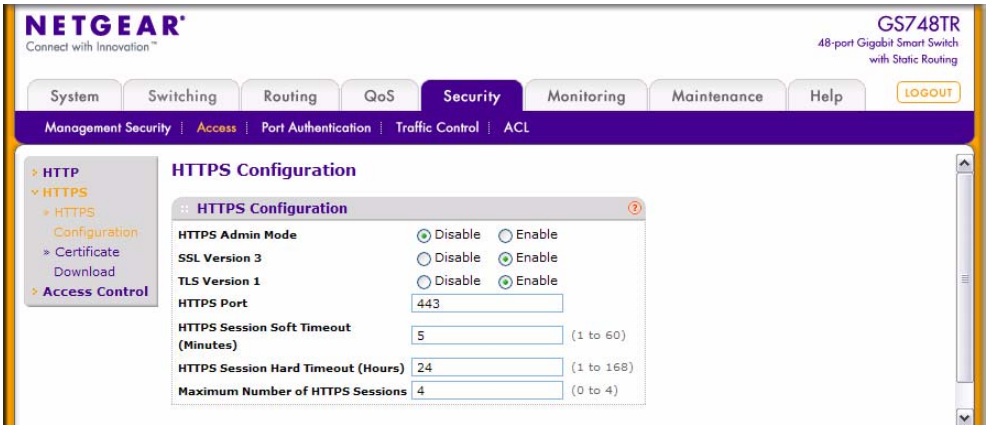


Figure 6-10

Table 6-12. Secure HTTP Configuration Fields

Field	Description
HTTPS Admin Mode	Enables or Disables the Administrative Mode of Secure HTTP. The currently configured value is shown when the web page is displayed. The default value is Disable. You can only download SSL certificates when the HTTPS Admin mode is disabled.
SSL Version 3	Enables or Disables Secure Sockets Layer Version 3.0. The currently configured value is shown when the web page is displayed. The default value is Enable.
TLS Version 1	Enables or Disables Transport Layer Security Version 1.0. The currently configured value is shown when the web page is displayed. The default value is Enable.
HTTPS Port	Sets the HTTPS Port Number. The value must be in the range of 1 to 65535. Port 443 is the default value. The currently configured value is shown when the web page is displayed.
HTTPS Session Soft Timeout	Sets the inactivity timeout for HTTPS sessions. The value must be in the range of (1 to 60) minutes. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.

Table 6-12. Secure HTTP Configuration Fields (continued)

Field	Description
HTTPS Session Hard Timeout	Sets the hard timeout for HTTPS sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (1 to 168) hours. The default value is 24 hours. The currently configured value is shown when the web page is displayed.
Maximum Number of HTTPS Sessions	Sets the maximum allowable number of HTTPS sessions. The value must be in the range of (0 to 4). The default value is 4. The currently configured value is shown when the web page is displayed.

Certificate Download

For the Web server on the switch to accept HTTPS connections from a management station, the Web server needs a public key certificate. You can generate a certificate externally (i.e., off-line) and download it to the switch.

To display the Certificate Download page, click **Security** > **Access**, and then click the **HTTPS** > **Certificate Download** link.

Downloading SSL Certificates. Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.

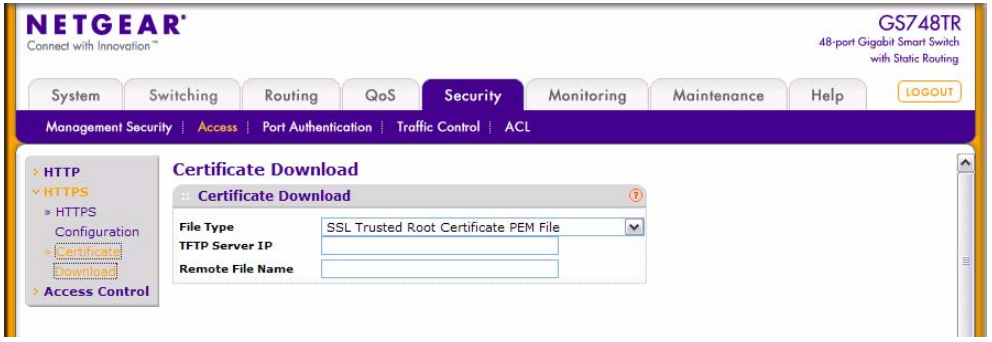


Figure 6-11

Table 6-13. Certificate Download Fields

Field	Description
File Type	Select the type of SSL certificate to download, which can be one of the following: • **SSL Trusted Root Certificate PEM File**: SSL Trusted Root Certificate File (PEM Encoded). • **SSL Server Certificate PEM File**: SSL Server Certificate File (PEM Encoded). • **SSL DH Weak Encryption Parameter PEM File**: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded). • **SSL DH Strong Encryption Parameter PEM File**: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
TFTP Server IP	Enter the IP address of the TFTP server in the form of an IP address in x.x.x.x format or a hostname starting with a letter of the alphabet. The factory default is 0.0.0.0. Make sure that the software image or other file to be downloaded is available on the TFTP server.
Remote File Name	Enter the name of the file to download. You may enter up to 32 characters. The factory default is blank.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Access Profile Configuration

Use the Access Profile Configuration page to configure settings that control management access to the switch.

To access the Access Profile Configuration page:

1. Click **Security** > **Access**, and then click the **Access Control** > **Access Profile Configuration** link.

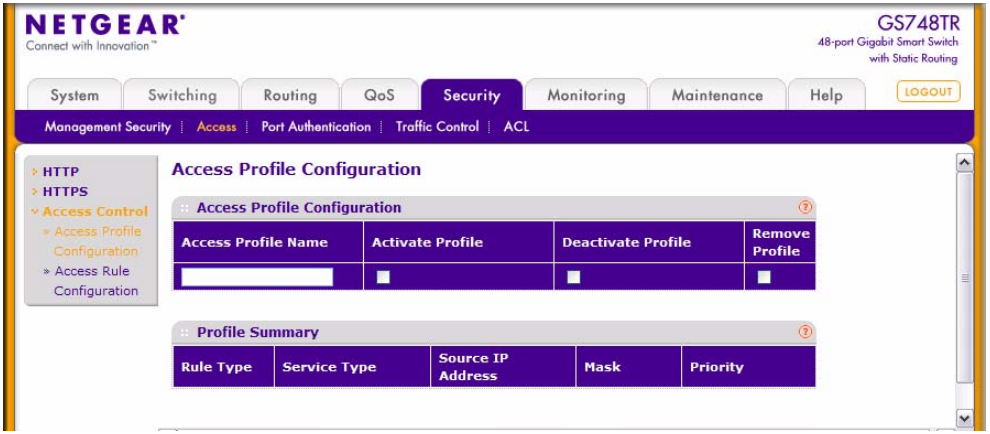


Figure 6-12

Table 6-14. Access Profile Configuration Fields

Field	Description
Access Profile Name	Enter the name of the access profile to be added. Maximum length is 32 characters.
Activate Profile	Select the check box to activate an access profile.
DeActivate Profile	Select the check box to de-activate an access profile
Remove Profile	Select the check box to remove an access profile. The access profile should be de-activated before removing the access profile.

The following table shows the fields in the Profile Summary table.

Table 6-15. Profile Summary Fields

Field	Description
Rule Type	Identifies the action the rule takes, which is either Permit or Deny.
Service Type	Shows the type of service to allow or prohibit from accessing the switch management interface: • None • SNMP • HTTP • HTTPS

Table 6-15. Profile Summary Fields (continued)

Field	Description
Source IP Address	Shows the IP Address of the client that may or may not originate management traffic.
Mask	Shows the subnet mask associated with the IP address.
Priority	Shows the priority of the rule. The rules are validated against the incoming management request in the ascending order of their priorities. If a rule matches, action is performed and subsequent rules below are ignored.

2. Click **Refresh** to update the page with the most current information.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Access Rule Configuration

Use the Access Rule Configuration page to configure the rules about what systems can access the GS700TR Web interface and what protocols are allowed.

To access the Access Rule Configuration page:

1. Click **Security** > **Access**, and then click the **Access Control > Access Rule Configuration** link.

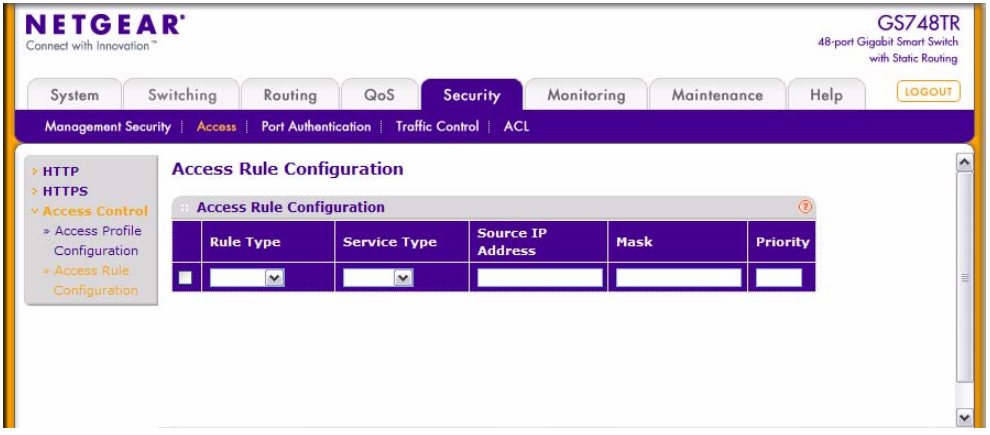


Figure 6-13

Table 6-16. Access Rule Configuration Fields

Field	Description
Rule Type	Select Permit to allow access to the switch administrative pages for traffic that meets the criteria you configure for the rule. Any traffic that does not meet the rules is denied. Select Deny to prohibit access to the switch administrative pages for traffic that meets the criteria you configure for the rule. Any traffic that does not meet the rules is allowed access to the switch.
Service Type	Select the type of service to allow or prohibit from accessing the switch management interface: • None • SNMP • HTTP • HTTPS
Source IP Address	Enter Source IP Address of the client originating the management traffic. Fill in the “Source IP address” in the text box provided.
Mask	Enter the subnet mask associated with the IP address.
Priority	Configure priority to the rule. The rules are validated against the incoming management request in the ascending order of their priorities. If a rule matches, action is performed and subsequent rules below are ignored. For example, if a Source IP 10.10.10.10 is configured with priority 1 to permit, and Source IP 10.10.10.10 is configured with priority 2 to Deny, then access is permitted if the profile is active, and the second rule is ignored.

2. To add an Access Rule, enter information into the appropriate fields and click **Add**.
3. To delete an Access Rule, select the check box next to the Rule Type, and then click **Delete**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make changes to the page, click **Apply** to apply the changes to the system.

Port Authentication

In port-based authentication mode, when 802.1X is enabled globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

The 802.1X network has three components:

- **Authenticators**: Specifies the port that is authenticated before permitting system access.
- **Supplicants**: Specifies the host connected to the authenticated port requesting access to the system services.
- **Authentication Server**: Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

The Port Authentication folder contains links to the following features:

- Basic:
  - “802.1X Configuration” on page 6-23
- Advanced:
  - “Port Authentication” on page 6-24
  - “Port Summary” on page 6-28

802.1X Configuration

Use the 802.1X Configuration page to enable or disable port access control on the system.

To display the 802.1X Configuration page:

1. Click **Security** > **Port Authentication**, then click **Basic** > **802.1X Configuration** in the navigation tree.

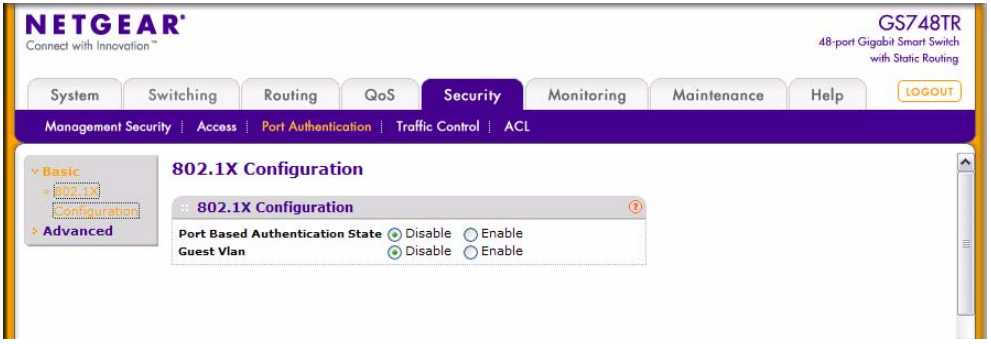


Figure 6-14

Table 6-17. Port Access Control—Port Configuration Fields

Field	Description
Port Based Authentication State	Select **Enable** or **Disable** 802.1X administrative mode on the switch. The default is **Disable**. This feature permits port-based authentication on the switch.
Guest VLAN	Select to **Enable** or **Disable** Guest VLAN Supplicant Mode. If enabled, when no 802.1X supplicant is authenticated on a port, the port still provide limited network access, as determined by a guest VLAN configured on authentication server. The default is **Disable**.

2. Click **Refresh** to refresh the page with the most current data from the switch.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you change the mode, click **Apply** to apply the new settings to the system.

Port Authentication

Use the Port Authentication page to enable and configure port access control on one or more ports.

To access the Port Authentication page:

1. Click **Security** > **Port Authentication**, and then click the **Advanced** > **Port Authentication** link.

Note: Use the horizontal scroll bar at the bottom of the browser to view all the fields on the Port Authentication page. Figure 6-15 and Figure 6-16 are both images of the Port Authentication page.

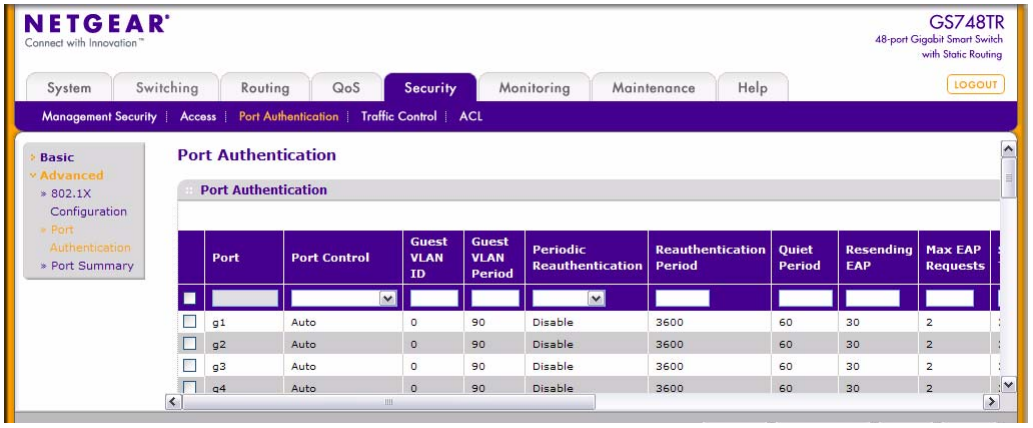


Figure 6-15

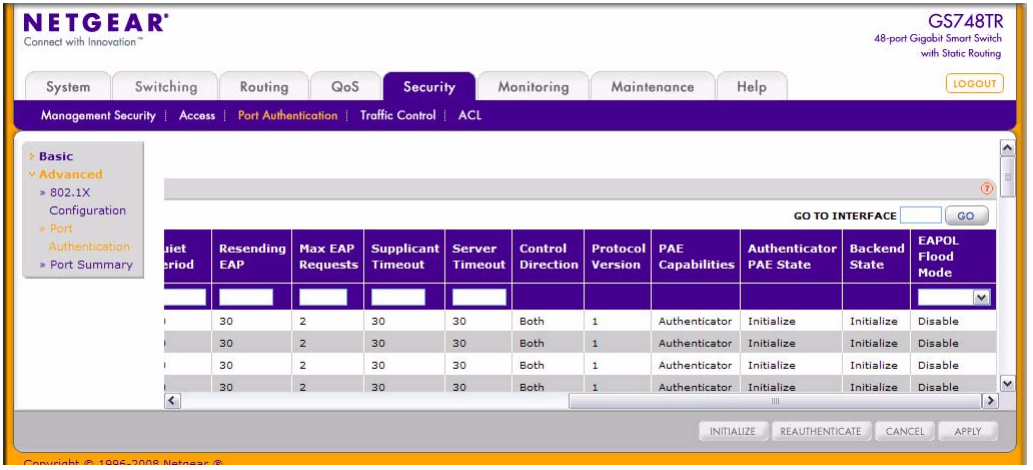


Figure 6-16

Table 6-18. Port Authentication Port Configuration Fields

Field	Description
Port	Selects the Unit and Port to configure.
Port Control	Defines the port authorization state. The control mode is only set if the link status of the port is link up. The possible field values are: • **Auto**: Automatically detects the mode of the interface. • **Authorized**: Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication. • **Unauthorized**: Denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface.
Guest VLAN ID	This field allows the user to configure Guest Vlan Id on the interface. The valid range is 0-4078.The default value is 0. Enter 0 to reset the Guest Vlan Id on the interface.
Guest VLAN Period	This input field allows the user to enter the guest Vlan period for the selected port. The guest Vlan period is the value, in seconds, of the timer used by the GuestVlan Authentication. The guest Vlan timeout must be a value in the range of 1 and 300. The default value is 90.
Periodic Reauthentication	Use this field to enable or disable reauthentication of the supplicant for the specified port. Selectable values are **Enable** and **Disable**. If the value is **Enable**, reauthentication will occur. Otherwise, reauthentication will not be allowed. The default value is **Disable**. Changing the selection will not change the configuration until the **Apply** button is pressed.
Reauthentication Period (secs)	Indicates the time span in which the selected port is reauthenticated. The field value is in seconds. The range is 1 - 65535, and the field default is 3600 seconds.
Quiet Period (secs)	Defines the amount of time that the switch remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field value is in seconds. The field default is 60 seconds.
Resending EAP	This input field allows you to configure the transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identify frame to the supplicant. The transmit period must be a number in the range of 1 to 65535. The default value is 30. Changing the value will not change the configuration until you click the **Apply** button.

Table 6-18. Port Authentication Port Configuration Fields (continued)

Field	Description
Max EAP Requests	This input field allows you to enter the maximum requests for the selected port. The maximum requests value is the maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The maximum requests value must be in the range of 1 to 10. The default value is 2. Changing the value will not change the configuration until you click the **Apply** button.
Supplicant Timeout (secs)	Defines the amount of time that lapses before EAP requests are resent to the user. The field value is in seconds. The field default is 30 seconds.
Server Timeout (secs)	Defines the amount of time that lapses before the switch resends a request to the authentication server. The field value is in seconds. The range is **1-65535**, and the field default is 30 seconds.
Control Direction	This displays the control direction for the specified port. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator. This affects whether the unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames) or just in the incoming direction (disabling only the reception of incoming frames). This field is not configurable on some platforms.
Protocol Version	This field displays the protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1X specification. This field is not configurable.
PAE Capabilities	This field displays the port access entity (PAE) functionality of the selected port. Possible values are **Authenticator** or **Supplicant**. This field is not configurable.
Authenticator PAE State	This field displays the current state of the authenticator PAE state machine. Possible values are as follows: • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized

Table 6-18. Port Authentication Port Configuration Fields (continued)

Field	Description
Backend State	This field displays the current state of the backend authentication state machine. Possible values are as follows: • Request • Response • Success • Fail • Timeout • Initialize • Idle
EAPOL Flood Mode	This field is used to **Enable** or **Disable** the EAPOL Flood mode per Interface.The default value is **Disable**.

2. Click **Initialize** to begin the initialization sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to click **Apply** for the action to occur.
3. Click **Reauthenticate** to begin the reauthentication sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to click **Apply** for the action to occur.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Apply** to send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.

Port Summary

Use the Port Summary page to view information about the port access control settings on a specific port.

To access the Port Summary page:

1. Click **Security** > **Port Authentication** > **Advanced** > **Port Summary** in the navigation menu.

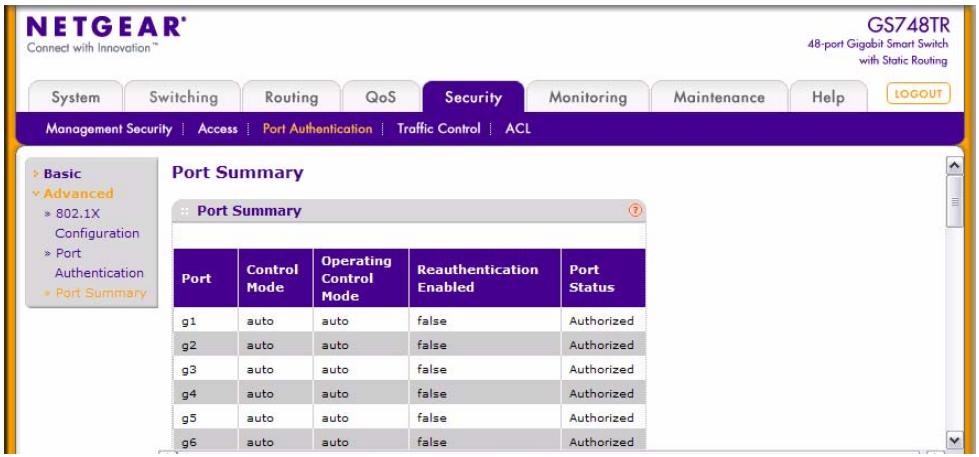


Figure 6-17

Table 6-19. Port Summary Fields

Field	Description
Port	The port whose settings are displayed in the current table row.
Control Mode	Defines the port authorization state. The control mode is only set if the link status of the port is link up. The possible field values are: • **Auto**: Automatically detects the mode of the interface. • **Force Authorized**: Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication. • **Force Unauthorized**: Denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface.
Operating Control Mode	This field indicates the control mode under which the port is actually operating. Possible values are: • ForceUnauthorized • ForceAuthorized • Auto • N/A: If the port is in detached state it cannot participate in port access control.

Table 6-19. Port Summary Fields (continued)

Field	Description
Reauthentication Enabled	Displays if reauthentication is enabled on the selected port. This is a configurable field. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.
Port Status	This field shows the authorization status of the specified port. The possible values are 'Authorized', 'Unauthorized' and 'N/A'. If the port is in detached state, the value will be 'N/A' since the port cannot participate in port access control.

2. Click **Refresh** to update the information on the screen.

Traffic Control

From the **Traffic Control** page, you can configure MAC Filters, Storm Control, Port Security, and Protected Port settings. To display the page, click the **Security** > **Traffic Control** tab.

The Traffic Control folder contains links to the following features:

- MAC Filter:
  - "MAC Filter Configuration" on page 6-30
  - "MAC Filter Summary" on page 6-32
- "Storm Control" on page 6-33
- Port Security:
  - "Port Security Configuration" on page 6-34
  - "Port Security Interface Configuration" on page 6-35
  - "Security MAC Address" on page 6-37
- "Protected Ports Membership" on page 6-38

MAC Filter Configuration

Use the MAC Filter Configuration page to create MAC filters that limit the traffic allowed into and out of specified ports on the system.

To display the MAC Filter Configuration page:

1. Click **Security** > **Traffic Control**, and then click the **MAC Filter** > **MAC Filter Configuration** link.

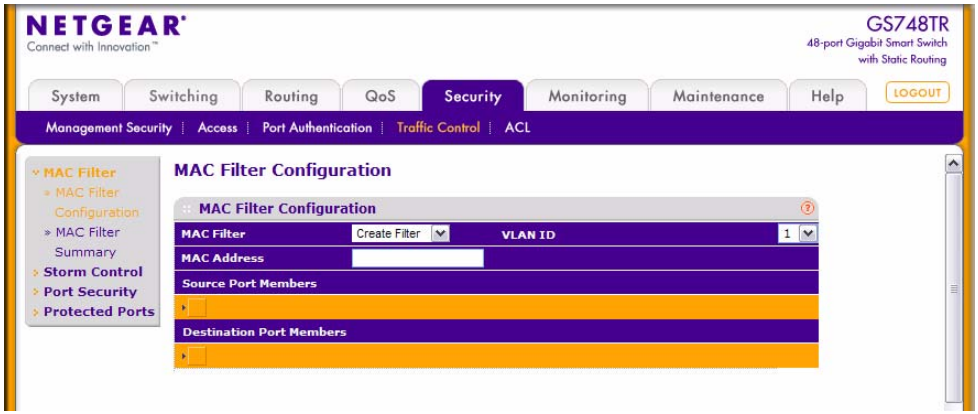


Figure 6-18

Table 6-20. Switch Configuration Fields

Field	Description
MAC Filter	This is the list of MAC address and VLAN ID pairings for all configured filters. To change the port mask(s) for an existing filter, select the entry you want to change. To add a new filter, select “Create Filter” from the top of the list
VLAN ID	The VLAN ID used with the MAC address to fully identify packets you want filtered. You can only change this field when you have selected the “Create Filter” option.
MAC Address	The MAC address of the filter in the format 00:01:1A:B2:53:4D. You can only change this field when you have selected the “Create Filter” option. You cannot define filters for these MAC addresses: • 00:00:00:00:00:00 • 01:80:C2:00:00:00 to 01:80:C2:00:00:0F • 01:80:C2:00:00:20 to 01:80:C2:00:00:21 • FF:FF:FF:FF:FF:FF
Source Port Members	Click the Unit link to display the available ports on the unit. Select the ports you want included in the inbound filter. If a packet with the MAC address and VLAN ID you selected is received on a port that is not in the list, it will be dropped.
Destination Port Members	Click the Unit link to display the available ports on the unit. Select the ports you want included in the outbound filter. Packets with the MAC address and VLAN ID you selected will only be transmitted out of ports that are in the list. Destination ports can be included only in the Multicast filter.

2. To delete a configured MAC Filter, select it from the menu, and then click **Delete**.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you make changes to the page, click **Apply** to apply the changes to the system.

MAC Filter Summary

Use the MAC Filter Summary page to view the MAC filters that are configured on the system.

To display the MAC Filter Summary page:

1. Click **Security** > **Traffic Control**, and then click the **MAC Filter** > **MAC Filter Summary** link.

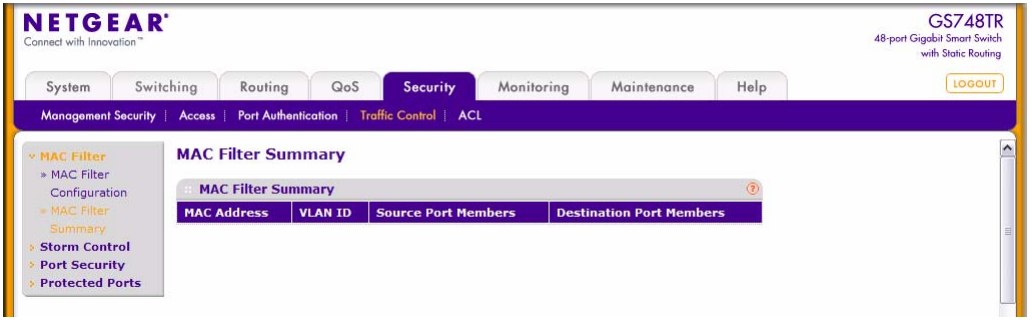


Figure 6-19

Table 6-21. Switch Configuration Fields

Field	Description
MAC Address	Identifies the MAC address that is filtered.
VLAN ID	The VLAN ID used with the MAC address to fully identify packets you want filtered. You can only change this field when you have selected the “Create Filter” option.
Source Port Members	Shows the ports included in the inbound filter.
Destination Port Members	Shows the ports included in the outbound filter.

2. Click **Refresh** to update the page with the most current information.

Storm Control

A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources and/or cause the network to time out.

The switch measures the incoming broadcast/multicast/unknown unicast packet rate per port and discards packets when the rate exceeds the defined value. Storm control is enabled per interface, by defining the packet type and the rate at which the packets are transmitted.

To display the Storm Control page:

1. Click **Security** > **Traffic Control**, and then click the **Storm Control** link.

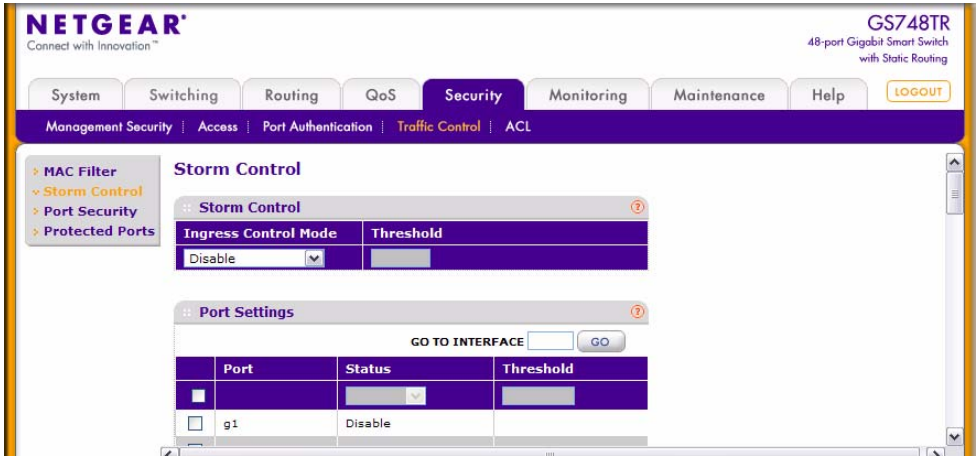


Figure 6-20

Table 6-22. Storm Control Fields

Field	Description
Ingress Control Mode	Select the mode of broadcast affected by storm control. • Disable — Do not use storm control. • Unknown Unicast — If the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. • Multicast — If the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. • Broadcast — If the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.
Threshold	Specifies the maximum rate at which unknown packets are forwarded. The range is a percent of the total threshold. The range is a percent of the total threshold between 0-100%.

Table 6-23. Port Settings Fields

Field	Description
Port	Select the check box next to the port to change the Storm Control administrative status.
Status	Shows whether the interfaces is enabled for storm control. If the port check box is selected, you can enable or disable storm control for the port.
Threshold	Used to set the threshold for either Broadcast or Multicast or Unknown Unicast traffic.

2. To go to an interface in the list, type the interface number in the **Go To Interface** field and click **Go**.
3. If you make changes to the page, click **Apply** to apply the changes to the system.

Port Security Configuration

Use the Port Security feature to lock one or more ports on the system. When a port is locked, only packets with allowable source MAC addresses can be forwarded. All other packets are discarded.

To display the Port Security Configuration page:

1. Click **Security** > **Traffic Control**, and then click the **Port Security** > **Port Security Configuration** link.

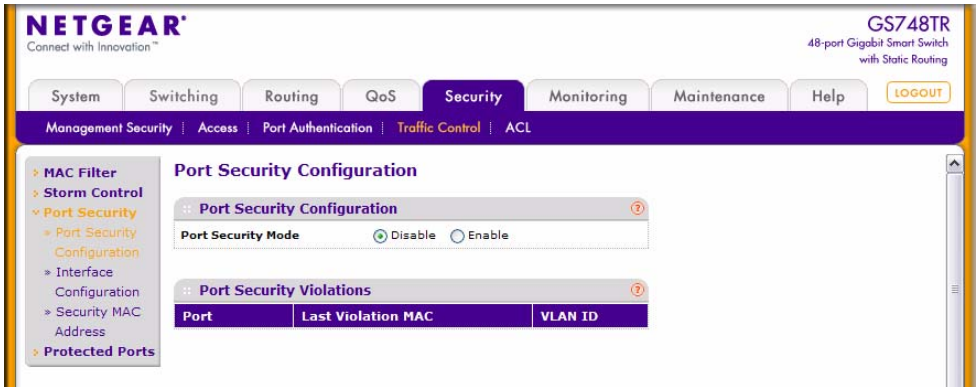


Figure 6-21

Table 6-24. Port Security Configuration Fields

Field	Description
Port Security Mode	**Enable** or **Disable** the port security feature.

Table 6-25. Port Security Violation Fields

Field	Description
Port	Identifies the port where a violation occurred.
Last Violation MAC	Displays the source MAC address of the last packet that was discarded at a locked port.
VLAN ID	Displays the VLAN ID corresponding to the Last Violation MAC address.

2. Click **Refresh** to refresh the page with the most current data from the switch.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you make changes to the page, click **Apply** to apply the changes to the system.

Port Security Interface Configuration

A MAC address can be defined as allowable by one of two methods: dynamically or statically. Note that both methods are used concurrently when a port is locked.

Dynamic locking implements a ‘first arrival’ mechanism for Port Security. You specify how many addresses can be learned on the locked port. If the limit has not been reached, then a packet with an unknown source MAC address is learned and forwarded normally. Once the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. Note that you can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

To display the Port Security Interface Configuration page:

1. Click **Security** > **Traffic Control**, and then click the **Port Security** > **Interface Configuration** link.

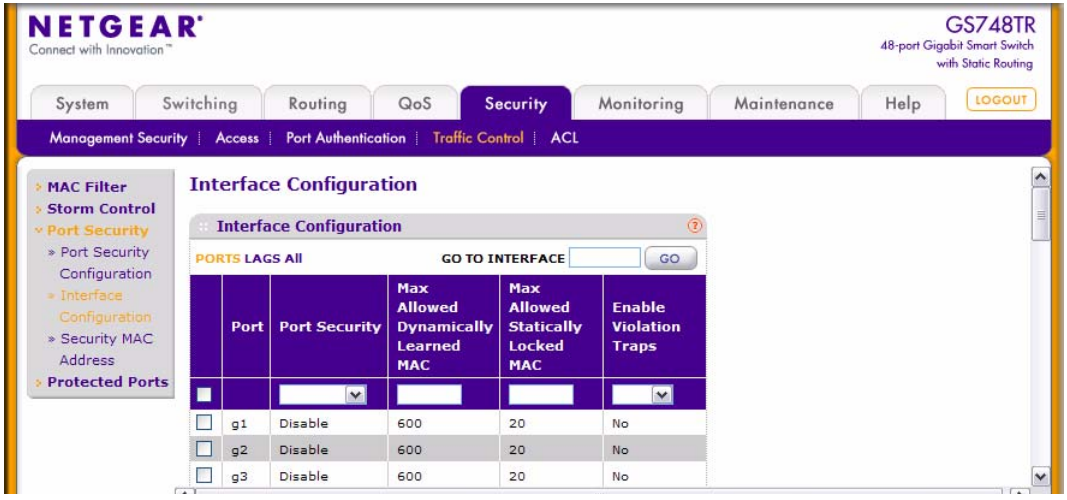


Figure 6-22

Table 6-26. Port Security Configuration Fields

Field	Description
Port	Identifies the port. To change the port security settings for the port, select the associated check box.
Port Security	Enable or Disable the port security feature for the selected port.

Table 6-26. Port Security Configuration Fields (continued)

Field	Description
Max Allowed Dynamically Learned MAC	Sets the maximum number of dynamically learned MAC addresses on the selected interface. Valid range is 0 to 600.
Max Allowed Statically Locked MAC	Sets the maximum number of statically locked MAC addresses on the selected interface. Valid range is 0 to 20.
Enable Violation Traps	Enables or disables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

2. To display the list of Ports, click **PORTS**.
3. To display the list of LAGs, click **LAGS**.
4. To display a list of both Ports and LAGs, click **ALL**.
5. To go to an interface in the list, type the interface number in the **Go To Interface** field and click **Go**.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. If you make changes to the page, click **Apply** to apply the changes to the system.

Security MAC Address

Use the Security MAC Address page to convert a dynamically learned MAC address to a statically locked address.

To display the Security MAC Address page:

1. Click **Security** > **Traffic Control**, and then click the **Port Security** > **Security MAC Address** link.

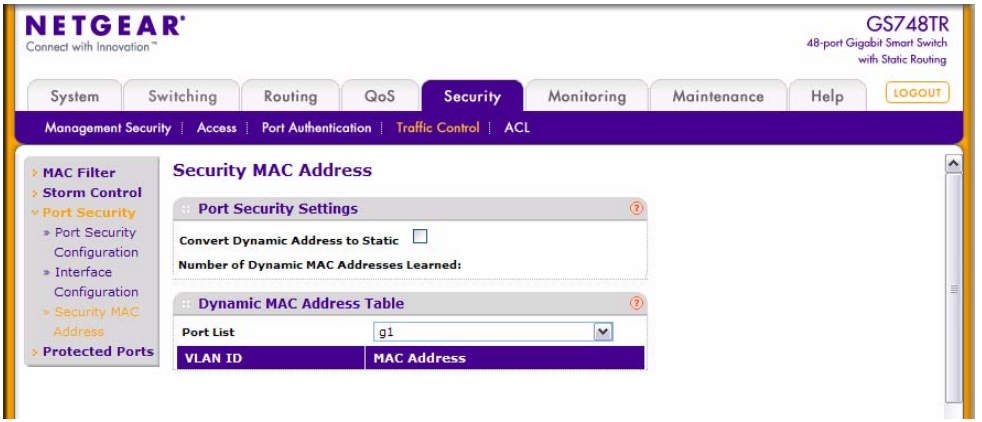


Figure 6-23

Table 6-27. Port Security Settings Fields

Field	Description
Convert Dynamic Address to Static	Select the check box to convert a dynamically learned MAC address to a statically locked address. The Dynamic MAC Address entries are converted to Static MAC address entries in a numerically ascending order until the Static limit is reached.

Table 6-28. Dynamic MAC Address Table Fields

Field	Description
Port List	Select the physical interface for which you want to display data.
VLAN ID	Displays the VLAN ID corresponding to the Last Violation MAC address.
MAC Address	Displays the MAC addresses learned on a specific port.

2. Click **Refresh** to refresh the page with the most current data from the switch.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you make changes to the page, click **Apply** to apply the changes to the system.

Protected Ports Membership

Use the Protected Ports Membership page to configure the ports as protected or unprotected. You need read-write access privileges to modify the configuration.

To display the Protected Ports Membership page:

1. Click the **Security** > **Traffic Control** > **Protected Ports** link.

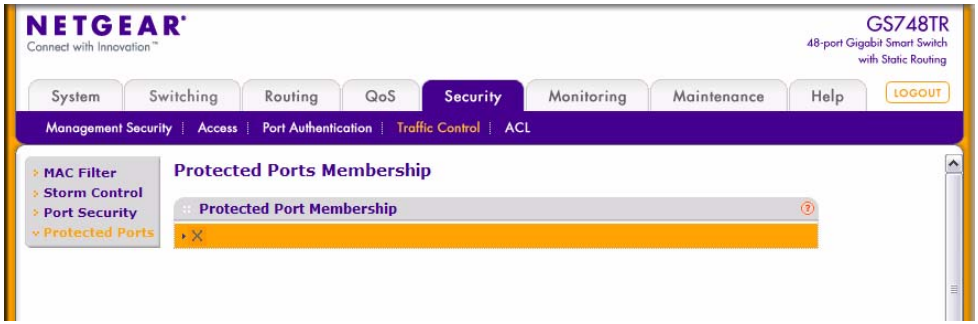


Figure 6-24

Table 6-29. Protected Ports Membership Fields

Field	Description
Protected Port(s)	The selection list consists of physical ports, protected as well as unprotected. The protected ports are highlighted in order to differentiate between them. No traffic forwarding is possible between two protected ports. If left unconfigured, the default state is **Unprotected**.

2. Click **Refresh** to refresh the page with the most current data from the switch.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

Configuring Access Control Lists

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network. GS700TR Smart Switch software supports IPv4 and MAC ACLs.

You first create an IPv4-based or MAC-based rule and assign a unique ACL ID. Then, you define the rules, which can identify protocols, source and destination IP and MAC addresses, and other packet-matching criteria. Finally, you use the ID number to assign the ACL to a port or to a VLAN interface.

The Security > ACL folder contains links to the following features:

- Basic:
  - "MAC ACL" on page 6-40
  - "MAC Rules" on page 6-42
  - "MAC Binding Configuration" on page 6-44
  - "MAC Binding Table" on page 6-45
- Advanced:
  - "IP ACL" on page 6-46
  - "IP Rules" on page 6-48
  - "IP Extended Rule" on page 6-49
  - "IP Binding Configuration" on page 6-53
  - "IP Binding Table" on page 6-55
  - "VLAN ACL Configuration" on page 6-56
  - "ACL Interface/VLAN Summary" on page 6-57

MAC ACL

A MAC ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match.

There are multiple steps involved in defining an ACL and applying it to the switch. First, you use the "MAC ACL" page to define the ACL type and assign an ID to it. Then, you use the "MAC Rules" page to create rules for the ACL. Finally, you use the "MAC Binding Configuration" page to assign the ACL by its ID number to a port. You can use the "MAC Binding Table" page to view the configurations.

To display the MAC ACL page:

1. Click **Security** > **ACL**. The MAC ACL page is under the **Basic** link.

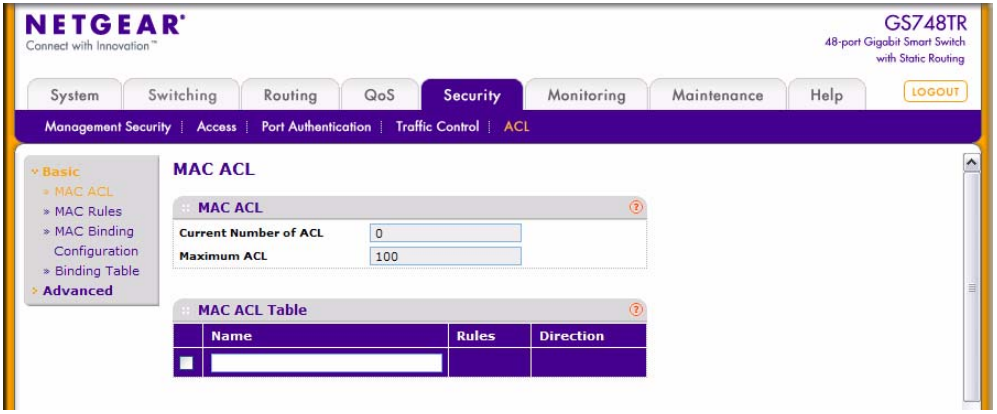


Figure 6-25

The MAC ACL table shows the number of ACLs currently configured in the switch and the maximum number of ACLs that can be configured. The current size is equal to the number of configured IPv4 ACLs plus the number of configured MAC ACLs.

Table 6-30. MAC ACL Table Fields

Field	Description
Name	Enter a name for the MAC ACL.. The name string may include alphabetic, numeric, dash, underscore, or space characters only. The name must start with an alphabetic character.
Rules	Shows the number of rules currently configured for the MAC ACL.
Direction	Shows the direction of packet traffic affected by the MAC ACL, which can be **Inbound** or blank.

2. To add a MAC ACL, enter information into the appropriate fields and click **Add**.
3. To delete a MAC ACL, select the check box next to the Name field, then click **Delete**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make changes to the page, click **Apply** to apply the changes to the system.

MAC Rules

Use the MAC Rules page to define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. A default 'deny all' rule is the last rule of every list.

To display the MAC Rules page:

1. Click **Security** > **ACL**, then click the **Basic** > **MAC Rules** link.

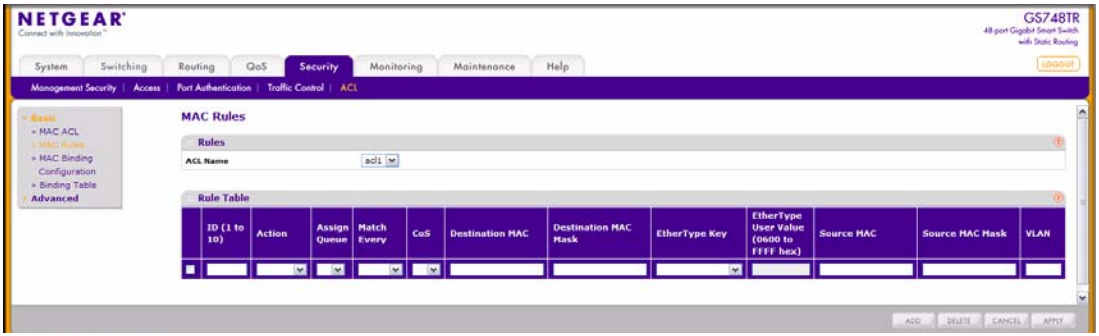


Figure 6-26

Table 6-31. MAC ACL Rule Configuration Fields

Field	Description
ACL Name	Specifies an existing MAC ACL. To set up a new MAC ACL use the "MAC ACL" page.
ID (1 to 10)	Enter a rule ID.
Action	Specify what action should be taken if a packet matches the rule's criteria: • Permit: Forwards packets that meet the ACL criteria. • Deny: Drops packets that meet the ACL criteria.
Assign Queue	Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Enter an identifying number from 0 to 7in the appropriate field.
Match Every	Requires a packet to match the criteria of this ACL. Select True or False from the dropdown menu. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.
CoS	Requires a packet's class of service (CoS) to match the CoS value listed here. Enter a CoS value between 0 and 7 to apply this criteria.

Table 6-31. MAC ACL Rule Configuration Fields (continued)

Field	Description
Destination MAC	Requires an Ethernet frame's destination port MAC address to match the address listed here. Enter a MAC address in the appropriate field. The valid format is xx:xx:xx:xx:xx:xx.
Destination MAC Mask	If desired, enter the MAC Mask associated with the Destination MAC to match. The MAC address mask specifies which bits in the destination MAC to compare against an Ethernet frame. Use F's and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is 00:00:ff:ff:ff:ff, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where *x* is any hexadecimal number).
EtherType Key	Requires a packet's EtherType to match the EtherType you select. Click **Configure**, and then select the EtherType value from the dropdown menu. If you select User Value, you can enter a custom EtherType value.
EtherType User Value	This field only appears if you select User Value from the EtherType dropdown menu. The value you enter specifies a customized Ethertype to compare against an Ethernet frame. The valid range of values is (0x0600 to 0xFFFF).
Source MAC	Requires a packet's source port MAC address to match the address listed here. Click **Configure**, and then enter a MAC address in the appropriate field. The valid format is xx:xx:xx:xx:xx:xx.
Source MAC Mask	If desired, enter the MAC mask for the source MAC address to match. Use Fs and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. The valid format is xx:xx:xx:xx:xx:xx.
VLAN	Requires a packet's VLAN ID to match the ID listed here. Enter the VLAN ID to apply this criteria. The valid range is 0 to 4078.

2. To add a rule, complete the desired fields and click **Add**.
3. To delete a rule, select the check box associated with the rule and click **Delete**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. To change a rule, select the check box associated with the rule, change the desired fields and click **Apply**.

MAC Binding Configuration

When an ACL is bound to an interface, all the rules that have been defined are applied to the selected interface. Use the MAC Binding Configuration page to assign MAC ACL lists to ACL Priorities and Interfaces.

To display the MAC Binding Configuration page:

1. Click **Security** > **ACL**, then click the **Basic** > **MAC Binding Configuration** link.

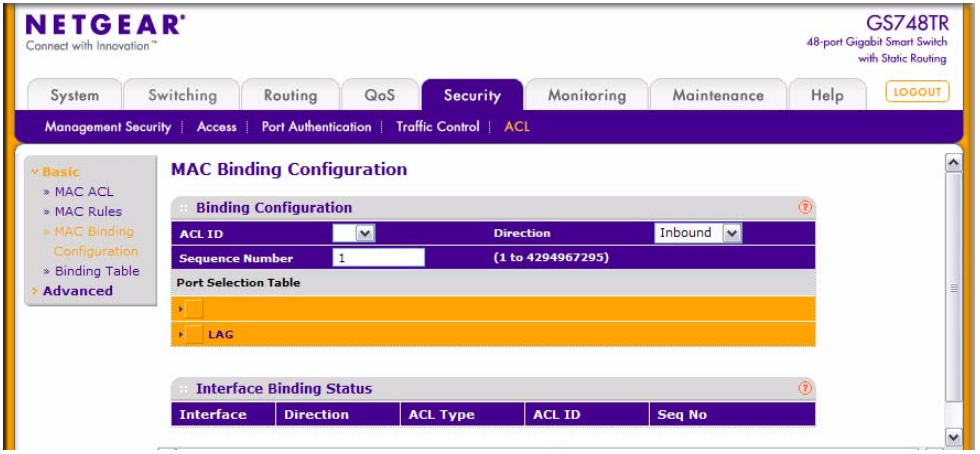


Figure 6-27

Table 6-32. MAC ACL Rule Configuration Fields

Field	Description
ACL ID	Select an existing MAC ACL.
Direction	Specifies the packet filtering direction for ACL. The only valid direction is **Inbound,** which means the MAC ACL rules are applied to traffic entering the port.

Table 6-32. MAC ACL Rule Configuration Fields (continued)

Field	Description
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction will be used. Valid range is (1 to 4294967295).
Port Selection Table	Specifies list of all available valid interfaces for ACL binding. All non-routing physical interfaces and interfaces participating in LAGs are listed.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Apply** to save any changes to the running configuration.

MAC Binding Table

Use the MAC Binding Table page to view or delete the MAC ACL bindings.

To display the MAC Binding Table:

1. Click **Security** > **ACL**, then click the **Basic** > **Binding Table** link.

Figure 6-28

Table 6-33. MAC ACL Rule Configuration Fields

Field	Description
Interface	Shows the interface to which the MAC ACL is bound.
Direction	Specifies the packet filtering direction for ACL. The only valid direction is Inbound, which means the MAC ACL rules are applied to traffic entering the port.
ACL Type	Displays the type of ACL assigned to selected interface and direction.
ACL ID	Displays the ACL Name identifying the ACL assigned to selected interface and direction.
Sequence No	Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. To delete the binding, select the check box next to the interface and click **Delete**.

IP ACL

IP ACLs allow network managers to define classification actions and rules for specific ingress ports. Packets can be filtered on ingress (inbound) ports only. If the filter rules match, then some actions can be taken, including dropping the packet or disabling the port. For example, a network administrator defines an ACL rule that says port number 20 can receive TCP packets. However, if a UDP packet is received the packet is dropped.

ACLs are composed of access control entries (ACE), or rules, that consist of the filters that determine traffic classifications.

Use the IP ACL Configuration page to add or remove IP-based ACLs.

To display the IP ACL page:

1. Click **Security** > **ACL**, then click the **Advanced** > **IP ACL** link.

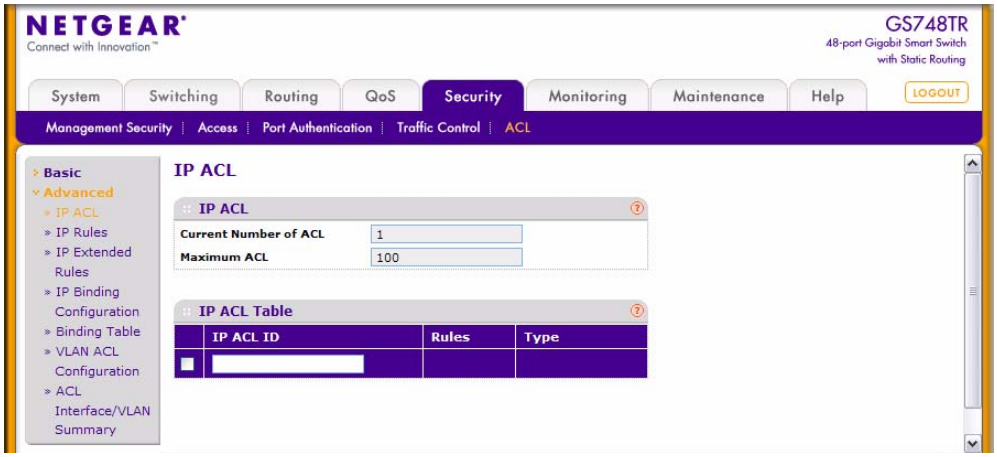


Figure 6-29

The top table shows the current size of the ACL table versus the maximum size of the ACL table. The current size is equal to the number of configured IPv4 plus the number of configured MAC ACLs. The maximum size is 100.

Table 6-34. IP ACL Configuration Fields

Field	Description
IP ACL	Enter an ACL ID. The ID is an integer in the following range: • 1-99: Creates an IP Standard ACL, which allows you to permit or deny traffic from a source IP address. • 100-199: Creates an IP Extended ACL, which allows you to permit or deny specific types of layer 3 or layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the standard IP ACL.
Rules	Shows the number of rules currently configured for the IP ACL.
Type	Identifies the ACL as either a standard or extended IP ACL.

2. To add an IP ACL, enter an ACL ID in the appropriate field, and then click **Add**.
3. To delete an IP ACL, select the check box associated withe ACL ID, and then click **Delete**. The **Delete** button only appears if a configured IP ACL is selected.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IP Rules

Use the IP Rules page to define rules for IP-based standard ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: There is an implicit “deny all” rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit “deny all” rule applies and the packet is dropped.

To display the IP Rules page:

1. Click **Security** > **ACL**, then click the **Advanced** > **IP Rules** link.

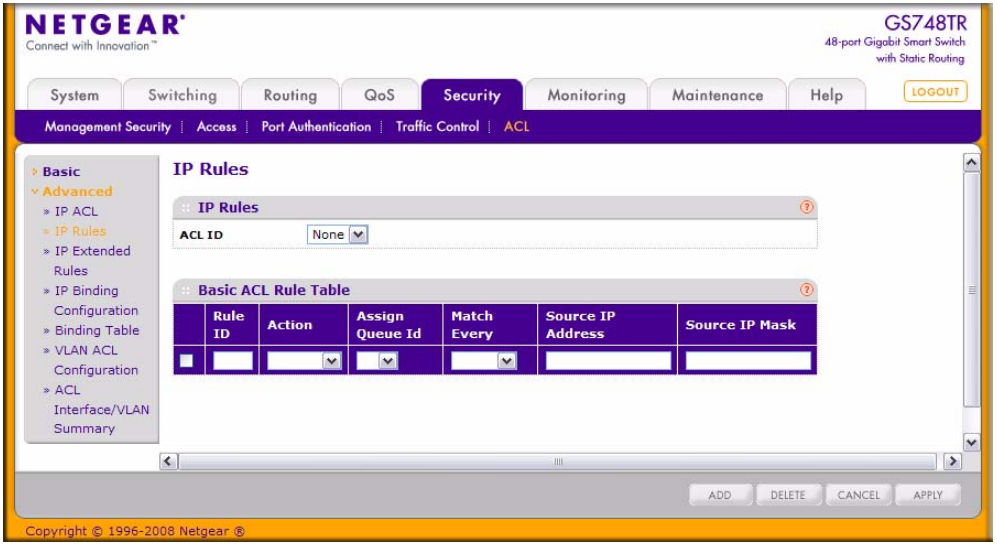


Figure 6-30

2. To add an IP ACL rule, select the ACL ID to add the rule to, complete the fields in the Basic ACL Rule Table and then click **Add**.
3. To delete an IP rule, select the check box associated with the rule, and then click **Delete**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Table 6-35. IP ACL Rule Configuration Fields

Field	Description
ACL ID	The menu contains the existing IP ACLs configured on the page. To set up a new IP ACL, see "IP ACL".
Rule ID	This field is only available if you select Create Rule from the Rule field. Enter a new Rule ID. After you click **Apply**, the new ID is created and you can configure the rule settings. You can create up to 10 rules for each ACL.
Action	Selects the ACL forwarding action, which is one of the following: • Permit — Forwards packets which meet the ACL criteria. • Deny — Drops packets which meet the ACL criteria.
Assign Queue ID	Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Enter an identifying number from 0 to 7 in the appropriate field.
Match Every	Requires a packet to match the criteria of this ACL. Select True or False from the dropdown menu. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.
Source IP Address	Requires a packet's source port IP address to match the address listed here. Enter an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's source IP Address.
Source IP Mask	Specifies the source IP address wildcard mask. Wild card masks determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored. This field is required when you configure a source IP address.

IP Extended Rule

Use the IP Extended Rules page to define rules for IP-based extended ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: There is an implicit “deny all” rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit “deny all” rule applies and the packet is dropped.

To display the IP extended Rules page:

1. Click **Security > ACL**, then click the **Advanced > IP Extended Rules** link.

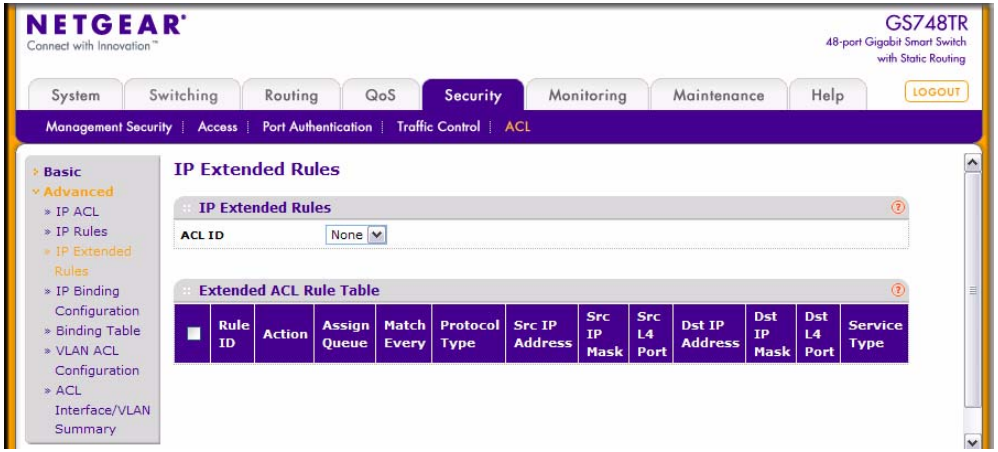


Figure 6-31

2. To add an IP ACL rule, select the ACL ID to add the rule to, and then click **Add**. The Extended ACL Rules configuration page displays as shown in Figure 6-32 on page 6-51.
3. To delete an IP rule, select the check box associated with the rule, and then click **Delete**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

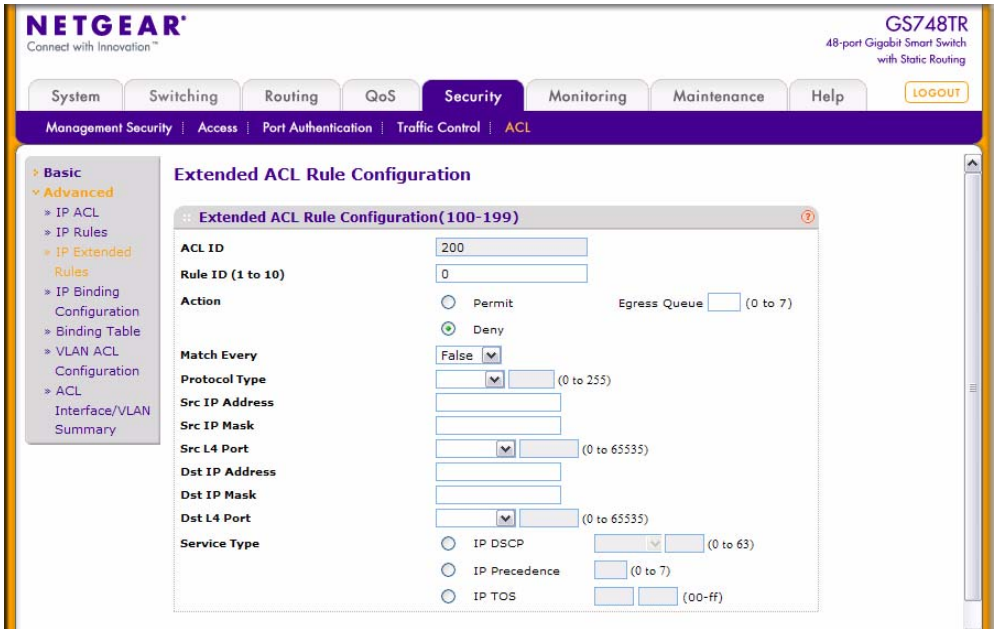


Figure 6-32

Table 6-36. IP ACL Rule Configuration Fields

Field	Description
ACL ID	Identifies the ACL to which the rule is being added.
Rule ID	Enter a whole number in the range 1 to 10 that will be used to identify the rule. After you click **Apply**, the new ID is created and you can configure the rule settings. You can create up to 10 rules for each IP ACL.
Action	Selects the ACL forwarding action that should be taken if a packet matches the rule's criteria. Possible values are: • Permit — Forwards packets which meet the ACL criteria. • Deny — Drops packets which meet the ACL criteria.
Assign Queue	Specifies the hardware egress queue identifier used to handle all packets matching this IP ACL rule. Valid range of Queue Ids is (0 to 7). This field is visible when 'Permit' is chosen as 'Action'.
Match Every	Requires a packet to match the criteria of this ACL. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen do not appear.

Table 6-36. IP ACL Rule Configuration Fields (continued)

Field	Description
Protocol Type	Requires a packet's protocol to match the protocol listed here. Select a type from the dropdown menu or enter the protocol number in the available field.
Src IP Address	Requires a packet's source port IP address to match the address listed here. Enter an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's source IP Address.
Src IP Mask	Specifies the source IP address wildcard mask. Wild card masks determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored. This field is required when you configure a source IP address.
Src L4 Port	Requires a packet's TCP/UDP source port to match the port listed here. Click Complete one of the following fields: • **Source L4 Keyword**: Select the desired L4 keyword from a list of source ports on which the rule can be based. • **Source L4 Port Number**: If the source L4 keyword is Other, enter a user-defined Port ID by which packets are matched to the rule.
Dst IP Address	Requires a packet's destination port IP address to match the address listed here. Enter an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's destination IP Address.
Dst IP Mask	Specify the IP Mask in dotted-decimal notation to be used with the Destination IP Address value.

Table 6-36. IP ACL Rule Configuration Fields (continued)

Field	Description
Dst L4 Port	Requires a packet's TCP/UDP destination port to match the port listed here. Complete one of the following fields: • **Destination L4 Keyword**: Select the desired L4 keyword from a list of destination ports on which the rule can be based. • **Destination L4 Port Number**: If the destination L4 keyword is Other, enter a user-defined Port ID by which packets are matched to the rule.
Service Type	Select one of the following three Match fields to use in matching packets to ACLs: • **IP DSCP**: Matches the packet DSCP value to the rule. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. Select the desired value from the dropdown menu of DSCP keyword values. • **IP Precedence**: Matches the packet IP Precedence value to the rule when checked. Enter the IP Precedence value to match. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. • **IP TOS Bits**: Matches on the Type of Service bits in the IP header when checked. - **TOS Bits**: Requires the bits in a packet's TOS field to match the two-digit hexadecimal number entered here. - **TOS Mask**: Specifies the bit positions that are used for comparison against the IP TOS field in a packet.

5. Click **Apply** to save any changes to the running configuration.

IP Binding Configuration

When an ACL is bound to an interface, all the rules that have been defined are applied to the selected interface. Use the IP Binding Configuration page to assign ACL lists to ACL Priorities and Interfaces.

To display the IP Binding Configuration page:

1. Click **Security** > **ACL**, then click the **Advanced** > **IP Binding Configuration** link

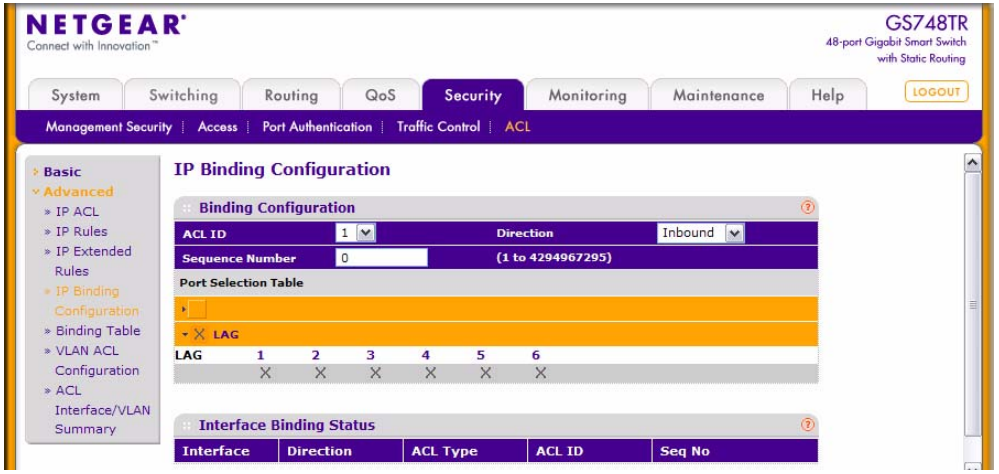


Figure 6-33

Table 6-37. IP ACL Binding Configuration Fields

Field	Description
ACL ID	Select an existing IP ACL.
Direction	Specifies the packet filtering direction for ACL. The only valid direction is **Inbound**, which means the IP ACL rules are applied to traffic entering the port.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction will be used. Valid range is (1 to 4294967295).
Port Selection Table	Specifies list of all available valid interfaces for ACL binding. All non-routing physical interfaces and interfaces participating in LAGs are listed. Click the Unit link to view all the available interfaces.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Apply** to save any changes to the running configuration.

IP Binding Table

Use the IP Binding Table page to view or delete the IP ACL bindings.

To display the IP Binding Table:

1. Click **Security** > **ACL**, then click the **Advanced** > **Binding Table** link.

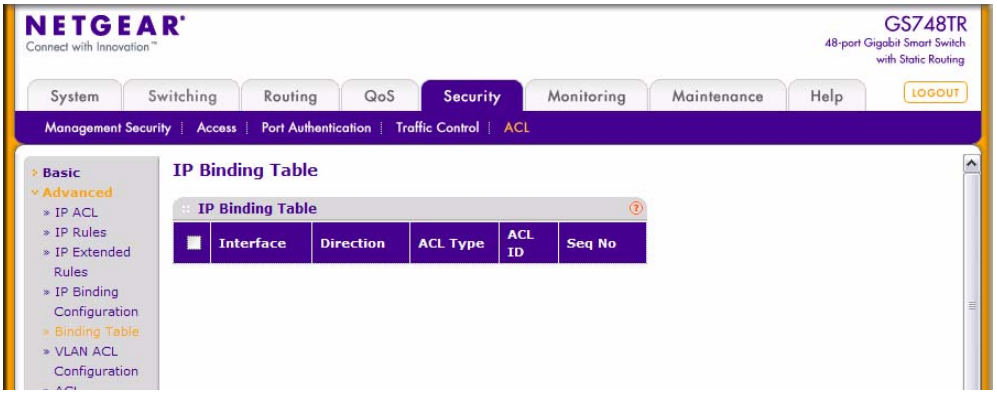


Figure 6-34

Table 6-38. IP ACL Binding Table Fields

Field	Description
Interface	Shows the interface to which the IP ACL is bound.
Direction	Specifies the packet filtering direction for ACL. The only valid direction is Inbound, which means the IP ACL rules are applied to traffic entering the port.
ACL Type	Displays the type of ACL assigned to selected interface and direction.
ACL ID	Displays the ACL Number identifying the ACL assigned to selected interface and direction.
Seq No.	Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

2. To delete the binding, select the check box next to the interface and click **Delete**.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

VLAN ACL Configuration

Use this page to configure ACLs to apply to VLANs on your system rather than to ports. At the bottom of the page, the table displays any currently-configured ACLs for the selected VLAN.

To display the VLAN ACL Configuration page:

1. Click **Security > ACL**, then click the **Advanced > VLAN ACL Configuration** link.

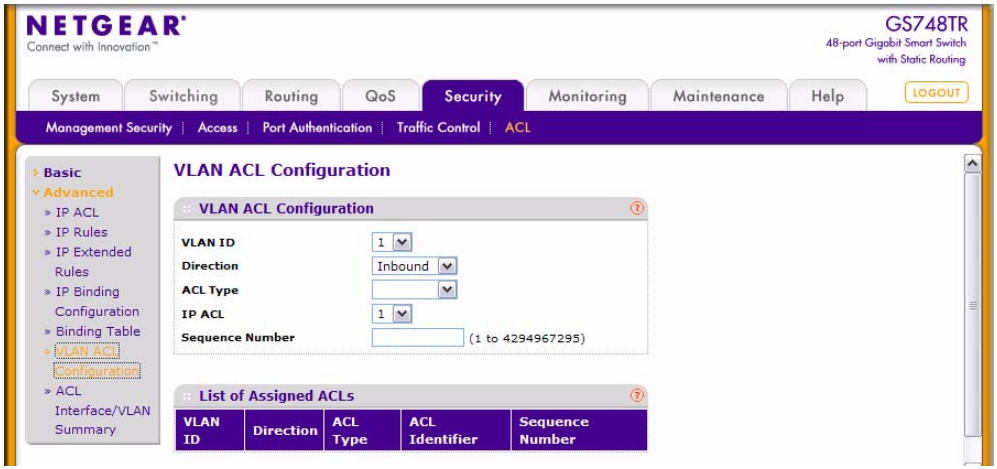


Figure 6-35

The table at the bottom of the page displays any currently configured ACLs on the selected VLAN interface.

Table 6-39. VLAN-Based ACL Configuration

Field	Description
VLAN ID	Select the configured VLAN ID that you want to associate an ACL to.
Direction	Specifies the packet filtering direction for the ACL. The system supports **Inbound** filtering, which means the system applies the ACL rules to packets as they enter the interface.
ACL Type	Use the menu to select the ACL type to which incoming packets are matched. Packets can be matched to IPv4- and MAC-based ACLs.
IP ACL	The dropdown menu contains all configured IP ACLs. Select the IP ACL to apply to the interface. This field is only visible if you select IP ACL as the ACL Type.

Table 6-39. VLAN-Based ACL Configuration

Field	Description
MAC ACL	The dropdown menu contains all configured MAC ACLs. Select the MAC ACL to apply to the interface. This field is only visible if you select MAC ACL as the ACL Type.
Sequence Number	Assigns the priority of this ACL. If more than one ACL is applied to an interface, then the match criteria for the highest sequence ACLs are checked first. A lower number indicates higher priority. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify a sequence number, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1-4294967295.

2. Click **Refresh** to update the page with the most current information.
3. To delete a VLAN ACL, select the ACL, then click **Delete**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make changes to the page, click **Apply** to apply the changes to the system.

ACL Interface/VLAN Summary

Use this page to view all ports and VLANs to which an ACL has been applied.

To access the page:

1. Click **Security** > **ACL**, and then click the **Advanced** > **ACL Interface/VLAN Summary** link.

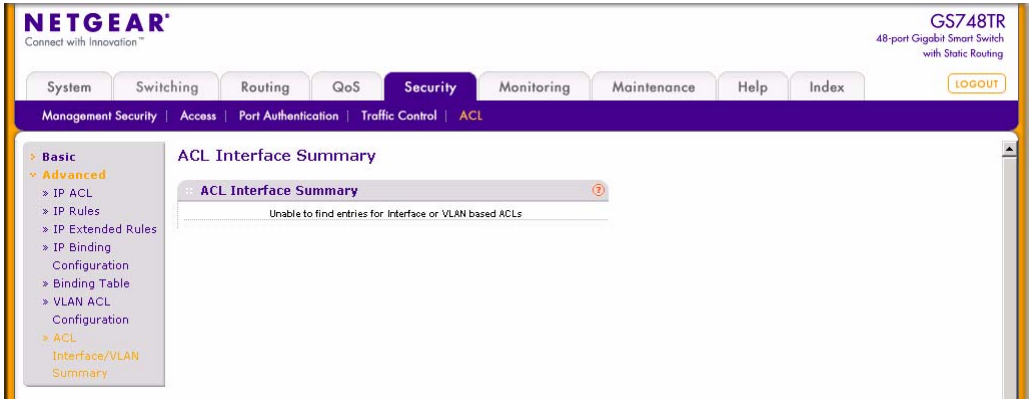


Figure 6-36

The table at the bottom of the page displays any currently configured ACLs on the selected VLAN interface.

Table 6-40. VLAN-Based ACL Configuration

Field	Description
Summary Display Selector	Select interface or VLAN to display summary. By default summary of Interface-based ACL(s) is displayed.
Port	Displays the interfaces to which the IP ACL applies.
VLAN(s)	Displays the VLAN(s) to which the IP ACL applies.
Direction	The direction of packet traffic affected by the IP ACL. The system supports inbound filtering.
ACL Type	Displays the type of ACL assigned to selected VLAN and direction.
ACL Identifier	Displays the ACL Number (for IPv4 ACLs) or the ACL Name (for MAC ACLs), which identifies the ACL assigned to the selected VLAN and direction.
Sequence Number	Displays the sequence number signifying the order of specified ACL relative to other ACLs assigned to selected VLAN and direction.

2. Click **Refresh** to update the screen with the most current information.

Chapter 7
Monitoring the System

Use the features available from the Monitoring tab to view a variety of information about the switch and its ports and to configure how the switch monitors events. The **Monitoring** tab contains links to the following features:

Switch Statistics

The pages in the Switch Statistics folder contain a variety of information about the number and type of traffic transmitted from and received on the switch.

The Switch Statistics page shows detailed statistical information about the traffic the switch handles.

To access the Switch Statistics page:

1. Click **Monitoring > Ports > Switch Statistics** in the navigation menu.

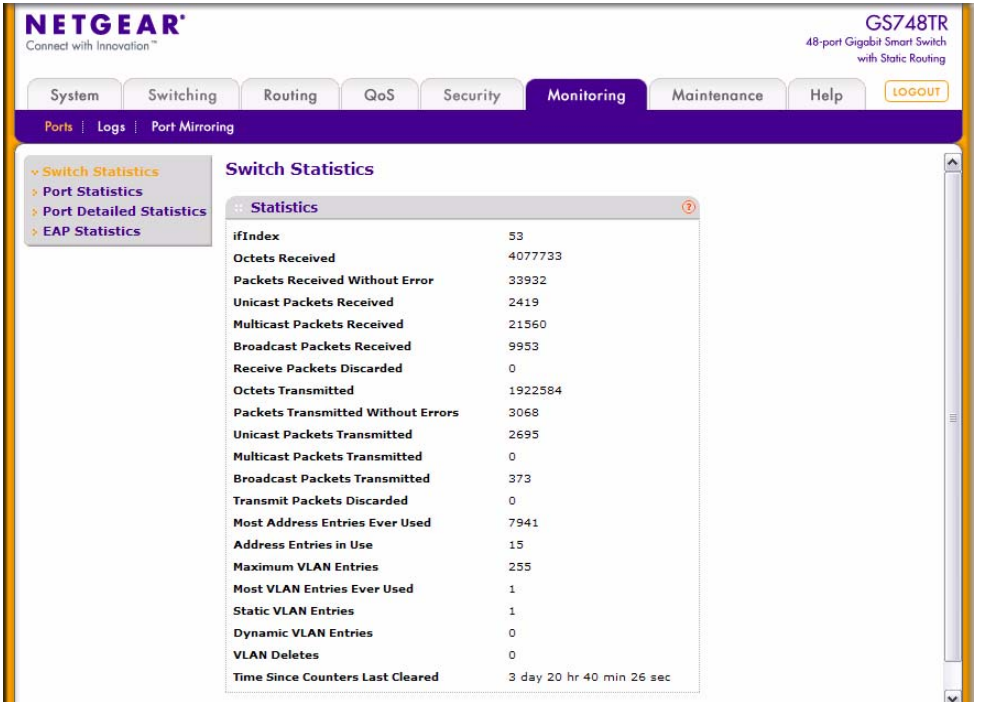


Figure 7-1

Table 7-1. Switch Statistics Fields

Field	Description
ifIndex	This object indicates the ifIndex of the interface table entry associated with the processor of this switch.
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Errors	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Table 7-1. Switch Statistics Fields (continued)

Field	Description
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded, even though no errors had been detected, in order to prevent their being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded, even though no errors had been detected, in order to prevent their being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

2. Click **Clear Counters** to clear all the statistics counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.
3. Click **Refresh** to refresh the page with the most current data from the switch.

Viewing Port Statistics

The pages in the Ports folder contain a variety of information about the number and type of traffic transmitted from and received on the switch.

- "Port Statistics" on page 7-4
- "Port Detailed Statistics" on page 7-5
- "EAP Statistics" on page 7-13

Port Statistics

The Port Statistics page shows a summary of per-port traffic statistics on the switch.

To access the Port Summary page:

1. Click **Monitoring > Ports**, and then click the **Port Statistics** link.

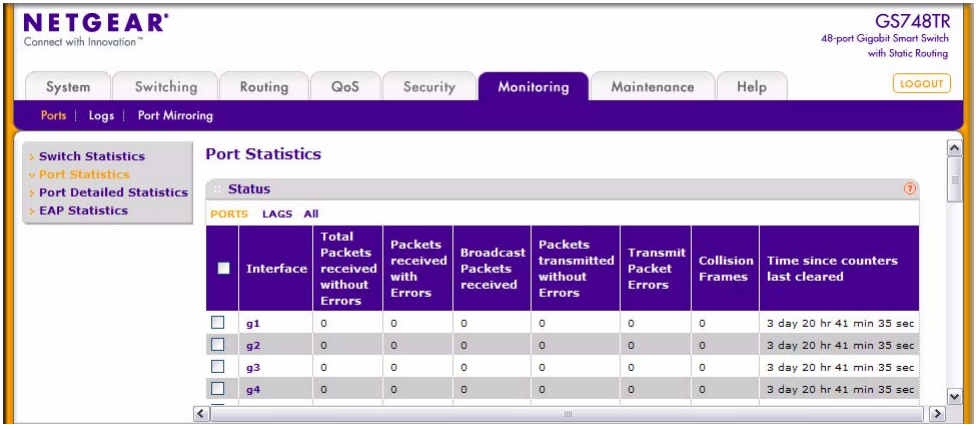


Figure 7-2

Table 7-2. Port Statistics Fields

Field	Description
Interface	Lists the ports on the system.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that have been transmitted by this port to its segment.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

2. To clear all the counters for all ports on the switch, select the check box in the row heading and click **Clear**. The button resets all statistics for all ports to default values.
3. To clear the counters for a specific port, select the check box associated with the port and click **Clear**.
4. Click **Refresh** to refresh the data on the screen and display the most current statistics.

Port Detailed Statistics

The Port Detailed Statistics page displays a variety of per-port traffic statistics.

To access the Port Detailed page:

1. Click the **Monitoring** > **Ports** tab, and then click **Port Detailed Statistics**. (Figure 7-3 shows some, but not all, of the fields on the Port Detailed Statistics page.)

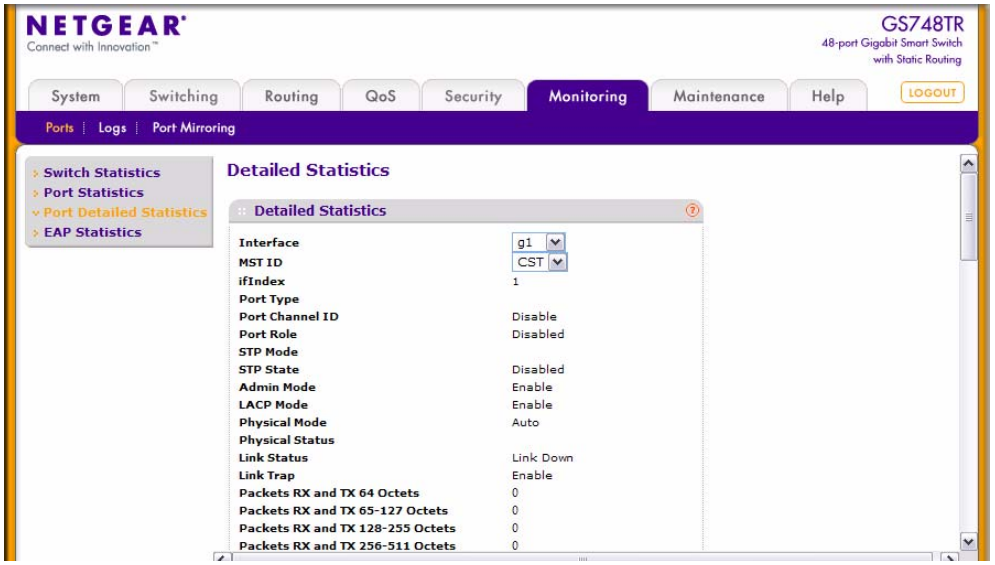


Figure 7-3

Table 7-3. Port Detailed Statistics Fields

Field	Description
Interface	Use the dropdown menu to select the interface for which data is to be displayed or configured.
MST ID	Displays the created or existing MSTs.
ifIndex	This field indicates the ifIndex of the interface table entry associated with this port on an adapter.
Port Type	For most ports this field is blank. Otherwise the possible values are: • **Mirrored:** Indicates that the port has been configured as a monitoring port and is the source port in a port mirroring session. For more information about port monitoring and probe ports, see "Multiple Port Mirroring" on page 7-23. • **Probe:** Indicates that the port has been configured as a monitoring port and is the destination port in a port mirroring session. For more information about port monitoring and probe ports, see "Multiple Port Mirroring" on page 7-23. • **Port Channel:** Indicates that the port has been configured as a member of a port-channel, which is also known as a link Aggregation Group (LAG).

Table 7-3. Port Detailed Statistics Fields (continued)

Field	Description
Port Channel ID	If the port is a member of a port channel, the port channel's interface ID and name are shown. Otherwise “Disable” is shown.
Port Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
STP Mode	Shows the Spanning Tree Protocol (STP) Administrative Mode for the port or LAG. The possible values for this field are: • **Enable:** Enables the Spanning Tree Protocol for this port. • **Disable:** Disables the Spanning Tree Protocol for this port.
STP State	Shows the port's current state Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port it will place that port into the broken state. The other five states are defined in IEEE 802.1D: • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Admin Mode	Use the dropdown menu to select the port control administration state, which can be one of the following: • **Enable:** The port can participate in the network (default). • **Disable:** The port is administratively down and does not participate in the network.
LACP Mode	Selects the Link Aggregation Control Protocol administration state: • **Enable:** Specifies that the port is allowed to participate in a port channel (LAG), which is the default mode. • **Disable:** Specifies that the port cannot participate in a port channel (LAG).
Physical Mode	Indicates the port speed and duplex mode. In auto-negotiation mode, the duplex mode and speed are set from the auto-negotiation process.
Physical Status	Indicates the port speed and duplex mode status.
Link Status	Indicates whether the Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled: • **Enable:** Specifies that the system sends a trap when the link status changes. • **Disable:** Specifies that the system does not send a trap when the link status changes.

Table 7-3. Port Detailed Statistics Fields (continued)

Field	Description
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1519-1522 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1523-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Received 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Table 7-3. Port Detailed Statistics Fields (continued)

Field	Description
Packets Received 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received > 1522 Octets	The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Total Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Table 7-3. Port Detailed Statistics Fields (continued)

Field	Description
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
Rx FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Total Received Packets Not Forwarded	A count of valid frames received which were discarded (i.e., filtered) by the forwarding process.
Local Traffic Frames	The total number of frames dropped in the forwarding process because the destination address was located off of this port.
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.
Multicast Tree Viable Discards	The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.
Reserved Address Discards	The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.
Broadcast Storm Recovery	The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.
CFI Discards	The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.
Upstream Threshold	The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

Table 7-3. Port Detailed Statistics Fields (continued)

Field	Description
Total Packets Transmitted (Octets)	The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Transmitted 65-127 Octets	The total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 128-255 Octets	The total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 256-511 Octets	The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 512-1023 Octets	The total number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 1024-1518 Octets	The total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 1519-1522 Octets	The total number of packets (including bad packets) transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
Total Packets Transmitted Successfully	The number of frames that have been transmitted by this port to its segment.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Table 7-3. Port Detailed Statistics Fields (continued)

Field	Description
Total Transmit Errors	The sum of Single, Multiple, and Excessive Collisions.
Tx FCS Errors	The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Tx Oversized	The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per second at 10 Mb/s.
Underrun Errors	The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Port Membership Discards	The number of frames discarded on egress for this port due to egress filtering being enabled.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.
802.3x Pause Frames Transmitted	A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

2. Click **Clear** to clear all the counters. This resets all statistics for this port to the default values.
3. Click **Refresh** to refresh the data on the screen and display the most current statistics.

EAP Statistics

Use the EAP Statistics page to display information about EAP packets received on a specific port.

To display the EAP Statistics page:

1. Click the **Monitoring** > **Ports** tab, and then click the **EAP Statistics** link.

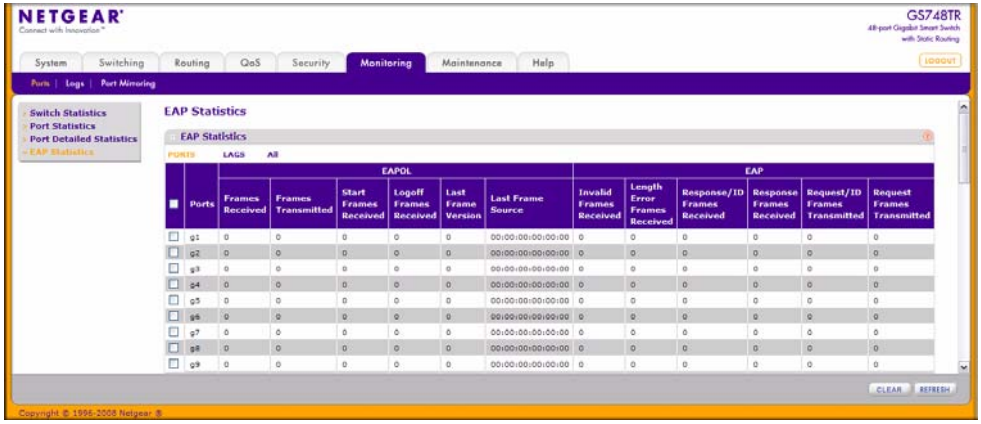


Figure 7-4

Table 7-4. EAP Statistics Fields

Field	Description
Ports	Specifies the interface which is polled for statistics.
Frames Received	Displays the number of valid EAPOL frames received on the port.
Frames Transmitted	Displays the number of EAPOL frames transmitted through the port.
Start Frames Received	Displays the number of EAPOL Start frames received on the port.
Log off Frames Received	Displays the number of EAPOL Log off frames that have been received on the port.
Last Frame Version	Displays the protocol version number attached to the most recently received EAPOL frame.
Last Frame Source	Displays the source MAC Address attached to the most recently received EAPOL frame.

Table 7-4. EAP Statistics Fields

Field	Description
Invalid Frames Received	Displays the number of unrecognized EAPOL frames received on this port.
Length Error Frames Received	Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.
Response/ID Frames Received	Displays the number of EAP Respond ID frames that have been received on the port.
Response Frames Received	Displays the number of valid EAP Response frames received on the port.
Request/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted through the port.
Request Frames Transmitted	Displays the number of EAP Request frames transmitted through the port.

2. To clear all the EAP counters for all ports on the switch, select the check box in the row heading and click **Clear**. The button resets all statistics for all ports to default values.
3. To clear the counters for a specific port, select the check box associated with the port and click **Clear**.
4. Click **Refresh** to refresh the data on the screen and display the most current statistics.

Managing Logs

The switch may generate messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored locally on the platform and can be forwarded to one or more centralized points of collection for monitoring purposes or long term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

The **Monitoring** > **Logs** tab contains links to the following folders:

- “Memory Logs” on page 7-15
- “FLASH Log Configuration” on page 7-17
- “Server Log Configuration” on page 7-19
- “Trap Logs” on page 7-21

- "Event Logs" on page 7-22

Memory Logs

The *in-memory* log stores messages in memory based upon the settings for message component and severity. Use the Memory Logs page to set the administrative status and behavior of logs in the system buffer.

To access the Memory Log page:

1. Click the **Monitoring > Logs** tab, and then click the **Memory Log** link.

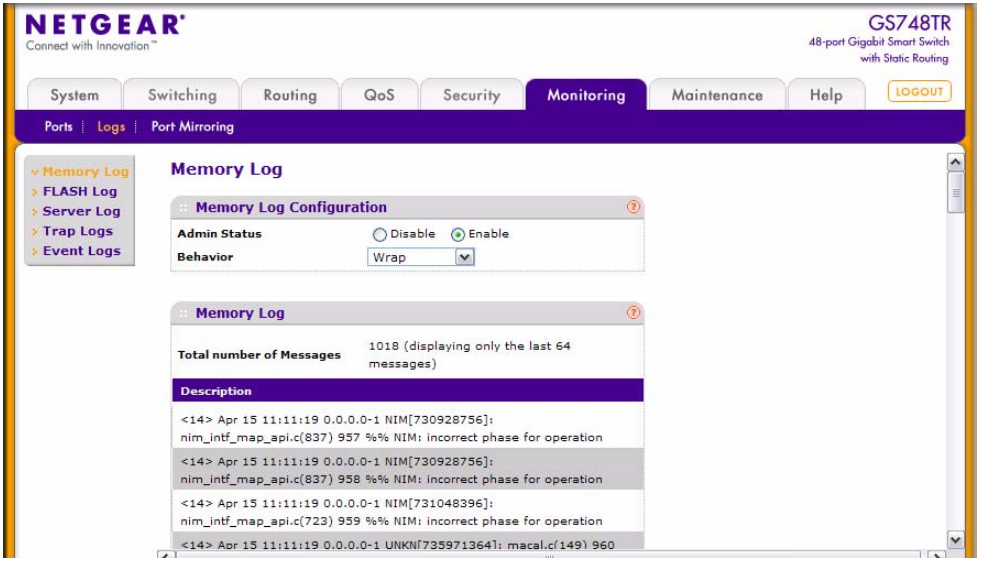


Figure 7-5

Table 7-5. Memory Log Configuration Fields

Field	Description
Admin Status	Determines whether **to log messages.** • **Enable: Enables system logging.** • **Disable: Prevents th**e system from logging messages.
Behavior	Indicates the behavior of the log when it is full. • **Wrap:** When the buffer is full, the oldest log messages are deleted as the system logs new messages. • **Stop on Full:** When the buffer is full, the system stops logging new messages and preserves all existing log messages.

The Memory Log table also appears on the Memory Log page.

Table 7-6. Memory Log Table Fields

Field	Description
Total Number of Messages	Shows the number of messages the system has logged in memory. Only the 64 most recent entries are displayed on the page.

The rest of the page displays the Memory Log messages. The following example applies to the format of all logged messages which are displayed for the message log, persistent log, or console log.

Messages logged to a collector or relay via syslog have an identical format of either type.

```
<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface
12 transitioned to root state on message age timer expiry
```

The example log message above indicates a message with severity 7(15 mod 8) (debug). The message was generated by the MSTP component running in thread id 2110. The message was generated on Aug 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged.

Example user-level message:

```
<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface
12 transitioned to root state on message age timer expiry
```

The example log message above indicates a user-level message (1) with severity 7 (debug). The message was generated by component MSTP running in thread id 2110. The message was generated on Aug 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged. Messages logged to a collector or relay via syslog have an identical format to the above message.

Number of log messages displayed: For the message log, only the latest 64 entries are displayed on the web page.

2. Click **Clear** to clear the messages out of the buffered log in the memory.
3. Click **Refresh** to update the page with the latest messages in the log.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you change the buffered log settings, click **Apply** to apply the changes to the system. To preserve the changes after a system reboot, you must perform a save.

FLASH Log Configuration

The persistent log is a log that is stored in persistent storage, which means that the log messages are retained across a switch reboot.

- The first log type is the ***system startup log***. The system startup log stores the first N messages received after system reboot. This log always has the log full operation attribute set to stop on full and can store up to 32 messages.
- The second log type is the ***system operation log***. The system operation log stores the last N messages received during system operation. This log always has the log full operation attribute set to overwrite. This log can store up to 1000 messages.

Either the system startup log or the system operation log stores a message received by the log subsystem that meets the storage criteria, but not both. In other words, on system startup, if the startup log is configured, it stores messages up to its limit. The operation log, if configured, then begins to store the messages.

Use the FLASH Log Configuration page to enable or disable persistent logging and to set the severity filter.

To access the FLASH Log Configuration page:

1. Click the **Monitoring > Logs** tab, and then click the **FLASH Log** link.

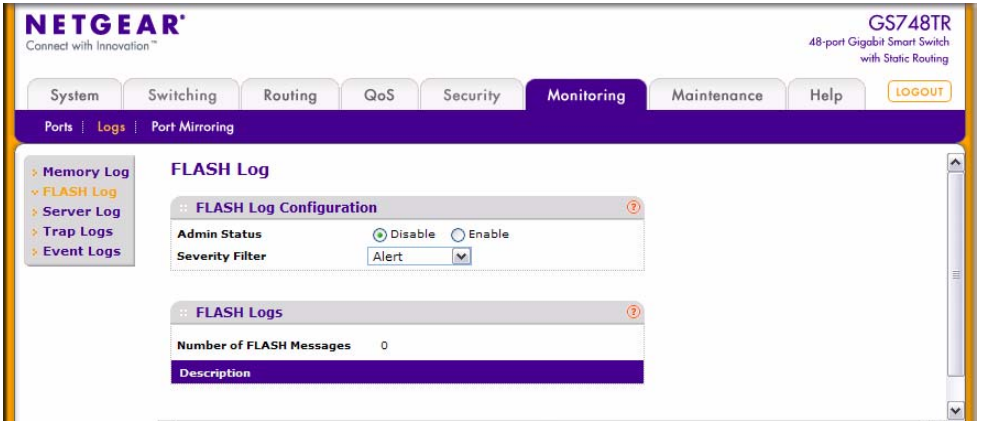


Figure 7-6

Table 7-7. FLASH Log Configuration Fields

Field	Description
Admin Status	Enable or disable logging by selecting the corresponding check box. The default is **Disable**. • **Enable:** A log that is 'Enabled' logs messages. • **Disable:** A log that is 'Disabled' does not log messages.
Severity Filter	A log records messages equal to or above a configured severity threshold. Use the menu to select the severity of the logs. For example, if you select **Error**, the logged messages include **Error**, **Critical**, **Alert**, and **Emergency**. The default severity level is **Alert(1)**. The severity can be one of the following levels: • **Emergency (0):** The highest level warning level. If the device is down or not functioning properly, an emergency log is saved to the device. • **Alert (1):** The second highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down. Action must be taken immediately. • **Critical (2):** The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional. • **Error (3):** A device error has occurred, such as if a port is offline. • **Warning (4):** The lowest level of a device warning. • **Notice (5):** Normal but significant conditions. Provides the network administrators with device information. • **Info (6):** Provides device information. • **Debug (7):** Provides detailed information about the log. Debugging should only be entered by qualified support personnel.

The rest of the page displays the persistent log messages.

Table 7-8. FLASH Log Fields

Field	Description
Number of FLASH Messages	Shows the number of persistent messages the system has logged.

2. Click **Clear** to clear the messages out of the buffered log.
3. Click **Refresh** to refresh the page with the most current data from the switch.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make any changes to the page, click **Apply** to apply the change to the system.

Server Log Configuration

Use the Server Log Configuration page to allow the switch to send log messages to the remote logging hosts configured on the system.

To access the Server Log Configuration page:

1. Click the **Monitoring** > **Logs** tab, and then click the **Server Log** link.

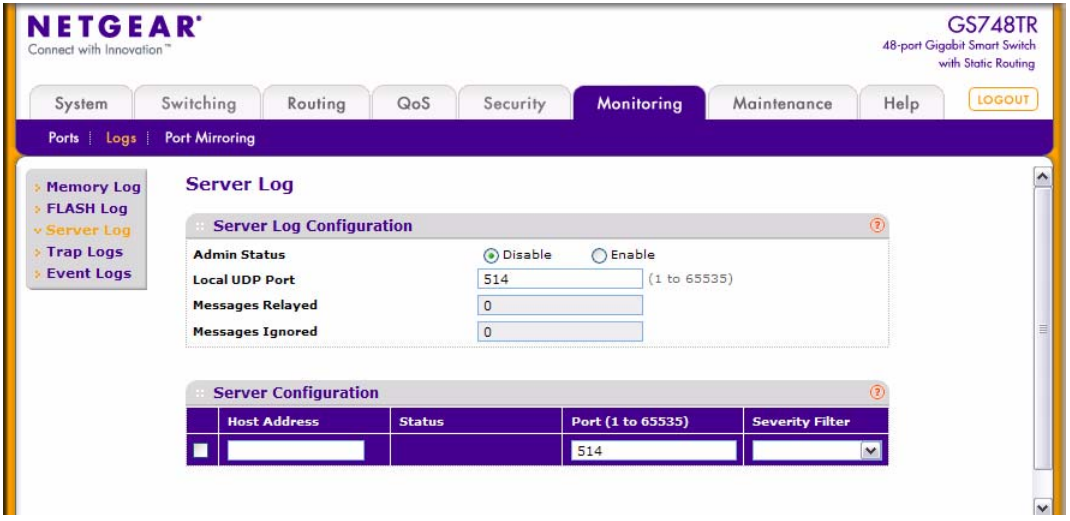


Figure 7-7

Table 7-9. Server Log Configuration Fields

Field	Description
Admin Status	Specifies whether to send log messages to the remote syslog hosts configured on the switch: • **Enable:** Messages will be sent to all configured hosts (syslog collectors or relays) using the values configured for each host. • **Disable:** Stops logging to all syslog hosts. Disable means no messages will be sent to any collector/relay.
Local UDP Port	Specifies the port on the switch from which syslog messages are sent. The default port is 514.
Messages Relayed	The number of messages forwarded by the syslog function to a syslog host. Messages forwarded to multiple hosts are counted once for each host.
Messages Ignored	The number of messages that were ignored.

The Server Log Configuration page also contains the Server Configuration table.

Table 7-10. Host Configuration Fields

Field	Description
Host Address	Enter the IP address or hostname of the host configured for syslog.
Status	Shows whether the remote logging host is currently active.
Port	Identifies the port on the host to which syslog messages are sent. The default port is 514. Specify the port in the text field.
Severity Filter	Use the menu to select the severity of the logs to send to the logging host. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert(1). The severity can be one of the following levels: • **Emergency (0):** The highest level warning level. If the device is down or not functioning properly, an emergency log is saved to the device. • **Alert (1):** The second highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down. • **Critical (2):** The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional. • **Error (3):** A device error has occurred, such as if a port is offline. • **Warning (4):** The lowest level of a device warning. • **Notice (5):** Provides the network administrators with device information. • **Informational (6):** Provides device information. • **Debug (7):** Provides detailed information about the log. Debugging should only be entered by qualified support personnel.

2. To add a remote logging host, enter the appropriate information into the Host Configuration table and click **Add**.
3. To delete an existing host, select the check box next to the host and click **Delete**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make any changes to the Server Log Configuration information, click **Apply** to apply the change to the system.
6. To modify the settings for an existing host, select the check box next to the host, change the desired information, and click **Apply**.

Trap Logs

Use the Trap Logs page to view information about the SNMP traps generated on the switch.

To access the Trap Logs page:

1. Click the **Monitoring > Logs** tab, and then click the **Trap Logs** link.

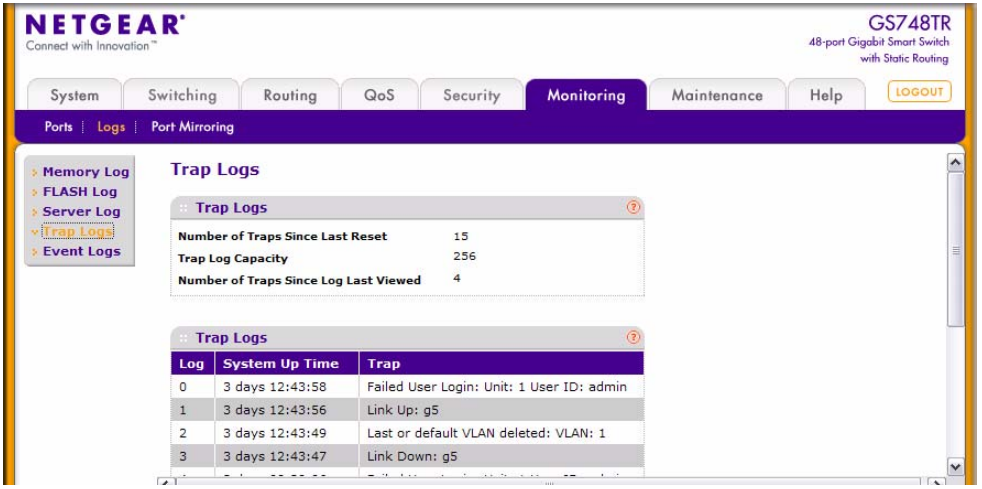


Figure 7-8

Table 7-11. Trap Log Statistics

Field	Description
Number of Traps Since Last Reset	The number of traps that have occurred since the switch last reboot.
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries will overwrite the oldest entries.
Number of Traps Since Log Last Viewed	The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, Web display, upload file from switch etc.) will cause this counter to be cleared to 0.

The page also displays information about the traps that were sent.

Table 7-12. Trap Logs

Field	Description
Log	The sequence number of this trap.
System Up Time	The time at which this trap occurred, expressed in days, hours, minutes and seconds since the last reboot of the switch.
Trap	Information identifying the trap.

2. Click **Clear Counters** to clear all the counters. This resets all statistics for the trap logs to the default values.

Event Logs

Use the Event Log page to display the event log, which is used to hold error messages for catastrophic events. After the event is logged and the updated log is saved in flash memory, the switch will be reset. The log can hold at least 2,000 entries and is erased when an attempt is made to add an entry after it is full. The event log is preserved across system resets.

To access the Event Log page:

1. Click the **Monitoring** > **Logs** tab, and then click the **Event Logs** link.

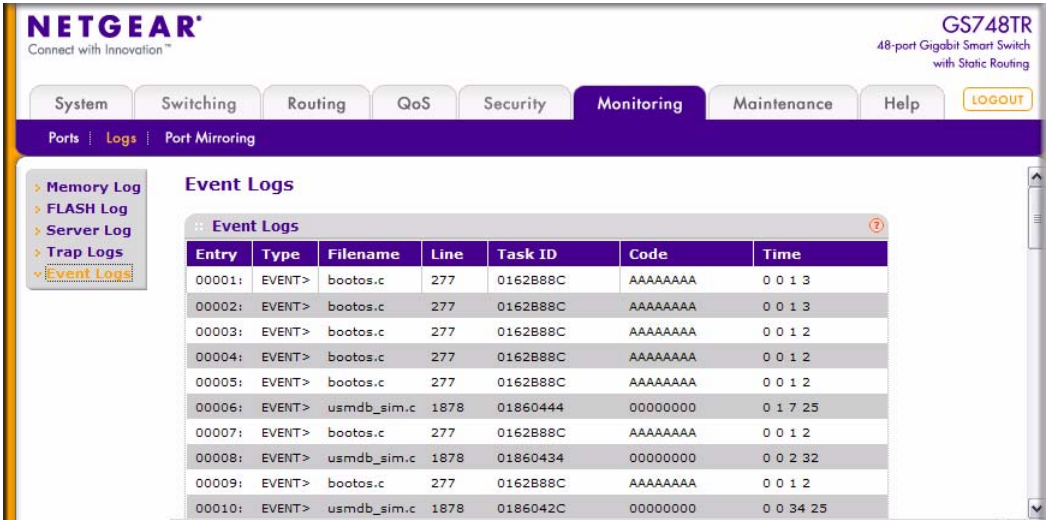


Figure 7-9

Table 7-13. Event Log Fields

Field	Description
Entry	The number of the entry within the event log. The most recent entry is first.
Type	Specifies the type of entry.
Filename	The GS700TR Smart Switch source code filename identifying the code that detected the event.
Line	The line number within the source file of the code that detected the event.
Task ID	The OS-assigned ID of the task reporting the event.
Code	The event code passed to the event log handler by the code reporting the event.
Time	The time the event occurred, measured from the previous reset.

2. Click **Clear** to clear the messages out of the Event Log.
3. Click **Refresh** to refresh the data on the screen and display the most current information.

Configuring Port Mirroring

The page under the Mirroring link allows you to view and configure port mirroring on the system.

Multiple Port Mirroring

Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port. You have the ability to configure how traffic is mirrored on a source port. Packets that are received on the source port, that are transmitted on a port, or are both received and transmitted, can be mirrored to the destination port.

The packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN tagged or untagged as it is being transmitted on the source port.

Use the Multiple Port Mirroring page to define port mirroring sessions.

To access the Multiple Port Mirroring page:

1. Click **Monitoring** > **Port Mirroring** in the navigation menu.

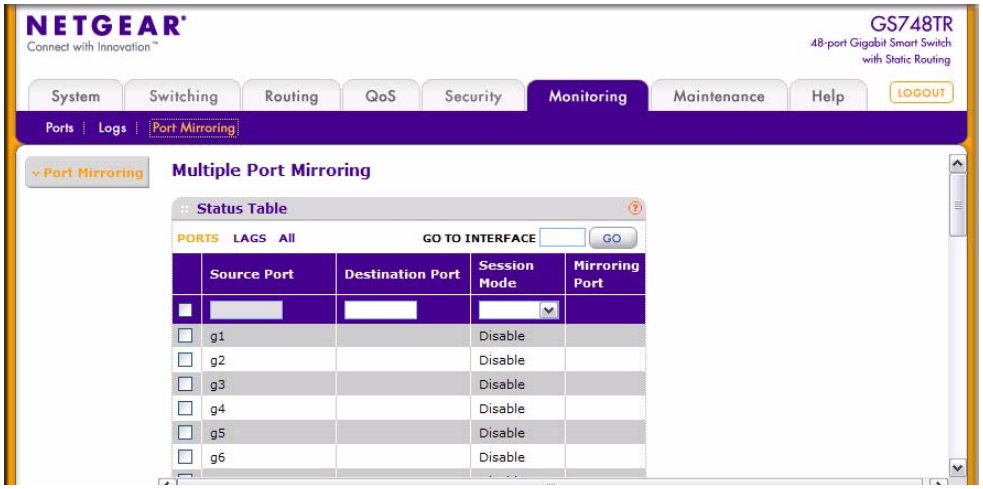


Figure 7-10

Table 7-14. Multiple Port Mirroring Fields

Field	Description
Source Port	Lists all the ports on the system. Select the check box next to a port to configure it as a source port.
Destination Port	After you select a source port, enter the port to which port traffic may be copied in g1, g2,...format. You can only configure one destination port on the system.
Session Mode	Select Enable to turn on Multiple Port Mirroring. Select Disable to turn off port mirroring. The session mode is a global value.
Mirroring Port	If the port is configured as a source port, the field value is Mirrored.

2. To delete a mirrored port, select the check box next to the mirrored port, and then click **Delete**.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. To add a mirrored port, select the source port, enter the destination port number (g1, g2,...) in the Destination port field. Select Enable from the Session Mode menu, and then click **Apply**.

Chapter 8
Maintenance

The Maintenance tab contains links to the following pages that help you manage the switch:

Save All Applied Changes

When you click **Apply**, the changes are applied to the system and saved in the running configuration file. However, these changes are not saved to non-volatile memory and will be lost if the system resets. Use the Save All Applied Changes page to make the changes you submit persist across a system reset.

To access the Save All Applied Changes page:

1. Click **Maintenance > Save Config > Save Configuration** in the navigation tree.

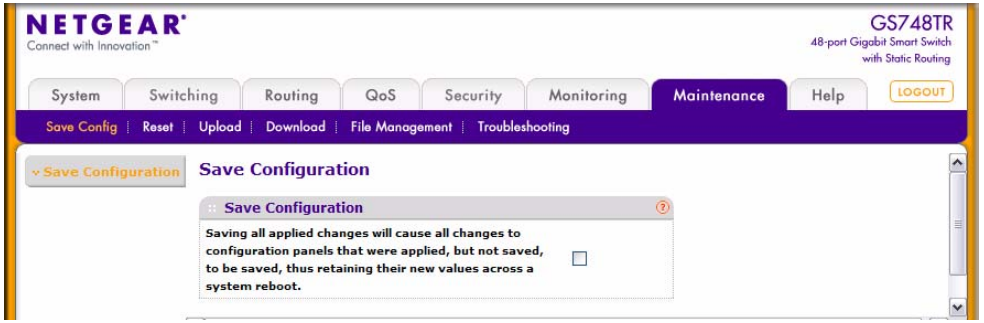


Figure 8-1

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Apply** to save all changes applied to the system to NVRAM so that they are retained if the system reboots.

System Reset

Use the Device Reboot page to reboot the system.

To access the Device Reboot page:

1. Click **Maintenance > Reset > Device Reboot** in the navigation tree.

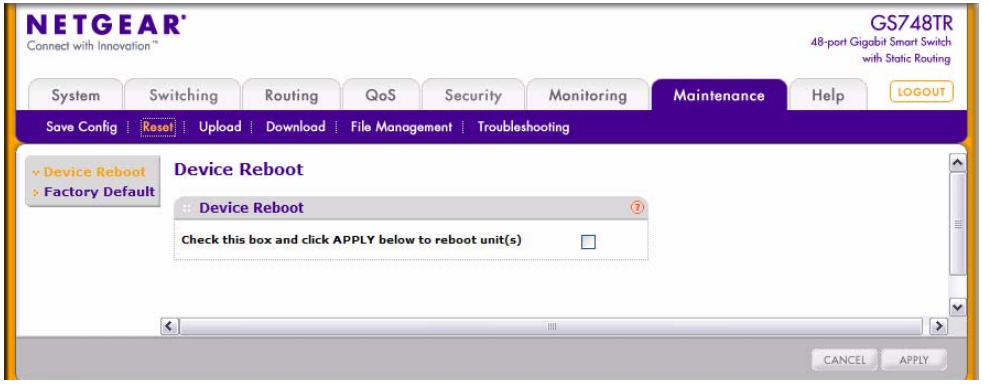


Figure 8-2

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

Reset Configuration to Defaults

Use the Factory Default page to reset the system configuration to the factory default values.

Note: For information about configuring network information, see "Connecting the Switch to the Network" on page 1-1.

To access the Factory Defaults page:

1. Click **Maintenance** > **Reset** > **Factory Default** in the navigation tree.

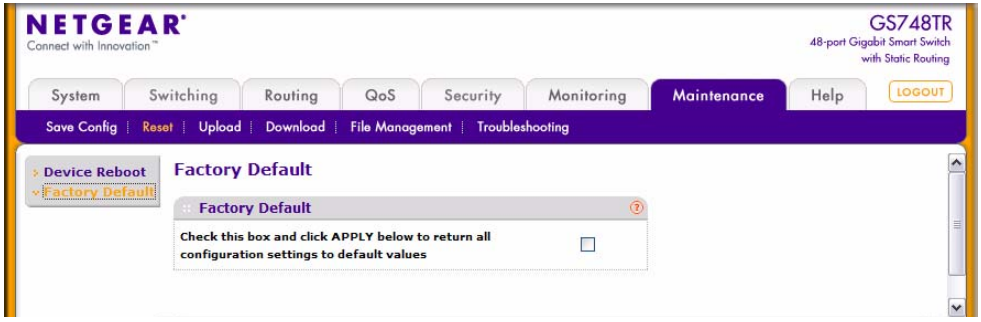


Figure 8-3

2. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Apply** to restore the factory default settings. The action takes place immediately.

Upload File From Switch

Use the File Upload page to upload configuration (ASCII) and image (binary) files from the switch to the TFTP server.

To display the File Upload page:

1. Click **Maintenance** > **Upload** > **File Upload** in the navigation tree.

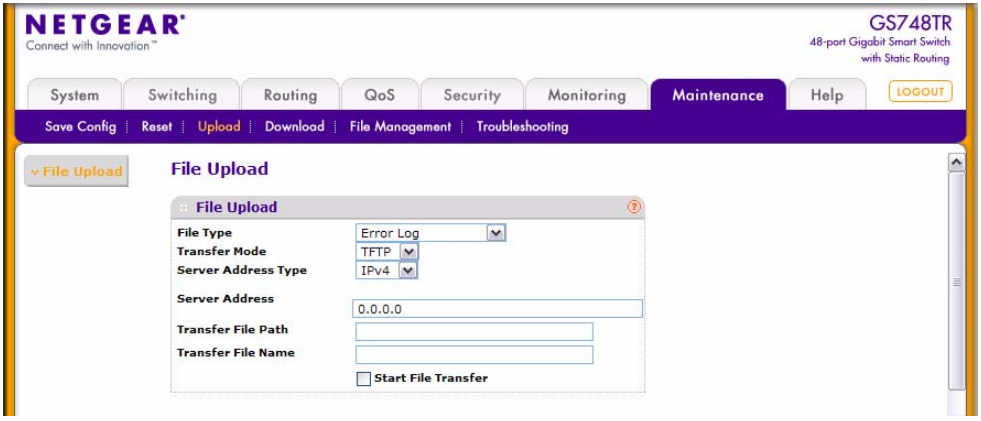


Figure 8-4

Table 8-1. Upload File from Switch Fields

Field	Description
File Type	Specify the type of file you want to upload: • **Code:** Retrieves a stored code image. • **Text Configuration**: Retrieves the text configuration file startup-config. • **Error Log:** Retrieves the system error (persistent) log, sometimes referred to as the event log. • **Buffered Log:** Retrieves the system buffered (in-memory) log. • **Trap Log:** Retrieves the system trap records. The default is **Error Log**.
Image Name	Specify the code image to upload, either image1 or image2. This field is only visible when **Code** is selected as the File Type. The factory default is image1.
Transfer Mode	Specify what protocol to use to transfer the file: • **TFTP**. Trivial File Transfer Protocol.
Server Address Type	Specify either **IPv4** or **DNS** address to indicate the format of the TFTP Server Address field. The factory default is **IPv4**.
Server Address	Enter the IP address of the TFTP server in accordance with the format indicated by the TFTP Server Address Type. The factory default is the IPv4 address **0.0.0.0**.
Transfer File Path	Enter the path on the TFTP server where you want to put the file. You may enter up to 32 characters. The factory default is blank.

Table 8-1. Upload File from Switch Fields (continued)

Field	Description
Transfer File Name	Enter a destination file name for the file to upload. You may enter up to 32 characters. The factory default is blank.
Start File Transfer	To initiate the file upload, check this box before clicking **Apply**.

The last row of the table is used to display information about the progress of the file transfer. The page will refresh automatically until the file transfer completes.

Uploading Files

Use the following procedures to upload a file from the switch to a TFTP server.

1. From the **File Type** field, select the type of file to copy from the switch to the TFTP server.
2. If you are uploading a GS700TR Smart Switch image (**Code**), select the image on the switch to upload. If you are uploading another type of file, the **Image Name** field is not available.
3. Complete the **Server Address Type**, **Server IP Address,** and **Transfer File Name** (full path without TFTP server IP address) fields.
4. Click the **Start File Transfe**r check box, and then click **Apply**.
5. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.

Download File To Switch (TFTP)

Use the Download File to Switch page to download device software, the image file, the configuration files and SSL files from a TFTP server to the switch.

You can also download files via HTTP. See “HTTP File Download” on page 8-8 for more information.

To access the TFTP File Download page:

1. Click **Maintenance** > **Download** > **TFTP File Download** in the navigation tree.

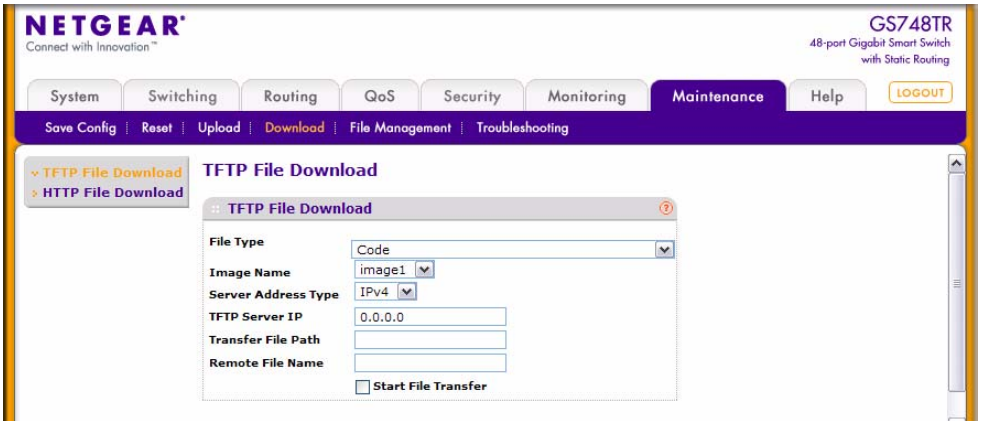


Figure 8-5

Table 8-2. Download File to Switch Fields

Field	Description
File Type	Specify what type of file you want to download to the switch: • **Code:** The code is the system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy; while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process. • **Text Configuration**: A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for Smart Switch to understand. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (i.e., change the device name, serial number, IP address, etc.), and download it to that device. • **SSL Trusted Root Certificate PEM File:** SSL Trusted Root Certificate File (PEM Encoded). • **SSL Server Certificate PEM File:** SSL Server Certificate File (PEM Encoded). • **SSL DH Weak Encryption Parameter PEM File:** SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded). • **SSL DH Strong Encryption Parameter PEM File:** SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).

Table 8-2. Download File to Switch Fields (continued)

Field	Description
Image Name	Specify the code image you want to download, either image1 or image2. This field is only visible when **Code** is selected as the File Type. The factory default is **image1**.
Transfer Mode	Specifies the protocol to be used for the transfer.
Server Address Type	Specify either IPv4 or DNS address to indicate the format of the TFTP Server Address field. The factory default is **IPv4**.
TFTP Server IP	Enter the IP address of the TFTP server in accordance with the format indicated by the TFTP Server Address Type. The factory default is the IPv4 address **0.0.0.0**.
Transfer File Path	Enter the path on the TFTP server where the selected file is located. You may enter up to 32 characters. The factory default is blank.
Remote File Name	Enter the name of the file you want to download from the TFTP server. You may enter up to 32 characters. The factory default is blank.
Start File Transfer	To initiate the download, check this box before clicking **Submit**.

2. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.

Downloading a File to the Switch

Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.

Use the following procedures to download a file from a TFTP server to the switch.

1. From the **File Type** field, select the type of file to download.
2. If you are downloading a GS700TR Smart Switch image (Code), select the image on the switch to overwrite. If you are downloading another type of file, the **Image Name** field is not available.

Note: It is recommended that you not overwrite the active image. The system will display a warning that you are trying to overwrite the active image.

3. Verify the IP address of the TFTP server and ensure that the software image or other file to be downloaded is available on the TFTP server.
4. Complete the **Server Address Type**, **TFTP Server IP Address** and **Remote File Name** (full path without TFTP server IP address) fields.
5. Click the Start File Transfer check box, and then click **Apply**.
6. After you click **Apply**, the screen refreshes and a "File transfer operation started" message appears. After the software is downloaded to the device, a message appears indicating that the file transfer operation completed successfully.

To activate a software image that you download to the switch, see "Dual Image Configuration" on page 8-9.

HTTP File Download

Use the HTTP File Download page to download files of various types to the switch using an HTTP session (i.e., via your web browser).

To display this page:

1. Click **Maintenance > Download > HTTP File Download** in the navigation menu.

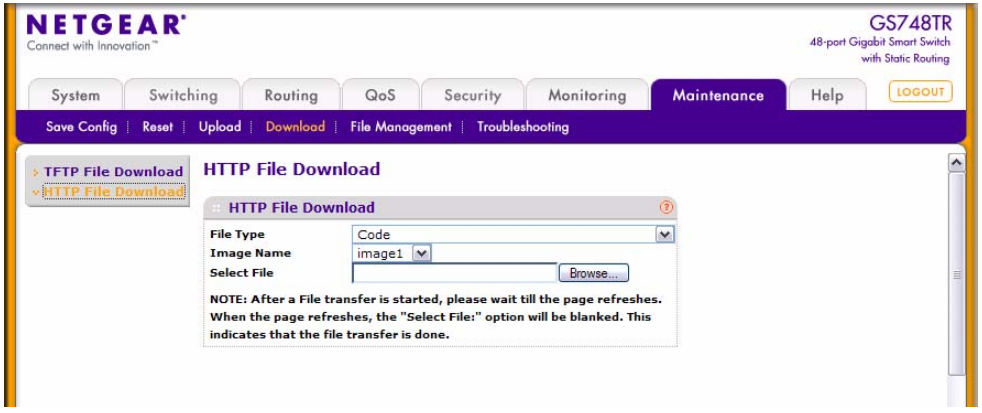


Figure 8-6

Table 8-3. HTTP File Download Fields

Field	Description
File Type	Specify the type of file you want to download: • **Code**: Choose this option to upgrade the operational software in flash (default). • **Configuration**: Choose this option to update the switch's configuration. If the file has errors the update will be stopped. • **SSL Trusted Root Certificate PEM File**: SSL Trusted Root Certificate File (PEM Encoded) • **SSL Server Certificate PEM File**: SSL Server Certificate File (PEM Encoded) • **SSL DH Weak Encryption Parameter PEM File**: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded) • **SSL DH Strong Encryption Parameter PEM File**: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)
Image Name	Specify the code image you want to download, either **image1** (the default) or **image2**. This field is only visible when **Code** is selected as the File Type.
Select File	Enter the path and filename or browse for the file you want to download. You may enter up to 80 characters.

2. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
3. Click the **Apply** button to initiate the file download.

Note: After a file transfer is started, please wait until the page refreshes. When the page refreshes, the “Select File” option will be blanked out. This indicates that the file transfer is done.

Dual Image Configuration

The system maintains two versions of the GS700TR Smart Switch software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded during subsequent switch restarts. This feature reduces switch down time when upgrading/ downgrading the GS700TR Smart Switch software.

The system running an older software version will ignore (not load) a configuration file created by the newer software version. When a configuration file created by the newer software version is discovered by the system running an older version of the software, the system will display an appropriate warning to the user.

Use the Dual Image Configuration page to set the boot image.

To display the Dual Image Configuration page:

1. Click **Maintenance > File Management > Dual Image > Dual Image Configuration** in the navigation menu.

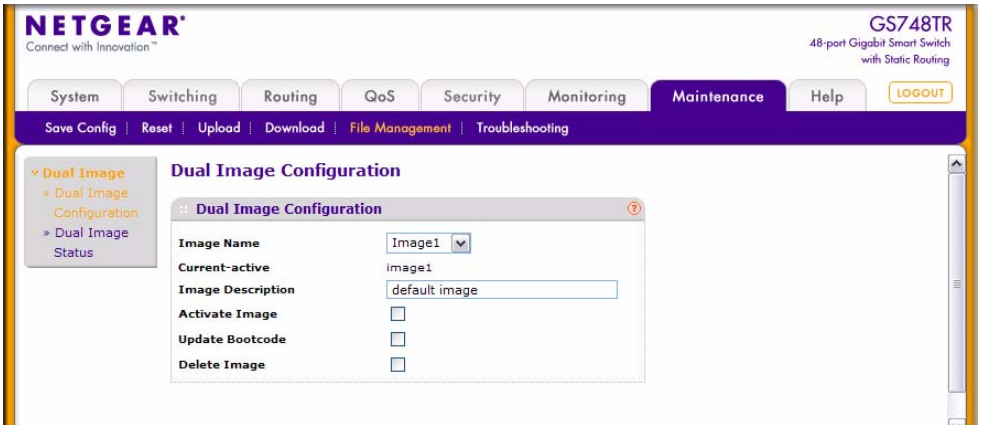


Figure 8-7

The Active Image page contains the following fields:

Table 8-4. Dual Image Configuration Fields

Field	Description
Image Name	Select image1 or image2 from the dropdown menu to display or configure information about that software image.
Current Active	Displays name of current active image.
Image Description	If desired, enter a descriptive name for the software image.

2. Click **Activate Image** to make the image that is selected in the **Image Name** field the next active image for subsequent reboots.

Note: After activating an image, you must perform a system reset of the switch in order to run the new code.

3. If the file you uploaded contains the boot loader code only, click **Update Bootcode**.
4. Click **Refresh** to reload the page and display the most current information.

5. Click **Delete Image** to remove the selected image from permanent storage on the switch.You cannot delete the active image.
6. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
7. Click **Apply** to update the image description on the switch.

Viewing the Dual Image Status

The Dual Image feature allows the switch to have two GS700TR Smart Switch software images in the permanent storage. One image is the active image, and the second image is the backup. This feature reduces the system down-time during upgrades and downgrades. You can use the Dual Image Status page to view information about the system images on the device.

To display the Dual Image Status page:

1. Click **Maintenance** > **File Management > Dual Image Status > Dual Image Status** in the navigation menu.

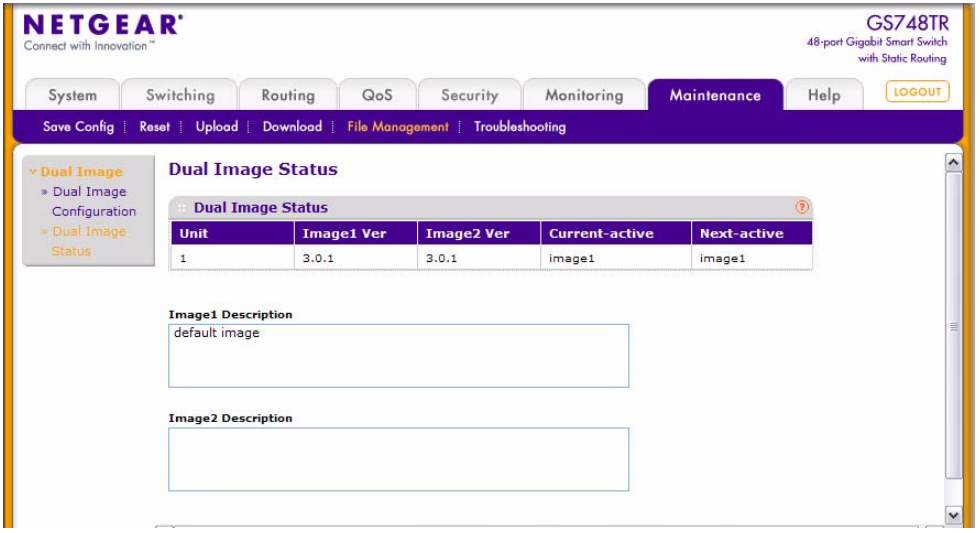


Figure 8-8

Table 8-5. Dual Image Status Fields

Field	Description
Unit	Displays the unit ID of the switch.
Image1 Ver	Displays the version of the image1 code file.
Image2 Ver	Displays the version of the image2 code file.
Current-active	Displays the currently active image on this unit.
Next-active	Displays the image to be used on the next restart of this unit.
Image1 Description	Displays the description associated with the image1 code file.
Image2 Description	Displays the description associated with the image2 code file.

2. Click **Refresh** to display the latest information from the router.
3. For information about how to update or change the system images, see "Dual Image Configuration" on page 8-9.

Ping

Use the Ping page to tell the switch to send a Ping request to a specified IP address. You can use this feature to check whether the switch can communicate with a particular network host.

To access the Ping page:

1. Click **Maintenance** > **Troubleshooting** > **Ping** in the navigation menu.

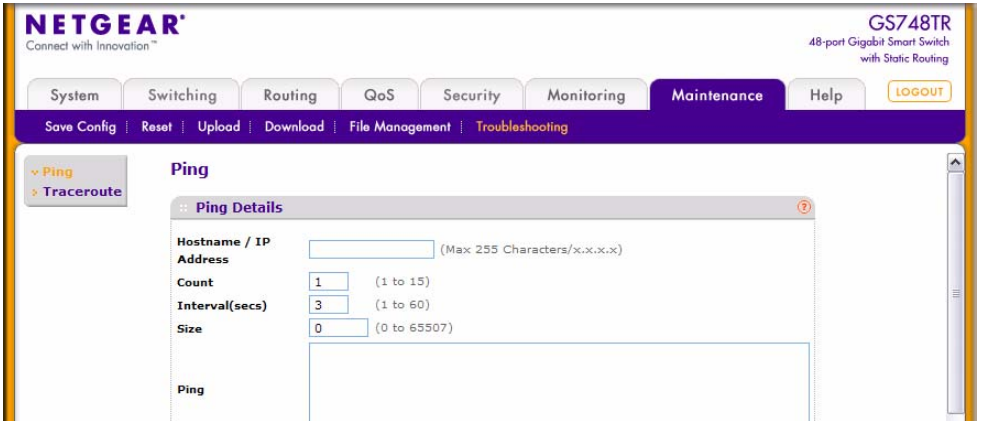


Figure 8-9

Table 8-6. Ping Fields

Field	Description
Hostname/IP Address	Enter the IP address or the host name of the station you want the switch to ping. The initial value is blank. This information is not retained across a power cycle.
Count	Specify the number of pings to send. The valid range is 1 to 15.
Interval	Specify the number of seconds between pings sent. The valid range is 1 to 60.
Size	Specify the size of the ping packet to send. The valid range is 0 to 65507.
Ping	Displays the results of the ping.

2. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Apply** to send the ping. The switch will send the number of pings configured and the results will be displayed below the configurable data.
   - If successful, you will see "Reply From IP/Host: icmp_seq = 0. time = xx usec. Tx = x, Rx = x Min/Max/Avg RTT = x/x/x msec"
   - If a reply to the ping is not received, you will see "Reply From IP/Host: Destination Unreachable. Tx = x, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec"

TraceRoute

You can use the TraceRoute utility to discover the paths that a packet takes to a remote destination.

To display this page:

1. Click **Maintenance** > **Troubleshooting** > **TraceRoute** in the navigation tree.

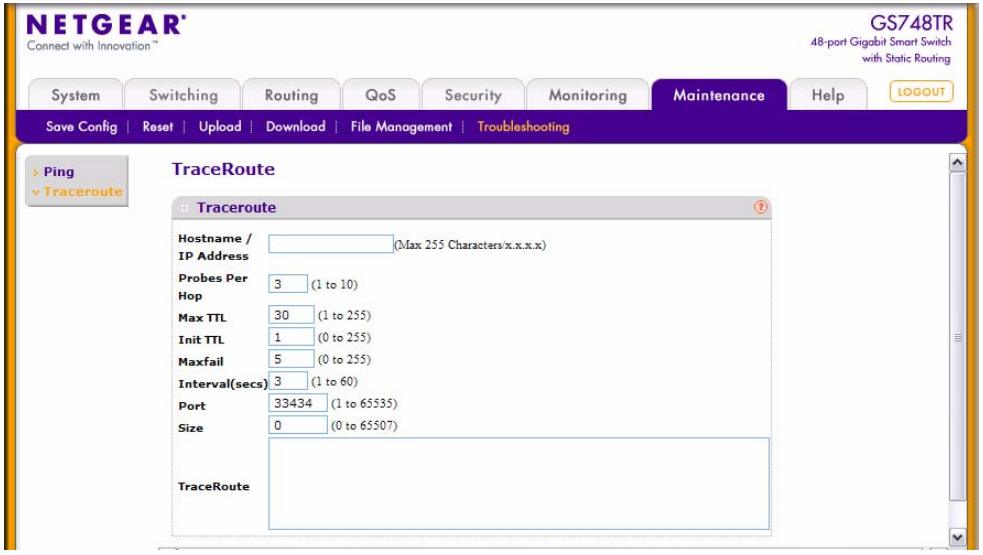


Figure 8-10

Table 8-7. TraceRoute Fields

Field	Definition
Hostname/IP Address	Enter the IP address or the hostname of the station you want the switch to discover path for.
Probes Per Hop	Enter the number of times each hop should be probed. The valid range is 1 to 10.
MaxTTL	Enter the maximum time-to-live for a packet in number of hops. The valid range is 1 to 255.
InitTTL	Enter the initial time-to-live for a packet in number of hops. The valid range is 0 to 255.
MaxFail	Enter the maximum number of failures allowed in the session. The valid range is 0 to 255.
Interval	Enter the time between probes in seconds. The valid range is 1 to 60.
Port	Enter the UDP destination port in probe packets. The valid range is 1 to 65535.
Size	Enter the size of probe packets. The valid range is 0 to 65507.
TraceRoute	Displays the output from a traceroute.

2. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Apply** to initiate the traceroute. The results display in the TraceRoute box.