



NETGEAR[®]

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches Software Administration Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

February 2012
202-10995-01
v1.0

©2012 NETGEAR, Inc. All rights reserved

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at

<http://support.netgear.com>

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): Check the list of phone numbers at

http://support.netgear.com/app/answers/detail/a_id/984

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2012 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve 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.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10995-01	v1.0	February 2012	First publication

Contents

Chapter 1 Getting Started

Getting Started with the Smart Switches	10
Switch Management Interface	10
Connecting the Switch to the Network	11
Switch Discovery in a Network with a DHCP Server	12
Switch Discovery in a Network without a DHCP Server	14
Configuring the Network Settings on the Administrative System	15
Web Access	16
Smart Control Center Utilities	17
Network Utilities	17
Configuration Upload and Download	19
Firmware Upgrade	20
Viewing and Managing Tasks	22
Understanding the User Interfaces	23
Using the Web Interface	23
Using SNMP	29
Interface Naming Convention	30

Chapter 2 Configuring System Information

Management	31
System Information	32
Slot Information	33
IP Configuration	35
IPv6 Network Configuration	37
IPv6 Network Neighbor	38
Time	40
Denial of Service	45
DNS	49
Green Ethernet	51
Stacking	61
Stack Features	61
Firmware Synchronization and Upgrade	62
Configuration Maintenance	62
Stack Master Election	62
Factory Defaults Reset Behavior	63
Stack Configuration	63
Stack Port Configuration	66
Stack Port Diagnostics	68
Stack Firmware Synchronization	69

PoE/PoE+ (GS728TPS and GS752TPS Only)	70
PoE Configuration	70
PoE Port Configuration	72
SNMP	75
SNMPv1/v2	75
Trap Configuration	77
Trap Flags	78
SNMP Supported MIBs	79
SNMP v3 User Configuration	79
LLDP	80
LLDP Configuration	81
LLDP Port Settings	82
LLDP-MED Network Policy	83
LLDP-MED Port Settings	85
Local Information	86
Neighbors Information	88
Services — DHCP Snooping	92
DHCP Snooping Global Configuration	93
Interface Configuration	94
Binding Configuration	95
Persistent Configuration	97
Statistics	98
Timer Schedule (GS728TPS and GS752TPS Only)	99
Timer Global Configuration	99
Timer Schedule Configuration	100

Chapter 3 Configuring Switching Information

Ports	102
Port Configuration	102
Flow Control	104
Link Aggregation Groups	105
LAG Configuration	105
LAG Membership	107
LACP Configuration	108
LACP Port Configuration	109
VLANs	110
VLAN Configuration	110
VLAN Membership Configuration	112
Port VLAN ID Configuration	113
MAC Based VLAN	114
Protocol Based VLAN Group Configuration	115
Protocol Based VLAN Group Membership	116
Voice VLAN	118
Voice VLAN Properties	118
Voice VLAN Port Setting	119
Voice VLAN OUI	120
Auto-VoIP	121

Spanning Tree Protocol	122
STP Switch Configuration	123
CST Configuration	125
CST Port Configuration	126
CST Port Status	128
Rapid STP	129
MST Configuration	130
MST Port Configuration	131
STP Statistics	134
Multicast	135
MFDB	135
Auto-Video Configuration	137
IGMP Snooping	138
IGMP Snooping Querier	144
MLD Snooping	147
Forwarding Database	156
MAC Address Table	156
Dynamic Address Configuration	158
Static MAC Address	159

Chapter 4 Configuring Routing

Configuring IP Settings	160
IP Configuration	161
IP Statistics	162
Configuring VLAN Routing	165
VLAN Routing Wizard	165
VLAN Routing Configuration	167
Configuring Router Discovery	168
Router Discovery Configuration	168
Configuring and Viewing Routes	169
Configuring ARP	171
ARP Cache	172
ARP Create	173
Global ARP Configuration	174
ARP Entry Management	175

Chapter 5 Configuring Quality of Service

Class of Service	177
Basic CoS Configuration	178
CoS Interface Configuration	179
Interface Queue Configuration	180
802.1p to Queue Mapping	182
DSCP to Queue Mapping	183
Differentiated Services	184
Defining DiffServ	184
Diffserv Configuration	185
Class Configuration	186

IPv6 Class Configuration	189
Policy Configuration	191
Service Configuration	195
Service Statistics	196

Chapter 6 Managing Device Security

Management Security Settings	197
Change Password	198
RADIUS Configuration	199
Configuring TACACS+	204
Authentication List Configuration	207
Configuring Management Access	210
HTTP Configuration	211
Secure HTTP Configuration	212
Certificate Management	213
Certificate Download	214
Access Profile Configuration	215
Access Rule Configuration	217
Port Authentication	218
802.1X Configuration	219
Port Authentication	220
Port Summary	224
Traffic Control	225
MAC Filter Configuration	225
MAC Filter Summary	227
Storm Control	228
Port Security Configuration	230
Port Security Interface Configuration	231
Security MAC Address	232
Protected Ports Membership	233
Configuring Access Control Lists	234
ACL Wizard	235
MAC ACL	237
MAC Rules	238
MAC Binding Configuration	240
MAC Binding Table	241
IP ACL	242
IP Rules	243
IP Extended Rule	245
IPv6 ACL	248
IPv6 Rules	249
IP Binding Configuration	252
IP Binding Table	254
VLAN Binding Table	255

Chapter 7 Monitoring the System

Ports	256
-----------------	-----

Switch Statistics	256
Port Statistics	259
Port Detailed Statistics	260
EAP Statistics	266
Cable Test	268
System Logs	270
Memory Logs	270
FLASH Log Configuration	272
Server Log Configuration	274
Trap Logs	276
Event Logs	277
Port Mirroring	278
Multiple Port Mirroring	278

Chapter 8 Maintaining the System

Reset	280
Device Reboot	280
Factory Default	281
Upload File From Switch	282
TFTP File Upload	282
HTTP File Upload	283
Download File To Switch	284
TFTP File Download	285
HTTP File Download	287
File Management	288
Copy	288
Dual Image Configuration	289
Dual Image Status	291
Troubleshooting	292
Ping	292
Ping IPv6	293
Traceroute	294

Chapter 9 Accessing Help

Online Help	296
Support	296
User Guide	297
Registration	298

Appendix A Hardware Specifications and Default Values

Switch Specifications	300
GS728TS Specifications	300
GS728TPS Specifications	300
GS752TS Specifications	301
GS752TPS Specifications	301
Switch Performance	301

Switch Features and Defaults	302
Traffic Control	302
Quality of Service	303
Security	303
System Setup and Maintenance	304
System Management	304
Other Features	305

Appendix B Configuration Examples

Virtual Local Area Networks (VLANs)	306
VLAN Example Configuration	307
Access Control Lists (ACLs)	308
MAC ACL Example Configuration	309
Standard IP ACL Example Configuration	310
Differentiated Services (DiffServ)	311
Class	312
DiffServ Traffic Classes	312
Creating Policies	313
DiffServ Example Configuration	314
802.1X	315
802.1X Example Configuration	317
MSTP	318
MSTP Example Configuration	320
Configuring VLAN Routing	322
Creating VLAN Routing Interfaces	322

Appendix C Notification of Compliance

Index

Getting Started

1

The *NETGEAR*®GS728TS, GS728TPS, GS752TS, and GS752TPS Smart Switch Software Administration Manual describes how to configure and operate the GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches by using the Web-based graphical user interface (GUI). This manual describes the software configuration procedures and explains the options available within those procedures.

Document Organization

The *GS728TS, GS728TPS, GS752TS, and GS752TPS Smart Switch Software Administration Manual* contains the following chapters:

- *Chapter 1, Getting Started*, contains information about performing the initial system configuration and accessing the user interface.
- *Chapter 2, Configuring System Information*, describes how to configure administrative features such as SNMP, DHCP, PoE, and Green Ethernet. It also describes how to configure stacking on the switches.
- *Chapter 3, Configuring Switching Information*, describes how to manage and monitor the layer 2 switching features.
- *Chapter 4, Configuring Routing*, describes how to manage and monitor IP routing.
- *Chapter 5, Configuring Quality of Service*, describes how to manage the Access Control Lists (ACLs), and how to configure Differentiated Services and Class of Service features.
- *Chapter 6, Managing Device Security*, contains information about configuring switch security information such as port access control and RADIUS server settings.
- *Chapter 7, Monitoring the System*, describes how to view a variety of information about the switch and its ports, and to configure how the switch monitors events.
- *Chapter 8, Maintaining the System*, describes features to help you manage the switch.
- *Chapter 9, Accessing Help*, describes how to access Online Help resources for the switch.
- *Appendix A, Hardware Specifications and Default Values*, contains hardware specifications and default values on the GS728TS, GS728TPS, GS752TS, and GS752TPS Smart Switches.

- [Appendix B, Configuration Examples](#), contains examples of how to configure various features on the GS728TS, GS728TPS, GS752TS, and GS752TPS Smart Switches, such as VLANs and ACLs.
- [Appendix C, Notification of Compliance](#), contains regulatory information about the GS728TS, GS728TPS, GS752TS, and GS752TPS Smart Switches.

Note: Refer to the release notes for the GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches for information about issues and workarounds.

Getting Started with the Smart Switches

This chapter provides an overview of starting your GS728TS, GS728TPS, GS752TS, or GS752TPS Smart Switch and accessing the user interface. It also leads you through the steps to use the Smart Control Center utility. This chapter contains the following sections:

- [Switch Management Interface](#) on page 10
- [Connecting the Switch to the Network](#) on page 11
- [Switch Discovery in a Network with a DHCP Server](#) on page 12
- [Switch Discovery in a Network without a DHCP Server](#) on page 14
- [Configuring the Network Settings on the Administrative System](#) on page 15
- [Web Access](#) on page 16
- [Smart Control Center Utilities](#) on page 17
- [Understanding the User Interfaces](#) on page 23
- [Interface Naming Convention](#) on page 30

Switch Management Interface

The NETGEAR GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches contain an embedded Web server and management software for managing and monitoring switch functions. Each switch can function as a simple switch without the management software. However, you can use the management software to configure more advanced features that can improve switch efficiency and overall network performance.

Web-based management lets you monitor, configure, and control your switch remotely using a standard Web browser instead of using expensive and complicated SNMP software products. From your Web browser, you can monitor the performance of your switch and optimize its configuration for your network. You can configure all switch features, such as VLANs, QoS, and ACLs by using the Web-based management interface.

NETGEAR provides the Smart Control Center utility with this product. This program runs under Microsoft® Windows® XP, Windows 2000, or Windows Vista® and provides a front end

that discovers the switches on your network segment (L2 broadcast domain). When you power up your switch for the first time, use the Smart Control Center to discover the switch and view the network information that has been automatically assigned to the switch by a DHCP server; or, if no DHCP server is present on the network, use the Smart Control Center to discover the switch and assign static network information.

In addition to enabling NETGEAR switch discovery, the Smart Control Center provides several utilities to help you maintain the NETGEAR switches on your network, such as password management, firmware upgrade, and configuration file backup. For more information, see [Smart Control Center Utilities](#) on page 17.

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 and configure it with network information (an IP address, subnet mask, and default gateway). The switch has a default IP address of 192.168.0.239 and a default subnet mask of 255.255.255.0.

Use one of the following three methods to change the default network information on the switch:

- Dynamic assignment through DHCP—DHCP is enabled by default on the switch. If you connect the switch to a network with a DHCP server, the switch obtains its network information automatically. You can use the Smart Control Center to discover the automatically-assigned network information. For more information, see [Switch Discovery in a Network with a DHCP Server](#) on page 12
- Static assignment through the Smart Control Center—If you connect the switch to a network that does not have a DHCP server, you can use the Smart Control Center to assign a static IP address, subnet mask, and default gateway. For more information, see [Switch Discovery in a Network without a DHCP Server](#) on page 14
- Static assignment by connecting from a local host—If you do not want to use the Smart Control Center to assign a static address, you can connect to the switch from a host (administrative system) in the 192.168.0.0/24 network and change the settings by using the Web-based management interface on the switch. For information about how to set the IP address on the administrative system so it is in the same subnet as the default IP address of the switch, see [Configuring the Network Settings on the Administrative System](#) on page 15.

Switch Discovery in a Network with a DHCP Server

This section describes how to set up your switch in a network that has a DHCP server. The DHCP client on the switch is enabled by default. When you connect it to your network, the DHCP server will automatically assign an IP address to your switch. Use the Smart Control Center to discover the IP address automatically assigned to the switch.

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

1. Connect the switch to a network with a DHCP server.
2. Power on the switch by connecting its AC-DC power adapter.
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click **Discover** for the Smart Control Center to find your switch. You should see a screen similar to the one shown in *Figure 1, Smart Switch Discovery*.

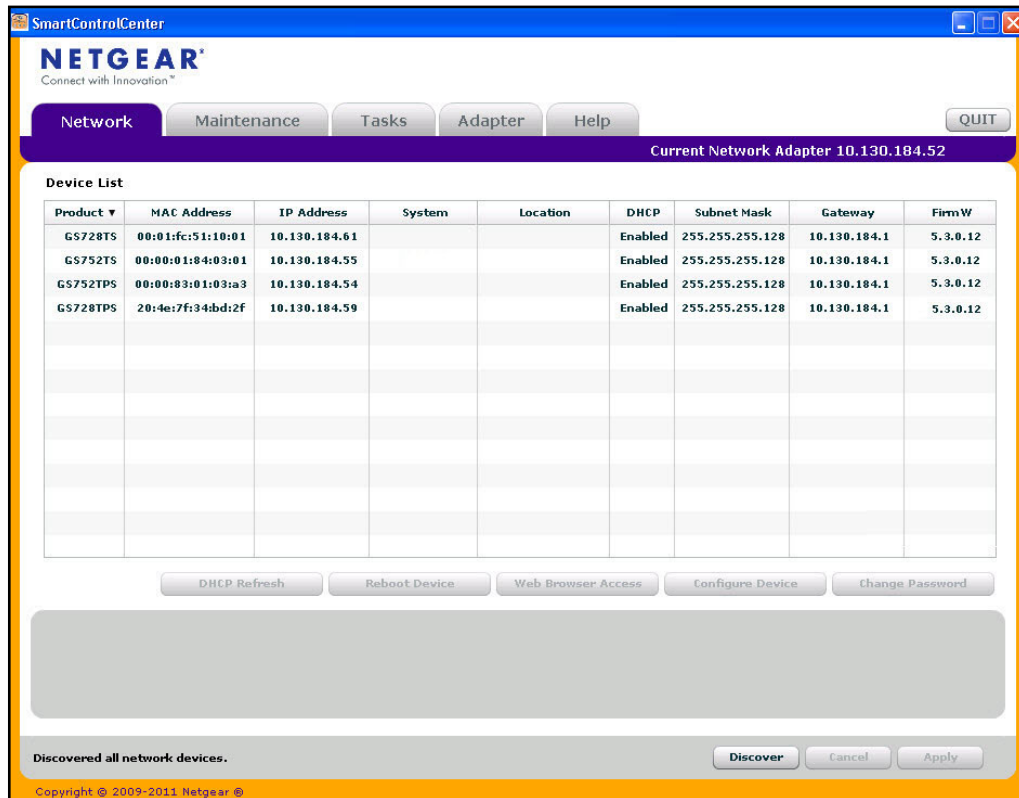
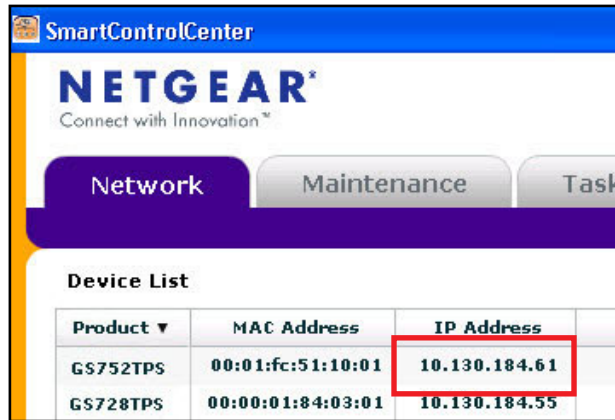
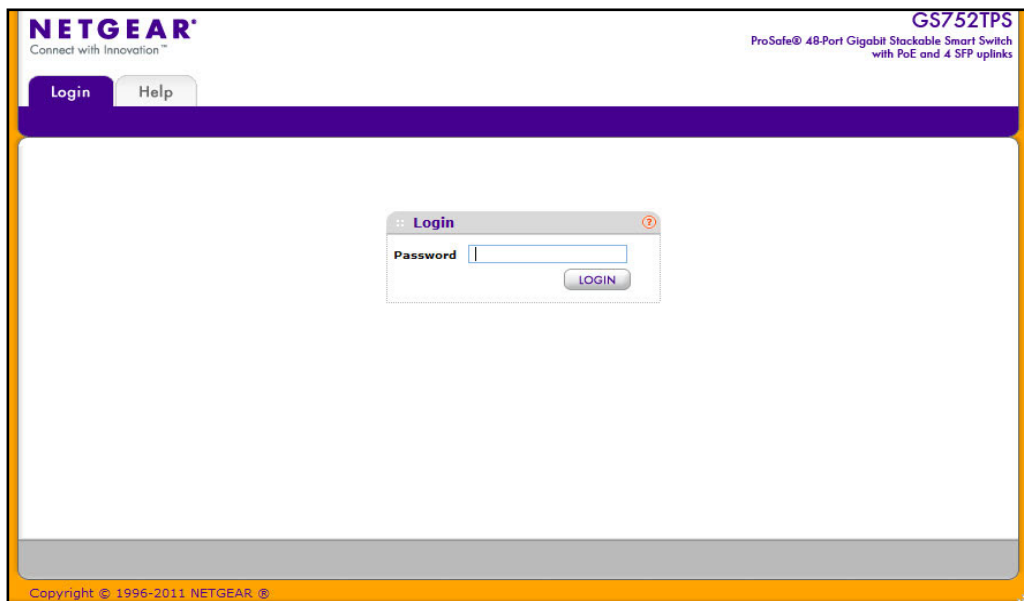


Figure 1. Smart Switch Discovery

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 Smart Control Center).



7. Select your switch by clicking the line that displays the switch, then click the **Web Browser Access** button. The Smart Control Center displays a login window similar to the following figure.



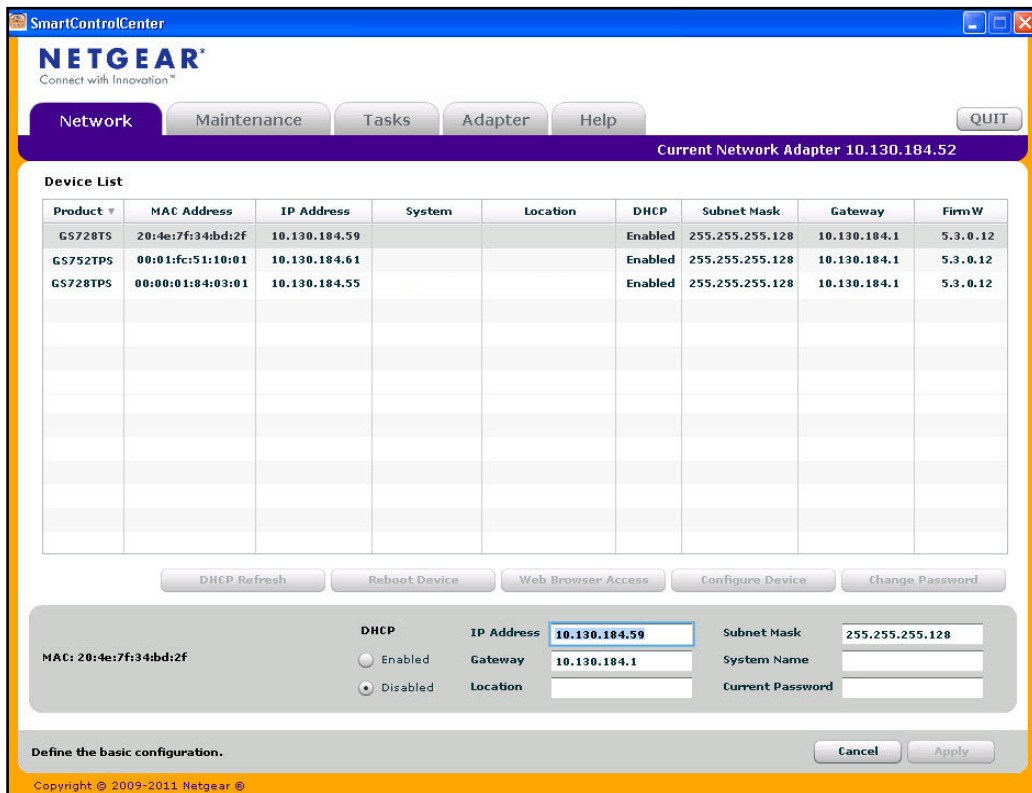
Use your Web browser to manage your switch. The default password is *password*. Then use this page to proceed to management of the switch covered in [Using the Web Interface](#) on page 23.

Switch Discovery in a Network without a DHCP Server

This section describes how to use the Smart Control Center to set up your switch in a network without a DHCP server. 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 switch to your existing network.
2. Power on the switch by plugging in the AC-DC power adapter.
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click **Discover** for the Smart Control Center to find your GS728TS, GS728TPS, GS752TS, or GS752TPS switch. The utility broadcasts Layer 2 discovery packets within the broadcast domain to discover the switch. You should see a screen similar to *Figure 1* on page 12.
6. Select the switch, then click **Configure Device**. The page expands to display additional fields at the bottom of the page, as the following figure shows.



7. Choose the **Disabled** radio box to disable DHCP.
8. Enter the static switch IP address, gateway IP address and subnet mask, and then type your password and click **Apply**.

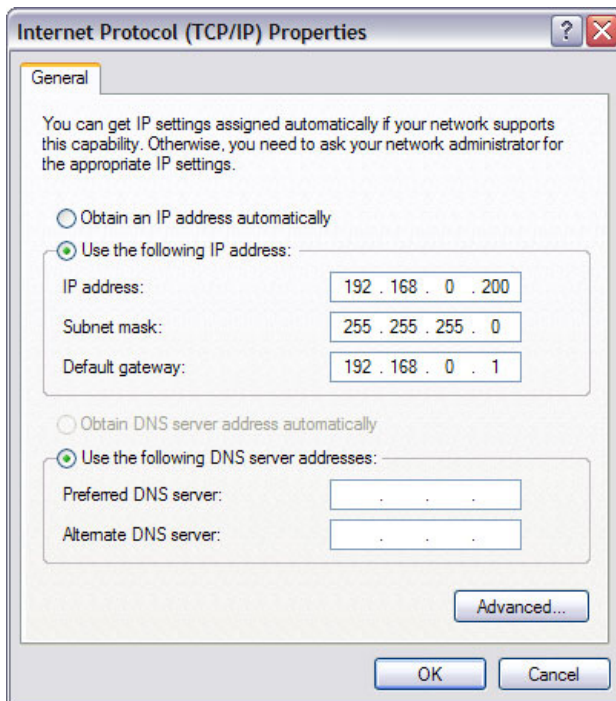
Tip: You must enter the current password every time you use the Smart Control Center to update the switch setting. The default password is *password*.

Please ensure that your PC and the switch are in the same subnet. Make a note of these settings for later use.

Configuring the Network Settings on the Administrative System

If you choose not to use the Smart Control Center to configure the network information on the switch, you can connect directly to the switch from an administrative system, such as a PC or laptop computer. The IP address of the administrative system must be in the same subnet as the default IP address on the switch. For most networks, this means you must change the IP address of the administrative system to be on the same subnet as the default IP address of the switch (192.168.0.239).

To change the IP address on an administrative system running a Microsoft® Windows® operating system, open the Internet Protocol (TCP/IP) properties screen that you access from the Local Area Connection properties, as shown in the following figure. You need Windows Administrator privileges to change these settings.





WARNING:

When you change the IP address of your administrative system, you will lose your connection to the rest of the network. Be sure to write down your current network address settings before you change them.

To modify the network settings on your administrative system:

1. On your PC, access the MS Windows operating system TCP/IP Properties.
2. Set the IP address of the administrative system to an address in the 192.168.0.0 network, such as 192.168.0.200. The IP address must be different from that of the switch but within the same subnet.
3. Click OK.

To configure a static address on the switch:

1. Use a straight-through cable to connect the Ethernet port on the administrative system directly to any port on the GS728TS, GS728TPS, GS752TS, or GS752TPS.
2. Open a Web browser on your PC and connect to the management interface as described in [Web Access](#) on page 16.
3. Change the network settings on the switch to match those of your network (this procedure is described in [IP Configuration on page 35](#)).

After you change the network settings on the switch, return the network configuration on your administrative system to the original settings.

Web Access

To access the GS728TS, GS728TPS, GS752TS, or GS752TPS management interface, use one of the following methods:

- From the Smart Control Center, select the switch and click **Web Browser Access**.
- Open a Web browser and enter the IP address of the switch in the address field.

You must be able to ping the IP address of the GS728TS, GS728TPS, GS752TS, or GS752TPS management interface from your administrative system for Web access to be available. If you used the Smart Control Center to set up the IP address and subnet mask, either with or without a DHCP server, use that IP address in the address field of your Web browser. If you did not change the IP address of the switch from the default value, enter 192.168.0.239 into the address field.

Clicking **Web Browser Access** on the Smart Control Center or accessing the switch directly from your Web browser displays the login screen shown in the following figure.

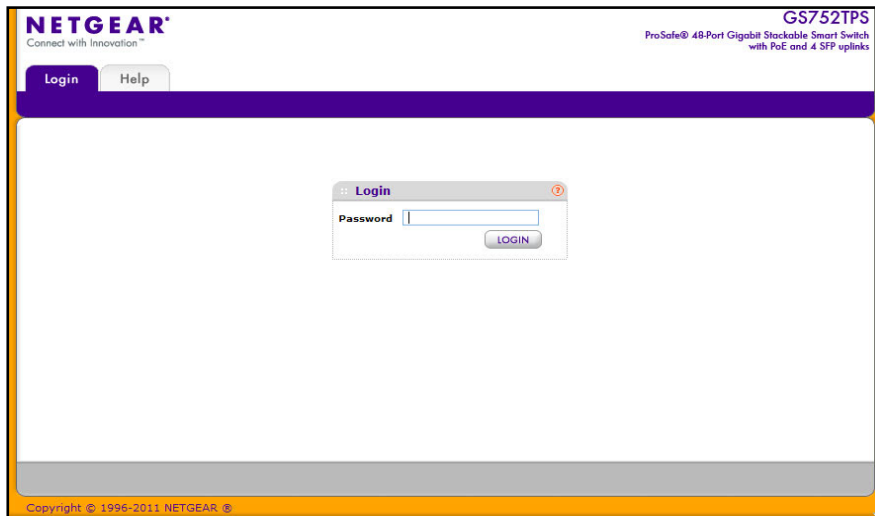


Figure 2. Login Screen

Smart Control Center Utilities

In addition to device discovery and network address assignment, the Smart Control Center includes several maintenance features. This section describes the following Smart Control Center utilities:

- *Network Utilities* on page 17
- *Configuration Upload and Download* on page 19
- *Firmware Upgrade* on page 20
- *Viewing and Managing Tasks* on page 22

Network Utilities

From the **Network** tab, you can perform the following functions:

- **DHCP Refresh**—Forces the switch to release the current bindings and request new address information from the DHCP server.
- **Reboot Device**—Reboots the selected device.
- **Web Browser Access**—Launches a Web browser and connects to the management interface for the selected device.
- **Configure Device**—Allows you to modify network information for the switch, including the IP address, DHCP client mode, system name, and location. For more information about this feature, see *Configuring the Device*.
- **Change Password**—Allows you to set a new password for the device. For more information about this feature, see *Changing the Switch Password*.

Configuring the Device

To modify switch information:

1. Select the switch.
2. Click **Configure Device**. Additional fields appear on the screen.

3. To assign or update a static IP address, default gateway, or subnet mask, disable the DHCP client and enter the new information. You can also specify a system name and location for the switch.
4. Type the password in the **Current Password** field. You cannot apply the changes without a valid switch password. The default password for the switch is *password*.
5. Click **Apply** to update the switch with the changes to the network information.

Changing the Switch Password

1. Select the switch.
2. Click **Change Password**. Additional fields appear on the screen.

3. Type the switch password in the **Current Password** field. The default password for the switch is *password*.
4. Type the new password in the **New Password** and **Confirm Password** fields. The password can contain up to 20 ASCII characters.
5. Click **Apply** to update the switch with the new password.

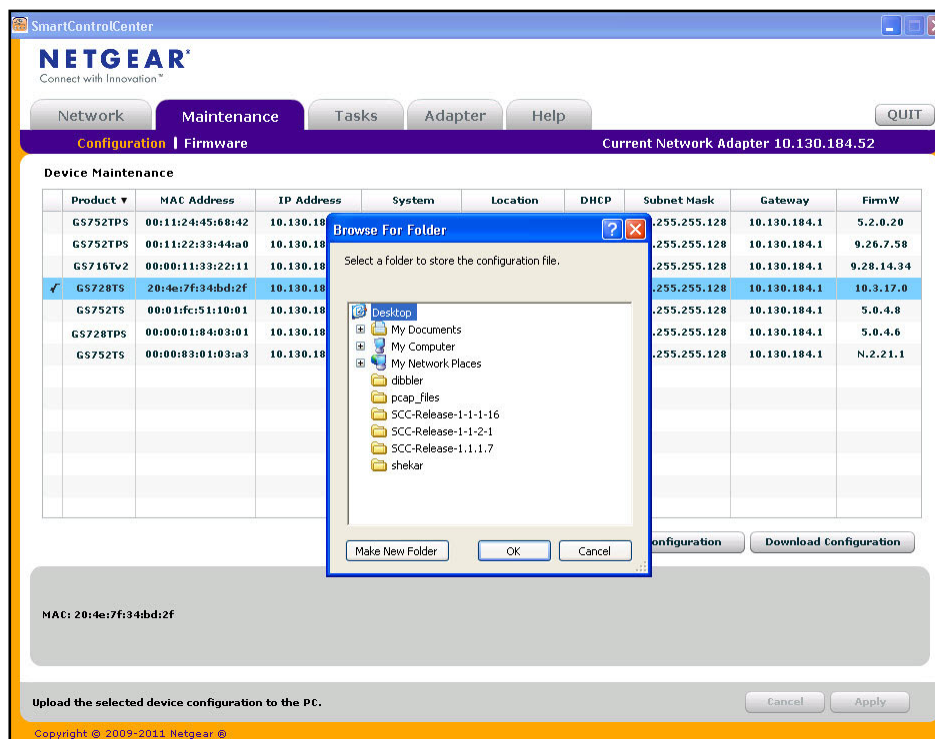
Configuration Upload and Download

When you make changes to the switch, the configuration information is stored in a file on the switch. You can backup the configuration by uploading the configuration file from the switch to an administrative system. You can download a saved configuration file from the administrative system to the switch. The configuration file you download to the switch overwrites the running configuration on the switch.

Configuration upload and download is useful if you want to save a copy of the current switch configuration (Upload Configuration) before you make changes. If you do not like the changes, you can use the Download Configuration option to restore the switch to the settings in the saved configuration file.

To save a copy of the current switch configuration on your administrative system:

1. Click the **Maintenance** tab and select the device with the configuration to save.
2. Click **Upload Configuration**.
3. From the **Browse for Folder** window that appears, navigate to and select the folder where you want to store the configuration file.



4. Click **OK**.
5. Enter the switch password and click **Apply**.

The file is uploaded to the administrative computer as a *.cfg file. You can open it and view the contents with a text editor.

To restore the configuration to a previously saved version:

1. Click the **Maintenance** tab and select the device with the configuration to restore.
2. Click **Download Configuration**.
3. From the **Select a Configuration** window that appears, navigate to and select the configuration file to download to the switch.
4. Click **Open**.
5. Enter the switch password and click **Apply** to begin the download process.

Optionally, you can schedule a different date and time to download the configuration file. To delay the download process, clear the **Run Now?** check box and enter a date and time to complete the download.

Note: Click the **Tasks** tab to view status information about the configuration download.

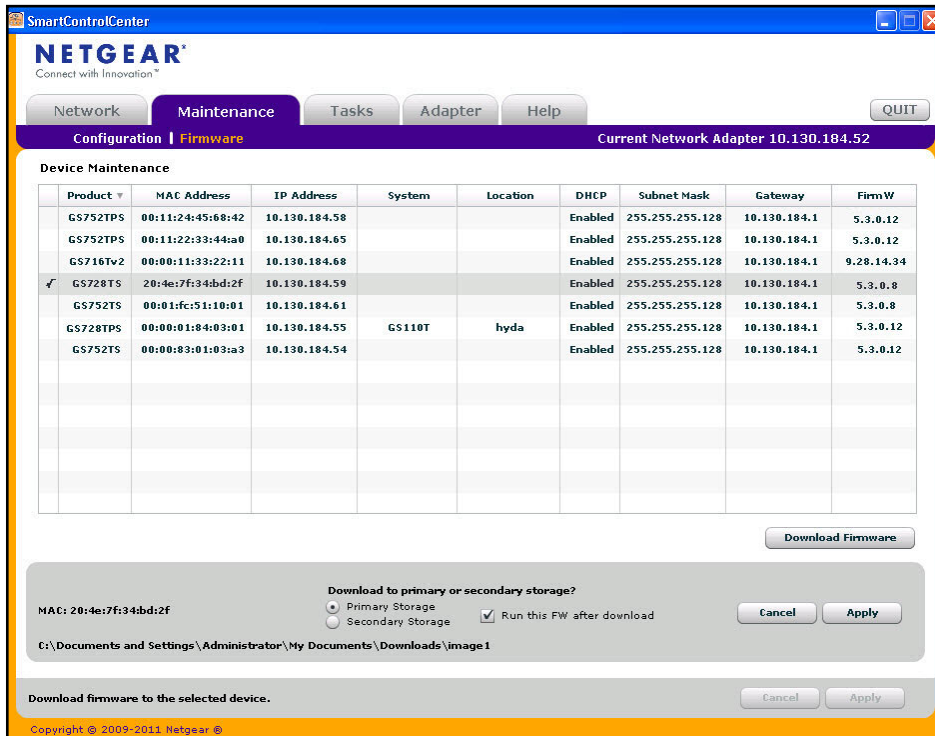
Firmware Upgrade

The application software for the GS728TS, GS728TPS, GS752TS, and GS752TPS Smart Switches 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 in this section. 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](#) on page 284.

To upgrade your firmware:

1. Click the **Maintenance** tab, and then click the **Firmware** link directly below the tabs (see [Figure 1](#) on page 12).
2. Select the switch to upgrade and click **Download Firmware**.
3. From the **Select new firmware** window that appears, navigate to and select the firmware image to download to the switch.
4. Click **Open**.



By default, the firmware is downloaded to primary storage and will become the active image after the download completes and the switch reboots. To download firmware to use as a backup image, select the **Secondary Storage** option. To prevent the switch from using the downloaded firmware as the active image, make sure the **Run this FW after download** option is clear.

Note: NETGEAR recommends that you download the same image as the primary and secondary image for redundancy.

5. Click **Apply**.
6. Enter the switch password to continue downloading the firmware.
Optionally, you can schedule a different date and time to download and install the firmware image. To delay the upgrade process, clear the **Run Now?** check box and enter a date and time to complete the upgrade.
7. Click **Apply** to download the firmware and upgrade the switch with the new image.
8. When the process is complete, the switch automatically reboots.

Note: Click the **Tasks** tab to view status information about the firmware upgrade.

**WARNING:**

It is important that you do not power-off the administrative system or the switch while the firmware upgrade is in progress.

Viewing and Managing Tasks

From the **Tasks** tab, you can view information about configuration downloads and firmware upgrades that have already occurred, are in progress, or are scheduled to take place at a later time. You can also delete or reschedule selected tasks. The following figure shows the **Tasks** page.

SmartControlCenter
NETGEAR
Connect with Innovation™

Network Maintenance **Tasks** Adapter Help QUIT

Current Network Adapter 10.130.184.52

Task Management From 09/26/2011 To 10/24/2011

MAC Address	System	Date	Time	Task Name	Task Status
20:4e:7f:34:bd:2f		10/04/2011	0:45 am	upload configuration	Task execution timeout.
00:11:24:45:68:42		10/04/2011	0:50 am	upload configuration	Successfully completed.

Delete Prior Tasks Delete One Task Reschedule

Select Range Cancel Apply

Copyright © 2009-2011 Netgear ©

The following list describes the command buttons that are specific to the **Tasks** page:

- **Delete Task**—Remove a completed or schedule task from the list.
- **Reschedule**—Change the scheduled date and time for a pending firmware upgrade or configuration download.
- **Select Range**—Select all tasks that occurred or are scheduled to occur within a certain period of time.

Understanding the User Interfaces

The GS728TS, GS728TPS, GS752TS, and GS752TPS switches 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 GS728TS, GS728TPS, GS752TS, and GS752TPS switches software. The method you use to manage the system depends on your network size and requirements, and on your preference.

The *GS728TS, GS728TPS, GS752TS, and GS752TPS 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
- Java Runtime Environment 1.6 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, as shown in *Figure 2* on page 17, and then click **Login**. Passwords are case sensitive.
3. After the system authenticates you, the System Information page displays.

Figure 3 on page 24 shows the layout of the Smart Switch Web interface.

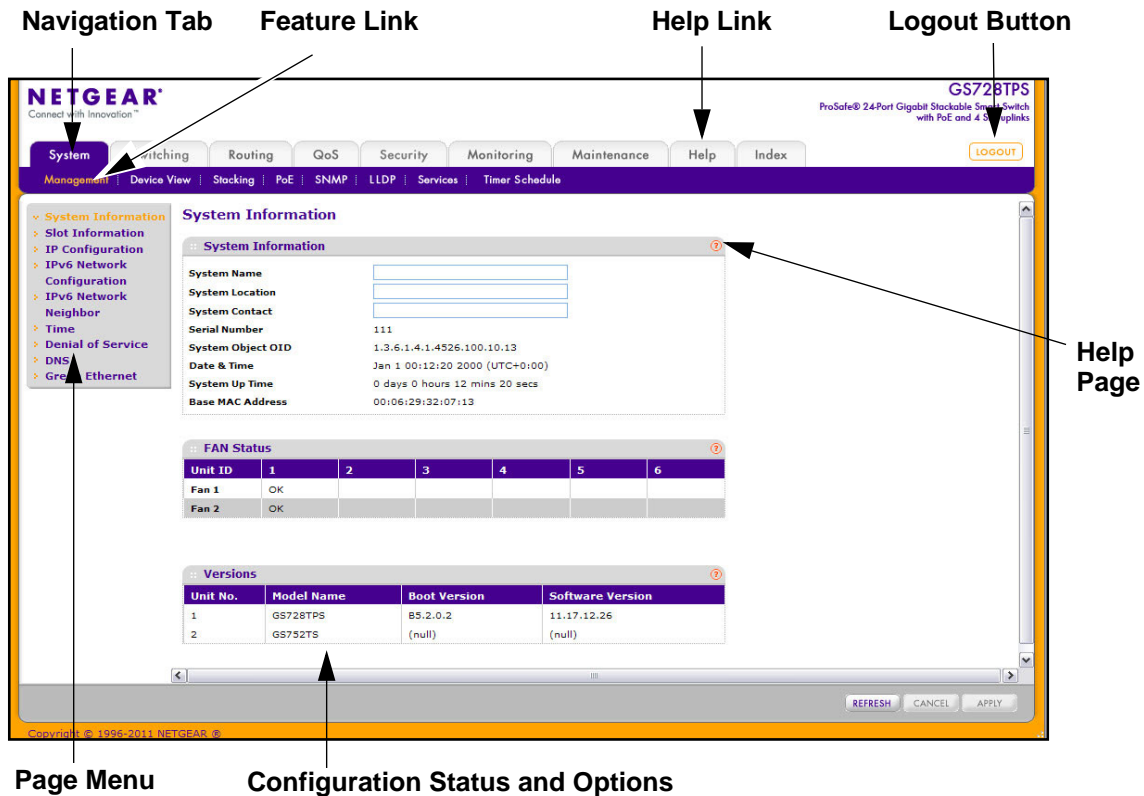


Figure 3. Administrative Page Layout

Navigation Tabs, Feature Links, and Page Menu

The navigation tabs along the top of the Web interface give you quick access to the various switch functions. The tabs are always available and remain constant, regardless of which feature you configure.

When you select a tab, the features for that tab appear as links directly under the tabs. The feature links in the blue bar change according to the navigation tab that is selected.

The configuration pages for each feature are available as links in the page menu on the left side of the page. Some items in the menu expand to reveal multiple configuration pages, as [Figure 4](#) on page 25. shows. When you click a menu item that includes multiple configuration pages, the item becomes preceded by a down arrow symbol and expands to display the additional pages.

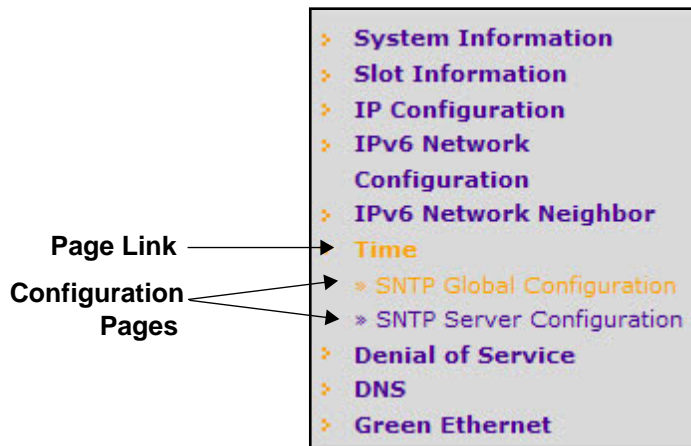


Figure 4. Menu Hierarchy

Configuration and Monitoring Options

The area directly under the feature links and to the right of the page 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 drop-down menus.

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

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

Table 1. Common Command Buttons

Button	Function
Add	Clicking Add adds the new item configured in the heading row of a table.
Apply	Clicking the Apply button sends the updated configuration to the switch. Configuration changes take effect immediately.
Cancel	Clicking Cancel cancels the configuration on the screen and resets the data on the screen to the latest value of the switch.
Delete	Clicking Delete removes the selected item.
Refresh	Clicking the Refresh button refreshes the page with the latest information from the device.
Logout	Clicking the Logout button ends the session.

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.

Depending upon the status of the port, the LED of the port status illuminates in Device View either red, green, or gray. Green indicates that the port is enabled. Red indicates that an error has occurred on the port, or red indicates that the link is disabled. Gray is applicable for ports 27 and 28 on the GS728TS/GS728TPS and ports 51 and 52 on the GS752TS/GS752TPS and indicates that the port is working in stack mode. The LED of the port speed illuminates either green or yellow.

- A green LED indicates operational ports at 1 Gbps or 2.5 Gbps (if used for stacking) link speed.
- A yellow LED indicates operational ports at 10/100 Mbps link speed.

The System LEDs are located on the left side of the front panel.

Power/Status LED

The power LED is a bicolor LED that serves as an indicator of power and diagnostic status. The following indications are given by the following LED states:

- A solid Green LED indicates that the power is supplied to the switch and operating normally.
- A solid Yellow LED indicates that system is in the boot-up stage.
- No lit LED indicates that power is disconnected.

FAN Status LED

FAN status is indicated as follows:

- A solid yellow LED indicates that the fan is faulty.
- No lit LED indicates that the fan is operating normally.

Stack Master LED

The Stack Master LED is lit if there is an active stack link and the unit is in stack mode.

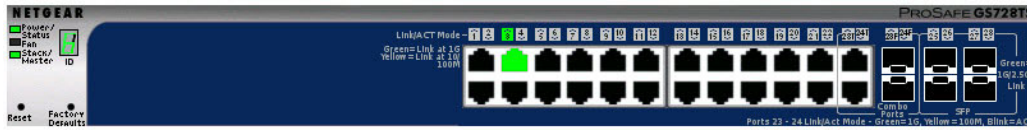
- A solid Green LED indicates that the switch acts as a master unit in a stack of switches.
- No lit LED indicates that the switch acts as a slave member in a stack of switches.

Seven-Segment LED for the Stacking ID

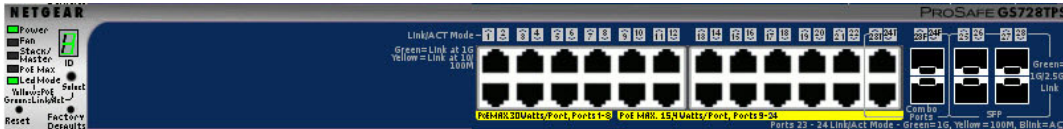
A solid Green LED displays the stack ID (1–6).

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

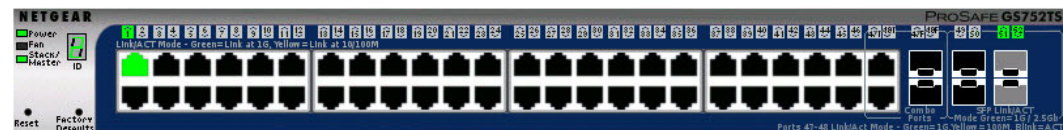
The following figure shows the Device View of the GS728TS.



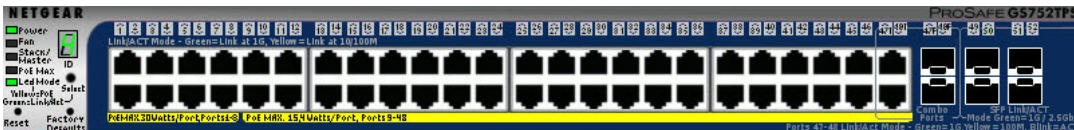
The following figure shows the Device View of the GS728TPS.



The following figure shows the Device View of the GS752TS.

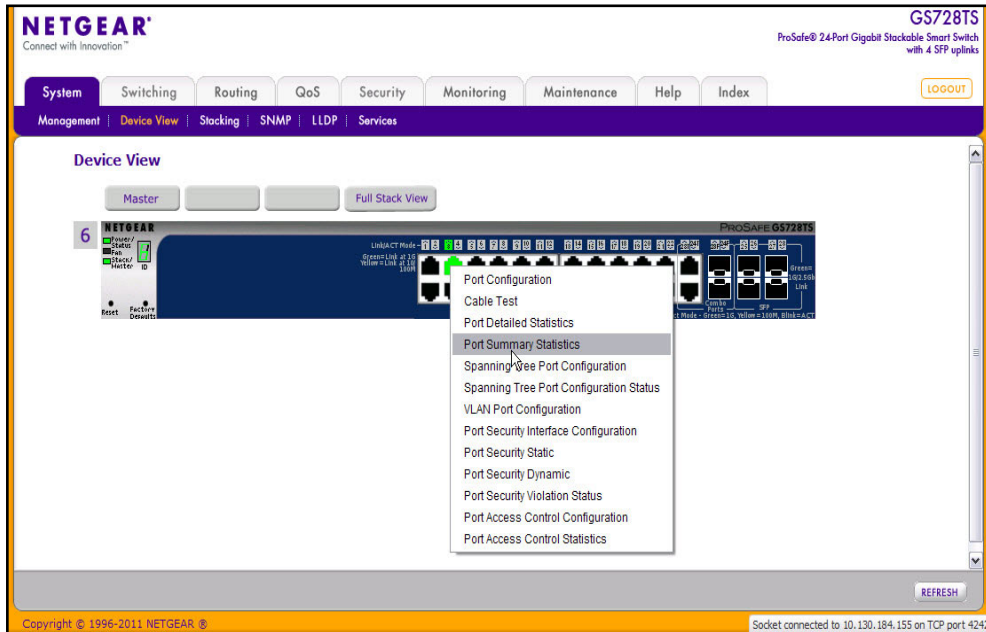


The following figure shows the Device View of the GS752TPS.

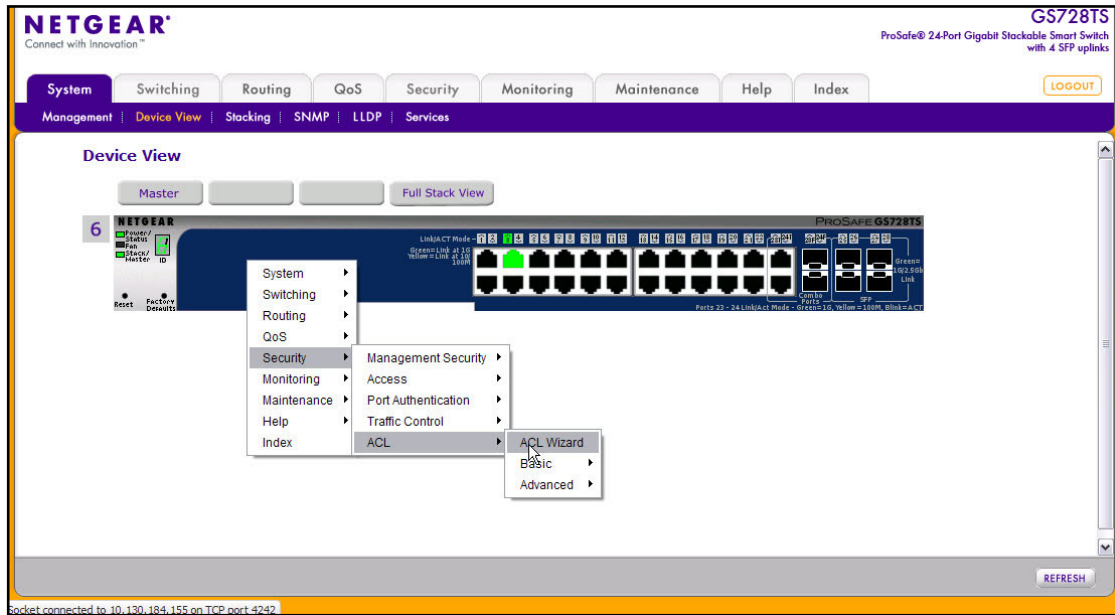


Click the port you want to view or configure to see a menu that displays statistics and configuration options. Click the menu option to access the page that contains the configuration or monitoring options.


GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches



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



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 3* on page 24 shows the location of the link to the Help Page on the Web interface.

User-Defined Fields

User-defined fields can contain 1 to 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

The GS728TS, GS728TPS, GS752TS, and GS752TPS switches software supports the configuration of SNMP groups and users that can manage traps that the SNMP agent generates. GS728TS, GS728TPS, GS752TS, and GS752TPS switches use 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, displays 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 authentication and encryption settings for the SNMPv3 admin profile by using the Web interface:

1. Navigate to the **System > SNMP > SNMPv3 > User Configuration** page.
2. To enable authentication, select an **Authentication Protocol** option, which is either **MD5** or **SHA**.
3. To enable encryption, select the **DES** option in the **Encryption Protocol** field. Then, enter an encryption code of eight or more alphanumeric characters in the **Encryption Key** field.
4. 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.

Interface Naming Convention

The GS728TS, GS728TPS, GS752TS, and GS752TPS switches software 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 can configure the logical interfaces by using the software. The following table describes the naming convention for all interfaces available on the switch.

Table 2. Interface Naming Conventions

Interface	Description	Example
Physical	The physical ports are gigabit Ethernet interfaces and are numbered sequentially starting from one. The number before the slash indicates the unit number of the stack member.	1/g1, 1/g2, 1/g3 3/g21, 3/g22
Link Aggregation Group (LAG)	LAG interfaces are logical interfaces that are only used for bridging functions.	l1, l2, l3
CPU Management Interface	This is the internal switch interface responsible for the switch base MAC address. This interface is not configurable and is always listed in the MAC Address Table.	c1

Configuring System Information

2

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:

- [Management](#) on page 31
- [Stacking](#) on page 61
- [PoE/PoE+ \(GS728TPS and GS752TPS Only\)](#) on page 70
- [SNMP](#) on page 75
- [LLDP](#) on page 80
- [Services — DHCP Snooping](#) on page 92
- [Timer Schedule \(GS728TPS and GS752TPS Only\)](#) on page 99

Management

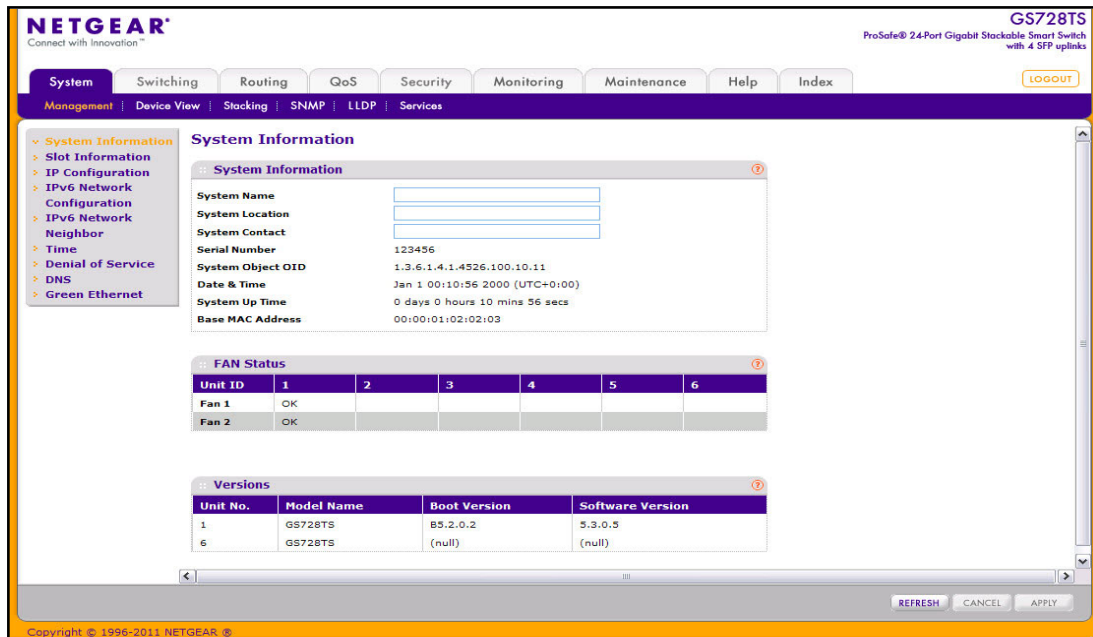
This section describes how to display the switch status and specify some basic switch information, such as the management interface IP address, system clock settings, and DNS information. From the Management link, you can access the following pages:

- [System Information](#) on page 32
- [Slot Information](#) on page 33
- [IP Configuration](#) on page 35
- [IPv6 Network Configuration](#) on page 37
- [IPv6 Network Neighbor](#) on page 38
- [Time](#) on page 40
- [Denial of Service](#) on page 45
- [DNS](#) on page 49
- [Green Ethernet](#) on page 51

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, click **System > Management > System Information**. A screen similar to the following is displayed.



To define system information:

1. Open the **System Information** page.
2. Define the following fields:
 - **System Name.** Enter the name you want to use to identify this switch. You may use up to 255 alphanumeric characters. The factory default is blank.
 - **System Location.** Enter the location of this switch. You may use up to 255 alphanumeric characters. The factory default is blank.
 - **System Contact.** Enter the contact person for this switch. You may use up to 255 alphanumeric characters. The factory default is blank.
3. Click **Apply**.

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

The following table describes the status information the System Page displays.

Field	Description
Serial Number	The serial number of the switch.
System Object OID	The base object ID for the switch's enterprise MIB.

Field	Description
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.
Fan Status Table	
Unit ID	Identifies the unit number assigned to the stack member. Up to six units are supported in a stack, and the table contains separate columns for each possible unit in the stack, whether the units are present or not.
Fan 1 and Fan 2	These fans remove the heat generated by the power, CPU and other chipsets, and allow the chipsets to work normally. Fan status has three possible values: OK, Failure, Not Present. If the Fan 1 and Fan 2 entries for a Unit ID are blank, then no switch with that unit number is present in the stack.
Versions Table	
Unit No.	Identifies the unit number assigned to the stack member.
Model Name	The model name of the switch.
Boot Version	The boot code version of the switch.
Software Version	The software version of the switch.

Slot Information

Use this page to display details of the different slots in the different units in the stack. The page also displays information about the card types and switch models supported in the stack.

To display the Slot Information page, click **System > Management > Slot Information**. A screen similar to the following is displayed.

The screenshot shows the Netgear management interface for a GS728TS switch. The 'Slot Information' page is active, displaying the following data:

Slot Summary									
Slot	Administrative Status	Power State	Configured Card Model ID	Configured Card Description	Inserted Card Model ID	Inserted Card Description	Card Power Down	Card Pluggable	
1/0	Full	Enable	BCM56321-24GE 4 1G	Broadcom BCM56321 - 24 GE Port 4 1G Dedicated Ethernet Line Card	BCM56321-24GE 4 1G	Broadcom BCM56321 - 24 GE Port 4 1G Dedicated Ethernet Line Card	False	False	
6/0	Empty	Enable	BCM56321-24GE 4 1G	Broadcom BCM56321 - 24 GE Port 4 1G Dedicated Ethernet Line Card			False	False	

Supported Card			
Card Model	Card Index	Card Type	Card Descriptor
BCM56321-48GE 4 10G	2	0x86320000	Broadcom BCM56321 - 48 GE Port 4 10G Dedicated Ethernet Line Card
BCM56321-48GE 4 10G	3	0x86320000	Broadcom BCM56321 - 48 GE Port 4 10G Dedicated Ethernet Line Card
BCM56321-24GE 4 1G	4	0x76320000	Broadcom BCM56321 - 24 GE Port 4 1G Dedicated Ethernet Line Card
BCM56321-24GE 4 1G	5	0x86320000	Broadcom BCM56321 - 24 GE Port 4 1G Dedicated Ethernet Line Card

Supported Switch			
Switch Model ID	Switch Index	Management Preference	Code Type
GS752TS	1	1	0x100b000
GS752TPS	2	1	0x100b000
GS728TS	3	1	0x100b000
GS728TPS	4	1	0x100b000

Click **Refresh** to refresh the screen with most recent data.

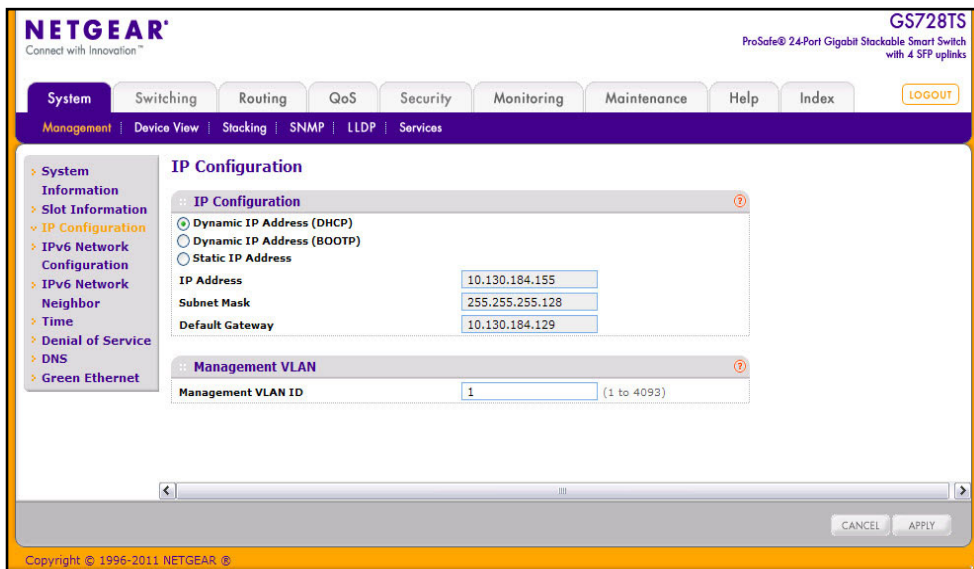
The following table describes the status information the Slot Information displays.

Field	Description
Slot Summary	
Slot	Identifies the slot using the format unit/slot.
Status	Displays whether the slot is empty or full.
Administrative State	Displays whether the slot is administratively enabled or disabled.
Power State	Displays whether the slot is powered on or not.
Configured Card Model ID	Displays the model ID of the card configured for the slot.
Configured Card Description	Displays the description of the card configured for the slot.
Inserted Card Model ID	Displays the model ID of the card physically present in the slot.
Inserted Card Description	Displays the description of the card physically present in the slot.
Card Power Down	Displays whether the card in the slot is powered down.
Card Pluggable	Displays whether the inserted card is pluggable or not.
Supported Card	
Card Model	Lists summary information about the card models supported for the stackable units.
Card Index	Displays the index assigned to the selected card type.
Card Type	Displays the hardware type of this supported card. This is a 32-bit data field.
Card Descriptor	Displays the additional information about each supported card.
Supported Switch	
Switch Model ID	Displays the list of models of all supported switches.
Switch Index	Displays the index assigned to the selected switch.
Management Preference	Identifies whether the unit prefers to be a stack master or stack member.
Code Type	Displays the Code Target ID on the supported switch

IP Configuration

Use the IP Configuration page to configure network information for the management interface, which is the logical interface used for in-band connectivity with the switch through 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.

To access the page, click **System > Management > IP Configuration**. A screen similar to the following is displayed.



To configure the network information for the management interface:

1. Select the appropriate radio button to determine how to configure the network information for the switch management interface:
 - **Dynamic IP Address (DHCP)**. Specifies that the switch must obtain the IP address through a DHCP server.
 - **Dynamic IP Address (BOOTP)**. Specifies that the switch must obtain the IP address through a BootP server.
 - **Static IP Address**. Specifies that the IP address, subnet mask, and default gateway must be manually configured. Enter this information in the fields below this radio button.
2. If you selected the Static IP Address option, configure the following network information:
 - **IP Address**. The IP address of the network interface. The factory default value is 192.168.0.239. 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.
 - **Default Gateway**. The default gateway for the IP interface. The factory default value is 192.168.0.254.

3. Specify the VLAN ID for the management VLAN.

The management VLAN is used to establish an IP connection to the switch from a workstation that is connected to a port in the same VLAN. If not specified, the active management VLAN ID is 1 (default), which allows an IP connection to be established through any port.

When the management VLAN is set to a different value, an IP connection can be made only through a port that is part of the management VLAN. It is also mandatory that the port VLAN ID (PVID) of the port to be connected in that management VLAN be the same as the management VLAN ID.

The management VLAN has the following requirements:

- Only one management VLAN can be active at a time.
- When a new management VLAN is configured, connectivity through the existing management VLAN is lost.
- The management station should be reconnected to the port in the new management VLAN.

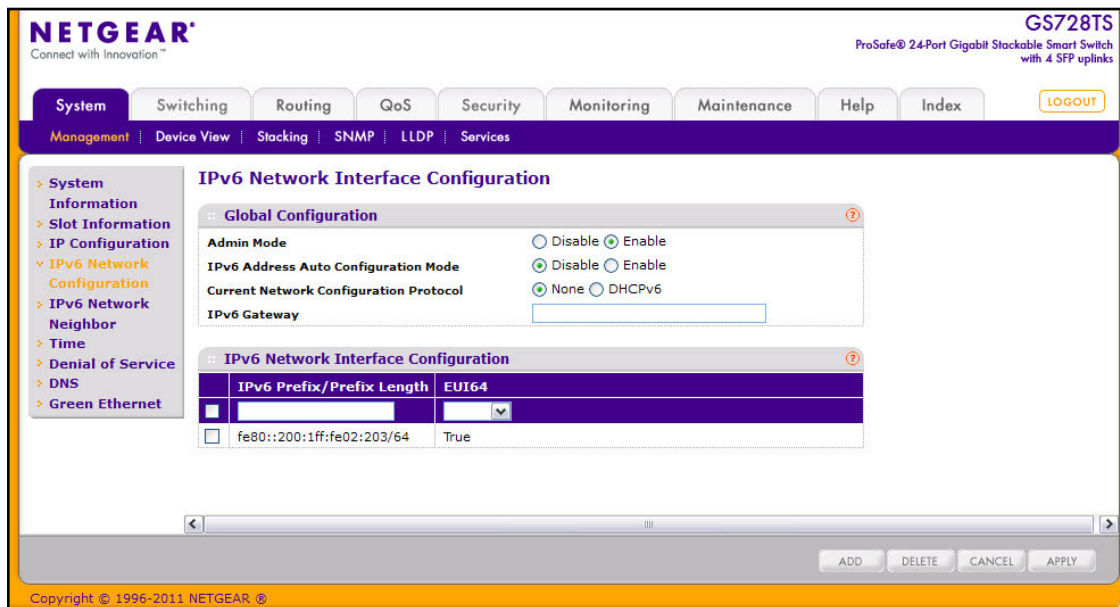
Note: Make sure that the VLAN to be configured as the management VLAN exists. And make sure that the PVID of at least one port that is a port of the VLAN is the same as the management VLAN ID. For information about creating VLANs and configuring the PVID for a port, see [VLANs](#) on page 110.

4. If you change any of the network connection parameters, click **Apply** to apply the changes to the system.
5. Click **Cancel** to abandon the changes.

IPv6 Network Configuration

Use the IPv6 Network Configuration page to configure the IPv6 network interface, which is the logical interface used for in-band connectivity with the switch via all 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.

To access the page, click **System > Management > IPv6 Network Configuration**. A screen similar to the following is displayed.



To access the switch over a IPv6 network, you must initially configure the switch with IPv6 information (IPv6 prefix, prefix length, and default gateway). IPv6 can be configured using any of the following options:

- IPv6 Auto Configuration
- DHCPv6

When in-band connectivity is established, IPv6 information can be changed using any of the following:

- SNMP-based management
- Web-based management

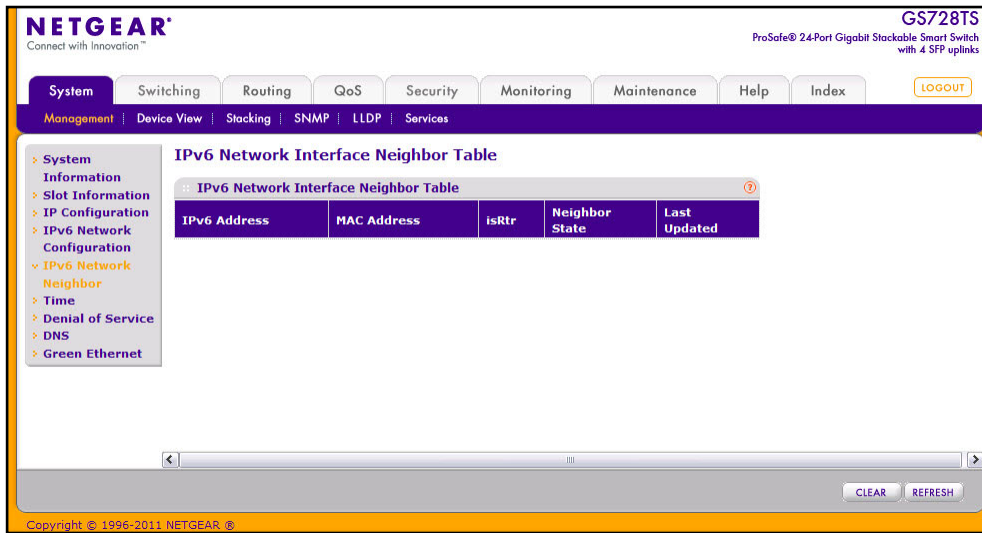
To configure the network information for an IPv6 network:

1. **Admin Mode.** Enable or disable the IPv6 network interface on the switch. The default value is Enable.
2. **IPv6 Address Auto Configuration Mode.** The IPv6 address for the IPv6 network interface is set in auto configuration mode if this option is enabled. The default value is Disable. Auto configuration can be enabled only when DHCPv6 is not enabled on any of the management interfaces.
3. **Current Network Configuration Protocol.** The IPv6 address for the IPv6 network interface is configured by DHCPv6 protocol if this option is enabled. The default value is None. DHCPv6 can be enabled only when IPv6 Auto configuration or DHCPv6 are not enabled on any of the management interfaces.
4. **DHCPv6 Client DUID.** Identifier used to identify the client's unique DUID value. This option only displays when DHCPv6 is enabled.
5. **IPv6 Gateway.** Specify the gateway for the IPv6 network interface. The gateway address is in IPv6 global or link-local address format.
6. **IPv6 Prefix/Prefix Length.** Add the IPv6 prefix and prefix length to the IPv6 network interface. The address is in the global address format.
7. **EUI64.** Specify whether format IPv6 address in EUI-64 format. The default value is False.
8. Click **Add** to add a new IPv6 address in global format.
9. Click **Delete** to delete a selected IPv6 address.
10. Click **Apply** to apply the changes to the system.
11. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IPv6 Network Neighbor

Use the IPv6 Network Neighbor page to view the IPv6 Network Interface IPv6 Neighbor Table. If no IPv6 neighbors are detected on the network, the table is empty.

To access the page, click **System > Management > IPv6 Network Neighbor**. A screen similar to the following is displayed.



Click **Clear** to delete all entries from the table. The table is repopulated as the IPv6 neighbors are discovered on the network. Click **Refresh** to refresh the screen with most recent data.

The following table describes the information the IPv6 Network Interface Neighbor Table displays

Field	Description
IPv6 Address	Specifies the IPv6 address of neighbor or interface.
MAC Address	Specifies MAC address associated with an interface.
IsRtr	Indicates whether the neighbor is a router. If the neighbor is a router, the value is True. If the neighbor is not a router, the value is False.
Neighbor State	Specifies the state of the neighbor cache entry. The following are the states for dynamic entries in the IPv6 neighbor discovery cache: <ul style="list-style-type: none"> • Reachable. Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • Stale. More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • Delay. More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. • Probe. A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. • Unknown. The switch cannot determine the state of the cache entry.
Last Updated.	Time since the address was confirmed to be reachable.

Time

The GS728TS, GS728TPS, GS752TS, and GS752TPS switch software supports the Simple Network Time Protocol (SNTP). You can also set the system time manually.

SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The GS728TS, GS728TPS, GS752TS, and GS752TPS switches operate only as SNTP clients and cannot provide time services to other systems.

Time sources are established by Stratum. Stratum defines 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 stratum:

- **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 server types for the server time.

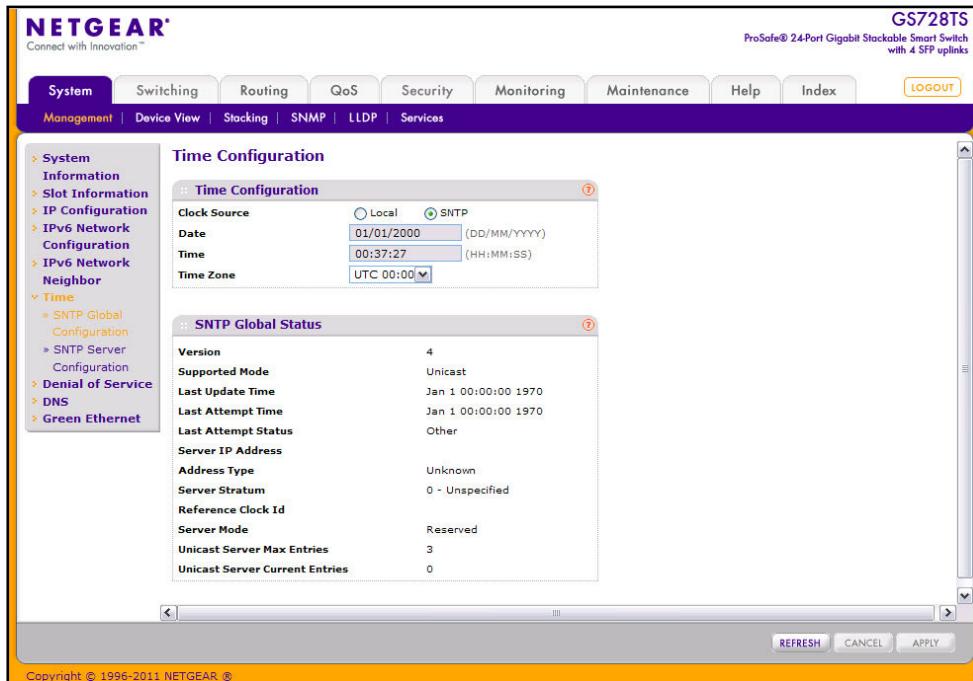
Polling for Unicast information is used for polling a server for which the IP address is known. SNTP servers that have been configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing 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.

The device retrieves synchronization information, either by actively requesting information or at every poll interval.

Time Configuration

Use the Time Configuration page to view and adjust date and time settings.

To display the Time Configuration page, click **System > Management > Time > SNTP Global Configuration**.



To configure the time by using the CPU clock cycle as the source:

1. From the Clock Source field, select **Local**.
2. In the **Date** field, enter the date in the DD/MM/YYYY format.
3. In the **Time** field, enter the time in HH:MM:SS format.

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

When the Clock Source is set to **Local**, the **Time Zone** field is grayed out (disabled).

4. Click **Apply** to send the updated configuration to the switch. Configuration changes occur immediately.

To configure the time through SNTP:

1. From the Clock Source field, select **SNTP**.
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.
2. Use the menu to select the Coordinated Universal Time (UTC) time zone in which the switch is located, expressed as the number of hours. The options in the Time Zone menu specify the time difference from UTC time zone.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
4. Use the **SNTP Server Configuration** page to configure the SNTP server settings, as described in *SNTP Server Configuration* on page 43.
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.

The SNTP Global Status table on the **Time Configuration** page displays information about the system's SNTP client. The following table describes the SNTP Global Status 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.
Last Attempt Status	Specifies the status of the last SNTP request or unsolicited message for both unicast mode. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes: <ul style="list-style-type: none"> • 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.

Field	Description
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 Server 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.

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

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, click **System > Management > Time > SNTP Server Configuration**.

The screenshot shows the Netgear web interface for a GS728TS switch. The main content area is titled "SNTP Server Configuration". It features a table for configuring SNTP servers and a table for monitoring their status.

SNTP Server Configuration					
Server Type	Address	Port (1 to 65535)	Priority (1 to 3)	Version (1 to 4)	
IPv4		123	1	4	

SNTP Server Status					
Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests

At the bottom of the configuration table, there are buttons for REFRESH, ADD, DELETE, CANCEL, and APPLY.

To configure a new SNTP Server:

1. Enter the appropriate SNTP server information in the available fields:
 - **Server Type.** Specifies whether the address for the SNTP server is an IP address (IPv4) or hostname (DNS).
 - **Address.** Enter the IP address or the hostname of the SNTP server.
 - **Port.** Enter a port number on the SNTP server to which SNTP requests are sent. The valid range is 1–65535. 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 1–3, with 1 being the default and the highest priority. Servers with lowest numbers have priority.
 - **Version.** Enter the protocol version number that corresponds to the NTP version running on the SNTP server. The range is 1–4, and the default version is SNTPv4.
2. Click **Add**.
3. Repeat the previous steps to add additional SNTP servers. You can configure up to three SNTP servers.
4. To removing an SNTP server, select the check box next to the configured server to remove, and then click **Delete**. The entry is removed, and the device is updated.
5. To change the settings for an existing SNTP server, select the check box next to the configured server and enter new values in the available fields, and then click **Apply**. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The SNTP Server Status table displays status information about the SNTP servers configured on your switch. The following table describes the SNTP Global 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.

Field	Description
Last Attempt Status	<p>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:</p> <ul style="list-style-type: none"> • 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.

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

Denial of Service

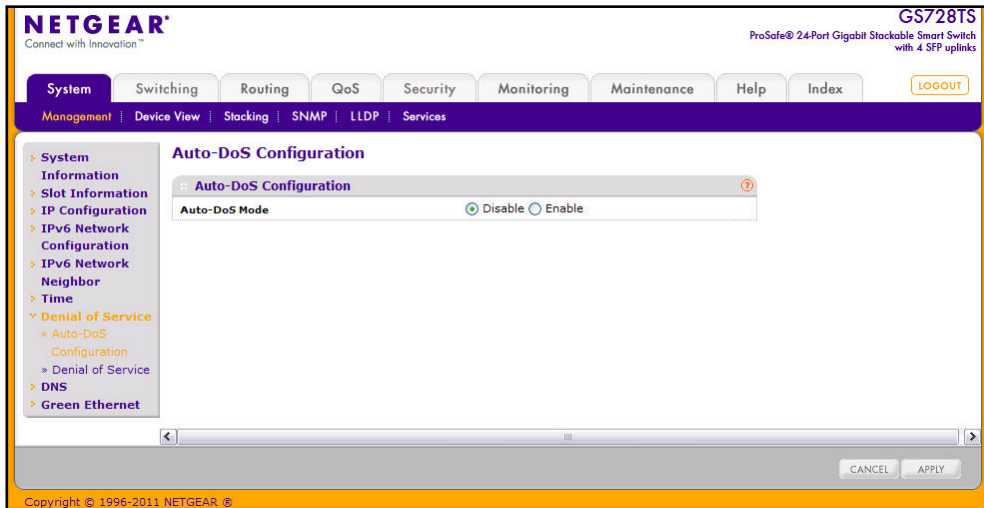
Use the Denial of Service (DoS) page to configure DoS control. The GS728TS, GS728TPS, GS752TS, and GS752TPS switches provide support for classifying and blocking specific types of DoS attacks. The type of DoS attacks the switch can detect and prevent are described on page 47.

Auto-DoS Configuration

The Auto-DoS Configuration page lets you automatically enable all the DoS features available on the switch, except for TCP and UDP port attacks. See [DoS Configuration](#) on page 47 for information about the types of DoS attacks the switch can monitor and block.

Note: When Auto-DoS is enabled, a port that is under attack is automatically shut down and does not forward traffic. The port can be enabled only manually by the admin user. A warning message is logged to the buffered log and is sent to the Syslog server.

To access the Auto-DoS Configuration page, click **System > Management > Denial of Service > Auto-DoS Configuration**.



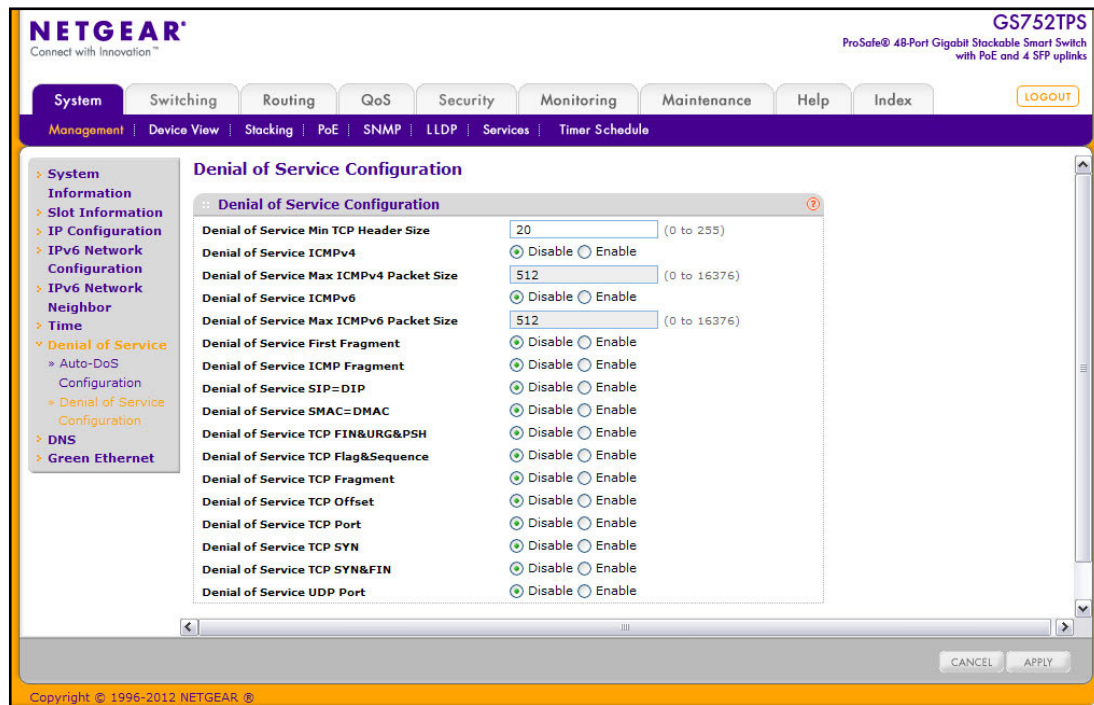
To configure the Auto-DoS feature:

1. Select a radio button to enable or disable Auto-DoS:
 - **Disable.** Auto-DoS is disabled (default).
 - **Enable.** Auto-DoS is enabled.
2. Click **Apply** to send the updated configuration to the switch. Configuration changes occur 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.

DoS Configuration

The **DoS Configuration** page lets you to select which types of DoS attacks for the switch to monitor and block.

To access the **DoS Configuration** page, click **System > Management > Denial of Service > Denial of Service Configuration**.



To configure individual DoS settings:

1. Select the types of DoS attacks for the switch to monitor and block and configure any associated values, as the following list describes.
 - **Denial of Service Min TCP Hdr Size.** Specify the minimum TCP header size allowed. If First Fragment DoS prevention is enabled, the switch will drop packets that have a TCP header smaller than this configured value. The factory default is 20 bytes.
 - **Denial of Service ICMPv4.** Enable or disable this option by selecting the appropriate radio button. Enabling ICMPv4 DoS prevention causes the switch to drop ICMPv4 packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 packet size. The factory default is Disable.
 - **Denial of Service Max ICMPv4 Size.** Specify the maximum allowed ICMPv4 packet size. If ICMPv4 DoS prevention is enabled, the switch will drop ICMPv4 ping packets that have a size greater than this configured maximum ICMPv4 packet size. The range is 0 to 16376, and the default value (when enabled) is 512.
 - **Denial of Service ICMPv6.** Enabling ICMPv6 DoS prevention causes the switch to drop ICMPv6 packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 maximum packet size. The factory default is disabled.

- **Denial of Service Max ICMPv6 Packet Size.** Specify the maximum allowed IPv6 ICMP packet size. If ICMPv6 DoS prevention is enabled, the switch will drop IPv6 ICMP ping packets that have a size greater than this configured maximum ICMPv6 packet size. The range is 0 to 16376, and the default value (when enabled) is 512.
- **Denial of Service First Fragment.** Enable or disable this option by selecting the appropriate radio button. 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 Disable.
- **Denial of Service ICMP Fragment.** Enable or disable this option by selecting the appropriate radio button. Enabling ICMP Fragment DoS prevention causes the switch to drop fragmented ICMP packets. The factory default is disabled.
- **Denial of Service SIP=DIP.** Enable or disable this option by selecting the appropriate radio button. 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 Disable.
- **Denial of Service SMAC=DMAC.** Enable or disable this option by selecting the appropriate radio button. Enabling SMAC=DMAC DoS prevention causes the switch to drop packets that have a source MAC address equal to the destination MAC address. The factory default is disabled.
- **Denial of Service TCP FIN&URG&PSH.** Enable or disable this option by selecting the appropriate radio button. Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets that have TCP Flags FIN, URG, and PSH set and a TCP Sequence Number equal to 0. The factory default is disabled.
- **Denial of Service TCP Flag &Sequence.** Enable or disable this option by selecting the appropriate radio button. Enabling TCP Flag DoS prevention causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0. The factory default is disabled.
- **Denial of Service TCP Fragment.** Enable or disable this option by selecting the appropriate radio button. Enabling TCP Fragment DoS prevention causes the switch to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size. The factory default is Disable.
- **Denial of Service TCP Offset.** Enable or disable this option by selecting the appropriate radio button. Enabling TCP Offset DoS prevention causes the switch to drop packets that have a TCP header Offset=1. The factory default is disabled.
- **Denial of Service TCP Port.** Enable or disable this option by selecting the appropriate radio button. Enabling TCP Port DoS prevention causes the switch to drop packets that have TCP source port equal to TCP destination port. The factory default is disabled.
- **Denial of Service TCP SYN.** Enable or disable this option by selecting the appropriate radio button. Enabling TCP SYN DoS prevention causes the switch to drop packets that have TCP Flags SYN set and L4 source = 0–1023. The factory default is disabled.

- **Denial of Service TCP SYN&FIN.** Enable or disable this option by selecting the appropriate radio button. Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets that have TCP Flags SYN and FIN set. The factory default is disabled.
 - **Denial of Service UDP Port.** Enable or disable this option by selecting the appropriate radio button. Enabling UDP Port DoS prevention causes the switch to drop packets that have UDP source port equal to UDP destination port. The factory default is disabled.
2. If you change any of the DoS settings, click **Apply** to apply the changes to 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.

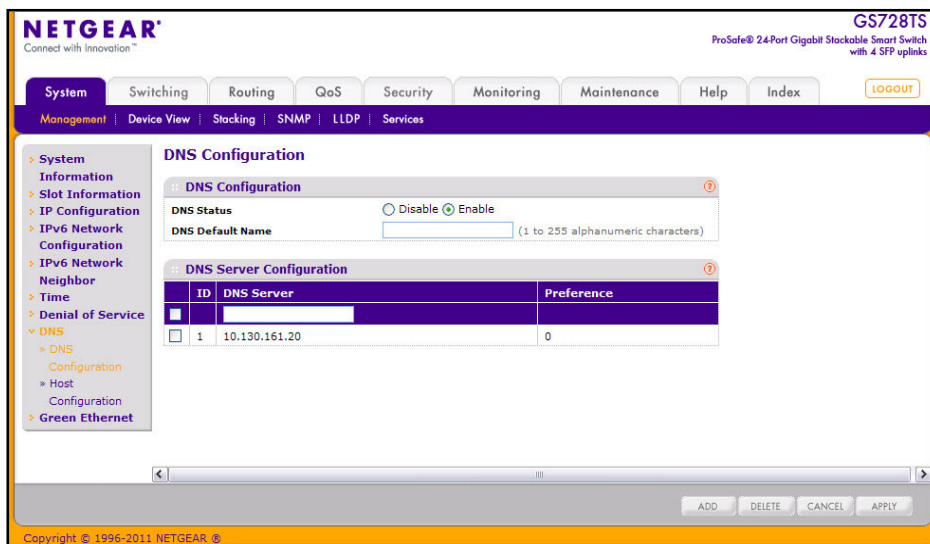
DNS

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

DNS Configuration

Use this page to configure global DNS settings and DNS server information.

To access this page, click **System > Management > DNS > DNS Configuration**.



To configure the global DNS settings

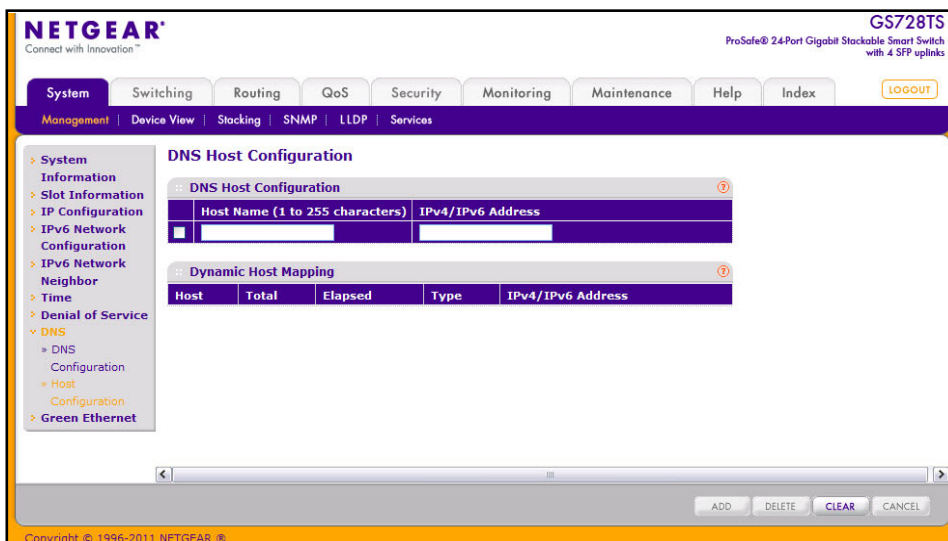
1. Specify whether to enable or disable the administrative status of the DNS Client.
 - **Enable.** Allow the switch to send DNS queries to a DNS server to resolve a DNS domain name. DNS is enabled by default.
 - **Disable.** Prevent the switch from sending DNS queries.

2. Enter the DNS default domain name to include in DNS queries. When the system is performing a lookup on an unqualified hostname, this field is provided as the domain name (for example, if default domain name is netgear.com and the user enters test, then test is changed to test.netgear.com to resolve the name). The name can contain 1–255 characters.
3. To specify the DNS server to which the switch sends DNS queries, enter an IP address in standard IPv4 dot notation in the **DNS Server Address** and click **Add**. The server appears in the list below. You can specify up to eight DNS servers. The preference is set in the order created.
4. To remove a DNS server from the list, select the check box next to the server 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.
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. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Host Configuration

Use this page to manually map host names to IP addresses or to view dynamic DNS mappings.

To access this page, click **System > Management > DNS > Host Configuration**.



To add a static entry to the local DNS table:

1. Specify the static host name to add. Each substring must be less than 64 characters in length separated by a dot, and the length of the whole string must not exceed 255 characters.
2. Specify the IPv4 or IPv6 address in standard notation to associate with the hostname.
3. Click **Add**. The entry appears in the list below.

4. To remove an entry from the static DNS table, select the check box next to the entry and click **Delete**.
5. To change the hostname or IP address in an entry, select the check box next to the entry and enter the new information in the appropriate field, and then click **Apply**.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The Dynamic Host Configuration table shows host name-to-IP address entries that the switch has learned. The following table describes the dynamic host fields:

Field	Description
Host	Lists the host name you assign to the specified IP address.
Total	Amount of time since the dynamic entry was first added to the table.
Elapsed	Amount of time since the dynamic entry was last updated.
Type	The type of the dynamic entry.
IPv4/IPv6 Addresses	Lists the IPv4 or IPv6 addresses associated with the host name.

Click **Clear** to delete Dynamic Host Entries. The table will be repopulated with entries as they are learned.

Green Ethernet

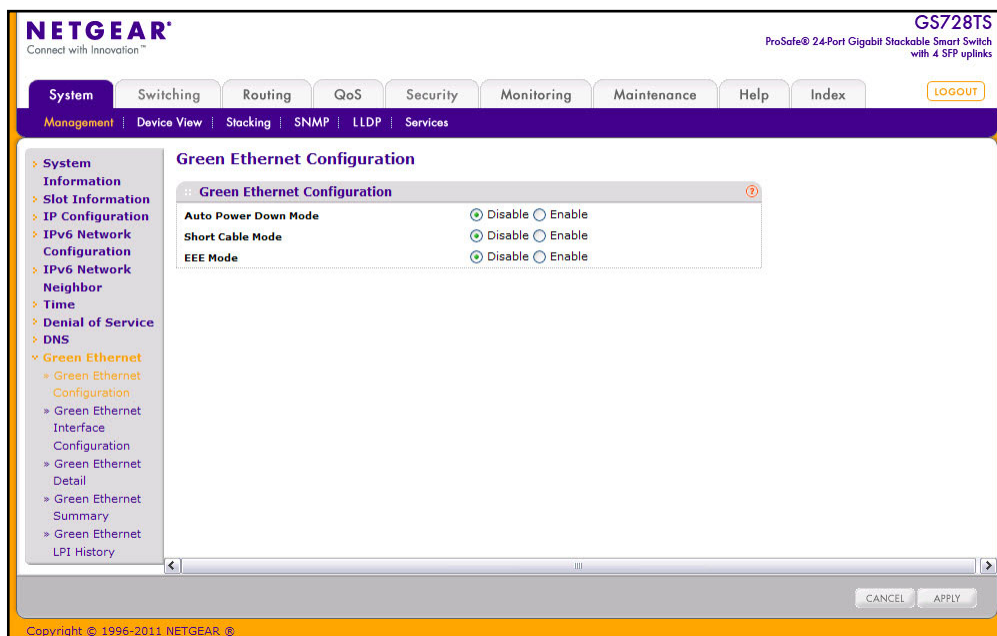
The Green Ethernet features allow the switch to reduce power consumption on a per-port basis. Each switch can support one or more of the following features:

- Energy-detect Mode - When the Energy Detect mode is enabled and the port link is down, the PHY automatically goes down for short period of time and then wakes up to check link pulses. This mode reduces power consumption on the port when no link partner is present.
- Short Cable Mode: With Short Cable mode enabled, the PHY goes into low power mode when the cable length is less than a certain limit.
- Energy Efficient Ethernet (EEE): EEE enables ports to enter a low-power mode to reduce power consumption during periods of low link utilization. EEE is defined by IEEE 802.3az. EEE enables both the send and receive sides of the link to disable some functionality for power savings when the link is lightly loaded.

Green Ethernet Configuration

Use this page to configure the administrative mode for the Green Ethernet features available on the switch. These features must also be enabled on each port to take advantage of the possible power savings.

To access this page, click **System > Management > Green Ethernet Configuration**.



To configure the Green Ethernet feature:

1. Enable or disable the **Auto Power-Down Mode**.
 - **Enable**. When the port link is down, the PHY automatically goes down for a short period of time and then wakes up to check link pulses. This behavior saves power consumption when there is no link partner while still allowing the port to perform auto-negotiation if a link partner does become present.
 - **Disable**. The PHY remains up even if no link partner is present.
2. Enable or disable the **Short Cable Mode**.
 - **Enable**. The switch performs a cable test on each cable connect to its ports. If the cable is less than 10m in length, the port is placed in low power mode (nominal power).
 - **Disable**. Full transmit power is provided to all ports, regardless of cable length.
3. Enable or disable the **EEE Mode**:
 - **Enable**. The switch allows ports to transition to low-power mode during link idle conditions.
 - **Disable**. Full transmit power is provided to all ports, regardless of port activity.
4. Click **Apply** to send the updated configuration to the switch, or click **Cancel** to abandon the changes. Applied configuration changes take effect immediately.

Green Ethernet Interface Configuration

Use this page to configure Green Ethernet features on a per-port basis. The Green Ethernet modes must be administratively enabled on the switch for the mode enabled on the port to take effect.

To access this page, click **System > Management > Green Ethernet > Green Ethernet Interface Configuration**.

The screenshot shows the NETGEAR web interface for a GS728TS switch. The main content area is titled "Green Ethernet Interface Configuration". It features a table with the following columns: "Port", "Auto Power Down Mode", "Short Cable Mode", and "EEE Mode". The table lists 11 ports (1/g1 to 1/g11). Each row has a checkbox in the "Port" column, and the "Auto Power Down Mode", "Short Cable Mode", and "EEE Mode" columns are currently set to "Disable". A "GO" button is located above the table to filter the results. The interface also includes a left-hand navigation menu and a top navigation bar with various system management options.

To configure the Green Ethernet Interface feature:

1. Select the check box next to the port to configure. You can select multiple ports to apply the same setting to all selected ports. To configure all ports, select the check box in the heading row.
2. Enable or disable the **Auto Power-Down Mode**.
 - **Enable.** When the port link is down, the PHY automatically goes down for a short period of time and then wake up to check link pulses. This behavior saves power consumption when there is no link partner while still allowing the port to perform auto-negotiation if a link partner does become present.
 - **Disable.** The PHY remains up even if no link partner is present.
3. Enable or disable the **Short Cable Mode**.
 - **Enable.** The switch performs a cable test on each cable connect to its ports. If the cable is less than 10m in length, the port is placed in low power mode (nominal power). Short cable mode and EEE mode cannot be enabled on the same port simultaneously.
 - **Disable.** Full transmit power is provided to all ports, regardless of cable length.

4. Enable or disable the **EEE Mode**:
 - **Enable**. The switch allows ports to transition to low-power mode during link idle conditions. Short cable mode and EEE mode cannot be enabled on the same port simultaneously.
 - **Disable**. Full transmit power is provided to all ports, regardless of port activity.
5. Click **Apply** to apply the change to the system. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Green Ethernet Detail

Use this page to configure Green Ethernet monitor and manage Green Ethernet features on a specific port.

To access this page, click **System > Management > Green Ethernet > Green Ethernet Detail**.

The screenshot shows the Netgear web interface for a GS728TS switch. The main navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar shows a tree view with 'Green Ethernet' expanded to 'Green Ethernet Interface Configuration'. The main content area is titled 'Port Green Mode Statistics' and contains two panels:

- Local Device Information:** Shows configuration for interface 1/g3. Key settings include:
 - Energy Detect Admin Mode: Disable
 - Operational Status: Inactive
 - Reason: Admin Down
 - Short Reach Admin Mode: Disable
 - Operational Status: Inactive
 - Reason: Admin Down
 - EEE Admin Mode: Disable
 - Rx Low Power Idle Event Count: 0
 - Rx Low Power Idle Duration (uSec): 0
 - Tx Low Power Idle Event Count: 0
 - Tx Low Power Idle Duration (uSec): 0
 - Tw_sys_tx (uSec): 17
 - Tw_sys_tx Echo (uSec): 17
 - Tw_sys_rx (uSec): 17
 - Tw_sys_rx Echo (uSec): 17
 - Fallback Tw_sys (uSec): 17
 - Tx_dll_enabled: No
 - Tx_dll_ready: No
 - Rx_dll_enabled: No
 - Rx_dll_ready: No
 - Time Since Counters Last Cleared: (empty)
- Remote Device Information:** Shows configuration for interface 1/g3. Key settings include:
 - Remote ID: 1
 - Remote Tw_sys_tx (uSec): (empty)
 - Remote Tw_sys_tx Echo (uSec): (empty)
 - Remote Tw_sys_rx (uSec): (empty)
 - Remote Tw_sys_rx Echo (uSec): (empty)
 - Remote Fallback Tw_sys (uSec): (empty)

At the bottom of the page, there are buttons for 'APPLY', 'CLEAR', and 'REFRESH'. The footer indicates 'Copyright © 1996-2011 NETGEAR'.

To configure or view details about the Green Ethernet feature on a port:

1. Within the Local Device Information, select the port to view or configure from the Interface menu.
2. Enable or disable the Energy Detect, Short Reach, or EEE administrative modes on the interface.
3. If you make any changes to the Green Ethernet modes for the port, click **Apply**.
4. View the additional Green Ethernet information that displays for the port:

Field	Description
Cumulative Energy Saved on this port due to Green Mode(s) (Watts * Hours)	Shows the energy savings per port, per hour.
Operational Status (Energy Detect)	Shows the Green Mode operational status, either Inactive or Active.
Reason	Shows the Admin status, either Admin Down or Admin Up.
Operational Status (Short Reach)	Shows the operational status of the port, either Active or Inactive.
Reason	Shows the reason why the port is either Active or Inactive.
Rx Low Power Idle Event Count	This field is incremented each time MAC RX enters LP IDLE state. Shows the total number of Rx LPI Events since EEE counters are last cleared.
Rx Low Power Idle Duration (uSec)	This field indicates duration of Rx LPI state in 10us increments. Shows the total duration of Rx LPI since the EEE counters are last cleared.
Tx Low Power Idle Event Count	This field is incremented each time MAC TX enters LP IDLE state. Shows the total number of Tx LPI Events since EEE counters are last cleared.
Tx Low Power Idle Duration (uSec)	This field indicates duration of Tx LPI state in 10us increments. Shows the total duration of Tx LPI since the EEE counters are last cleared.
Tw_sys_tx (uSec)	Integer that indicates the value of Tw_sys that the local system can support.
Tw_sys_tx Echo (uSec)	Integer that indicates the remote system's Transmit Tw_sys that was used by the local system to compute the Tw_sys that it wants to request from the remote system.
Tw_sys_rx (uSec)	Integer that indicates the value of Tw_sys that the local system requests from the remote system.
Tw_sys_rx Echo (uSec)	Integer that indicates the remote systems Receive Tw_sys that was used by the local system to compute the Tw_sys that it can support.
Fallback Tw_sys (uSec)	Integer that indicates the value of fallback Tw_sys that the local system requests from the remote system.
Tx_dll_enabled	Data Link Layer Enabled: Initialization status of the EEE transmit Data Link Layer management function on the local system.

Field	Description
Tx_dll_ready	Data Link Layer ready: This variable indicates that the tx system initialization is complete and is ready to update/receive LLDP PDUs containing EEE TLV.
Rx_dll_enabled	Status of the EEE capability negotiation on the local system.
Rx_dll_ready	Data Link Layer ready: This variable indicates that the rx system initialization is complete and is ready to update/receive LLDP PDUs containing EEE TLV.
Time Since Counters Last Cleared	Time Since Counters Last Cleared (since the time of power up, or after EEE counters are cleared).

- To view information received from a partner link, select the port connected to the remote device from the Interface menu in the Remote Device Information area.

The page refreshes and shows the information in the following table if LLDP data has been received on the interface

Field	Description
Remote ID	Specifies the remote client identifier assigned to the remote system.
Remote Tw_sys_tx (uSec)	Integer that indicates the value of Tw_sys that the remote system can support.
Remote Tw_sys_tx Echo (uSec)	Integer that indicates the value Transmit Tw_sys echoed back by the remote system.
Remote Tw_sys_rx (uSec)	Integer that indicates the value of Tw_sys that the remote system requests from the local system.
Remote Tw_sys_rx Echo (uSec)	Integer that indicates the value of Receive Tw_sys echoed back by the remote system.
Remote Fallback Tw_sys (uSec)	Integer that indicates the value of fallback Tw_sys that the remote system is advertising.

- Click **Clear** to reset the counters on the page to their default values.
- Click **Refresh** to update the page with the current information.

Green Ethernet Summary

This page summarizes the Green Ethernet Summary settings currently in use.

To access this page, click **System > Management > Green Ethernet > Green Ethernet Summary**.

The screenshot shows the Netgear web interface for a GS728TS switch. The main content area is titled "Green Mode Statistics Summary" and contains three sections:

- Current Power Consumption by all ports in Stack (mWatts):** 5435
- Estimated Percentage Power Saving per stack (%):** 0
- Cumulative Energy Saving per Stack (Watts*Hours):** 0

Below this is a table titled "Green Features supported on this unit":

Unit	Green Features supported on this unit
1	Short-Reach Energy-Detect EEE LPI-History LLDP-Cap-Exchg Pwr-Usq-Est
6	Short-Reach Energy-Detect

At the bottom is a detailed table for interface settings:

Interface	Energy Detect Admin Mode	Energy Detect Operational Status	Short Reach Admin Mode	Short Reach Operational Status	EEE Admin Mode
1/g1	Disable	Inactive	Disable	Inactive	Disable
1/g2	Disable	Inactive	Disable	Inactive	Disable
1/g3	Disable	Inactive	Disable	Inactive	Disable
1/g4	Disable	Inactive	Disable	Inactive	Disable
1/g5	Disable	Inactive	Disable	Inactive	Disable
1/o6	Disable	Inactive	Disable	Inactive	Disable

The following table describes the information available on the Green Mode Statistics Summary page.

Field	Description
Current Power Consumption by all ports in Stack (mWatts)	Estimated Power Consumption by all ports in the stack in mWatts.
Estimated Percentage Power Saving per stack (%)	Estimated Percentage Power saved on all ports in the stack due to Green mode(s) enabled.
Cumulative Energy Saving per Stack (Watts*Hours)	Estimated Cumulative Energy saved per stack in (Watts x Hours) due to all green modes enabled.

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

Field	Description
Unit	Identifies the stack member number.
Green Features supported on this unit	List of Green Features supported on the given unit which could be one or more of the following: <ul style="list-style-type: none"> • Energy-Detect (Energy Detect) • Short-Reach (Short Reach) • EEE (Energy Efficient Ethernet) • LPI-History (EEE Low Power Idle History) • LLDP-Cap-Exchg (EEE LLDP Capability Exchange) • Pwr-Usg-Est (Power Usage Estimates).
Interface	Identifies the interface associated with the rest of the data in the row.
Energy Detect Admin Mode	Shows whether Energy Detect Mode is administratively enabled on the port.
Energy Detect Operational Status	Shows the current operational status of the Green Mode for the selected port.
Short Reach Admin Mode	Shows the administrative status of Short Reach Mode on the port. With short reach mode enabled, PHY goes into low power mode when cable length is less than a given limit.
Short Reach Operational Status	Indicates whether the port is in low-power mode due to the cable length.
EEE Admin Mode	Shows the administrative status of Energy Efficient Ethernet Mode on the port. With EEE mode enabled, the port transitions to low power mode during link idle condition.

Click **Refresh** to update the page with the most current data from the switch

Green Ethernet LPI History

Use this page to set the sampling interval for EEE LPI data and to specify the number of samples to keep. From this page, you can also view per-port EEE LPI data.

To access this page, click **System > Management > Green Ethernet > Green Ethernet LPI History**.

The screenshot shows the Netgear web interface for a GS728TS switch. The main content area is titled "Port GreenMode EEE History". It features a configuration section with the following fields:

- Interface:** 1/g1 (dropdown menu)
- Sampling Interval:** 3600 (range: 30 to 36000)
- Max Samples to keep:** 168 (range: 1 to 168)
- Percentage LPI time per Stack:** 0

Below the configuration fields is a table with the following columns:

Sample No.	Time Since The Sample Was Recorded	Percentage Time spent in LPI mode since last sample	Percentage Time spent in LPI mode since last reset
1			

At the bottom of the page, there are "APPLY" and "REFRESH" buttons. The footer of the page reads "Copyright © 1996-2011 NETGEAR".

You do not need to select a port to configure the LPI sampling interval and maximum number of samples to keep. These settings are global, and the values you specify are applied to all ports. To configure the LPI settings for the switch:

1. Specify the LPI sampling interval, which determines the interval at which EEE LPI data needs to be collected. the default value is 3600, and the range is 30 to 36000.
2. Specify the maximum number of LPI samples to store on the switch. The default is 168, and the range is 1 to 168.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
4. Click **Refresh** to refresh the page with the most current data from the switch.

The page also provides the information shown in the following table:

Field	Description
Percentage LPI time per Stack	Time spent in LPI mode since EEE counters are last cleared.
Sample No	Sample index.
Time Since The Sample Was Recorded	Each time the page is refreshed it shows a different time as it reflects the difference in current time and time at which the sample was recorded.
Percentage Time spent in LPI mode since last sample	Percentage of time spent in LPI mode during the current measurement interval.
Percentage Time spent in LPI mode since last reset	Percentage of time spent in LPI mode since EEE LPI statistics were last reset.

Stacking

A stackable switch is a switch that is fully functional operating as a stand-alone unit but can also be set-up to operate together with up to five other switches. This group of switches shows the characteristics of a single switch while having the port capacity of the sum of the combined switches.

From the Stacking link under the System tab, you can access the following pages:

- [Stack Configuration](#) on page 63
- [Stack Port Configuration](#) on page 66
- [Stack Port Diagnostics](#) on page 68
- [Stack Firmware Synchronization](#) on page 69

One of the switches in the stack controls the operation of the stack. This switch is called the stack *master*. The remaining switches in the stack are stack *members*. The stack members use stacking technology to behave and work together as a unified system. Layer 2 and higher protocols present the entire switch stack as a single entity to the network.

The stack master is the single point of stack-wide management. From the stack master, you configure the following:

- System-level (global) features that apply to all stack members
- Interface-level features for all interfaces on any stack member

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack master. Every stack member is uniquely identified by its own stack member number, which is from 1–6. The stack master can be any number within that range.

Stack Features

Stacking on the GS728TS, GS728TPS, GS752TS, and GS752TPS switches supports the following:

- Up to six switches per stack, which can be any combination of GS728TS, GS728TPS, GS752TS, or GS752TPS switches.
- Single IP address management through a web browser or the SCC.
- Master-slave configuration.
 - The master retains configuration for entire stack.
 - Automatic detection of new members, with synchronization of firmware (upgrade or downgrade as needed).
- Configuration updates across the stack through a single operation.
- Automatic master fail-over. Fully resilient stack with chain and ring topology.
- Hot swapping (insertion and removal) of stack members.

Firmware Synchronization and Upgrade

All stack members must run the same software version to ensure compatibility within the stack. By default, if a unit is added to the stack and its software version is not the same as the stack master, that unit is not allowed to join the stack. You can enable the Stack Firmware Auto Upgrade feature, which will automatically synchronize the firmware version on the new unit with the version running on the stack master. The synchronization operation may result in either upgrade or downgrade of firmware on the mismatched stack member.

Upgrading the firmware on a stack of switches is the same as upgrading the firmware on a single switch. After you download a new image by using the File Download page or SCC, the downloaded image is distributed to all the connected units of the stack.

Note: It is recommended to set the active image for all stack members the same as the active image of the stack master. In other words, if image1 is the active image on the stack master, all units should have image1 as the active image. For information about configuring the active image, see [Dual Image Configuration](#) on page 289.

Configuration Maintenance

The stack master stores and maintains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes. If the master is removed from the stack or becomes unavailable, another member will be elected master, and will then run from that saved configuration.

The switch master copies its running configuration to the stack member configured as the *standby* unit whenever it changes (subject to some restrictions to reduce overhead). This enables the standby unit to take over the stack operation with minimal interruption if the stack master becomes unavailable. The running-config synchronization also occurs when the running configuration is auto-saved on the stack master or when the standby unit changes.

Stack Master Election

All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master from among themselves. The following factors determine which switch is elected the stack master:

- The switch that is master always has priority to retain the role of master
- Assigned priority
- MAC address

When the stack is powered up and completes the boot process or the original stack master becomes unavailable, the stack master is determined through an election process.

The rules for stack master Election are as follows:

- If a unit had previously been elected stack master, then it will remain the stack master and other units will simply be stack members.
- If no units were stack masters, or more than one unit was a stack master, then the unit with the highest management preference is elected stack master. The management preference can be assigned by the administrator. However, if all units have the same management preference, then the unit with the highest MAC address is assigned as the stack master.

Factory Defaults Reset Behavior

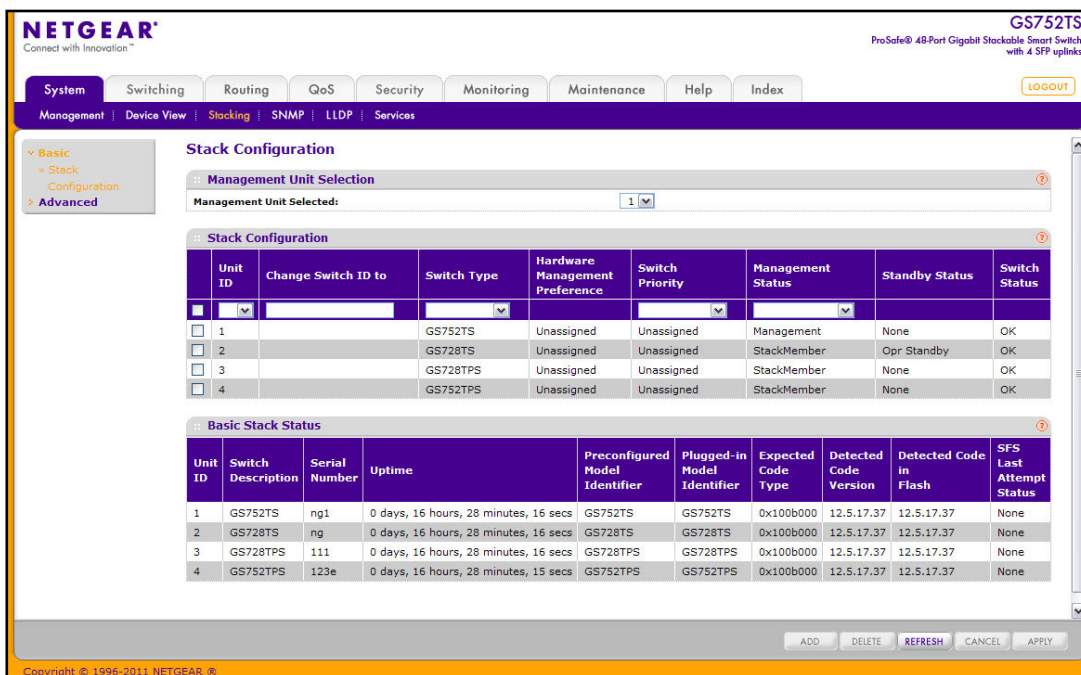
If the stack master is reset to the factory default settings (see [Factory Default](#) on page 281), the stack master applies the default settings to all the stack members and resets the stack, including all participating stack members. When the stack boots, the stack master election process begins.

Stack Configuration

From this page, you can preconfigure stack members before adding them to the stack, change the unit number assigned to a stack member, and to select a new stack master or give management preference to one or more units.

If you change the unit ID on a stack member, the member reloads. A stack move causes all routes and layer 2 addresses to be lost. The administrator is prompted to confirm the management move.

To display the Stack Configuration page, click **System > Stacking > Basic > Stack Configuration**. A screen similar to the following is displayed.



To select a new stack master:

1. In the **Management Unit Selected** menu, select the unit ID of the stack member to become the stack master.
2. A message indicating that moving stack management will unconfigure entire stack including all interfaces.
3. Click OK to confirm the selection and reload the stack. The stack will be unavailable until the boot process completes.

To configure a stack member before adding it to the stack:

1. Select the **Unit ID** of the stack member to add.
2. Select the switch model number of the new unit from the **Switch Type** field.
3. Optionally, specify the **Switch Priority** to select whether you want this unit to become a management unit in preference to another unit. The default value for this setting is undefined. If the preference level is set to zero, then the device cannot become a management unit. A higher value indicates a higher priority, the maximum value is 15.
4. Use the **Management Status** field to indicate whether the selected switch is the stack master, a normal stacking member, or the standby unit. A standby unit takes over the stack master responsibilities if the stack master becomes unavailable.
5. Click **Add** to add the preconfigured unit to the stack.

To change the settings for an existing stack member:

1. Select the check box next to the stack member to configure.
2. If desired, specify a new unit ID for the stack member in the **Change to Switch ID** field. The renumbering process causes the unit to reload.
3. Specify the switch type, priority, or management status from the available fields.
4. Click **Apply** to save the changes to the stack member.

Note: *If you configured a new unit number for an existing stack member, you are asked to confirm the change. Click **OK** to continue or **Cancel** to retain the original settings.*

5. Click **Delete** to remove the selected unit from the stack.
6. Click **Refresh** to update the page with the latest information 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.

The following table describes the Stack Configuration fields.

Field	Description
Hardware Management Preference	The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.
Standby Status	Identifies the switch that is configured as the Standby Unit. The possible values are: <ul style="list-style-type: none"> • Cfg Standby - Indicates that the unit is configured as the Standby Unit. The unit configured as the Standby switch becomes the stack manager if the current manager fails. • Opr Standby - Indicates that this unit is operating as the Standby Unit and the configured Standby Unit is not part of the stack. • None - The switch is not configured as the Standby Unit.
Switch Status	Displays the status of the selected unit. The possible values are: <ul style="list-style-type: none"> • OK • Unsupported • Code Mismatch • Config Mismatch • Not Present

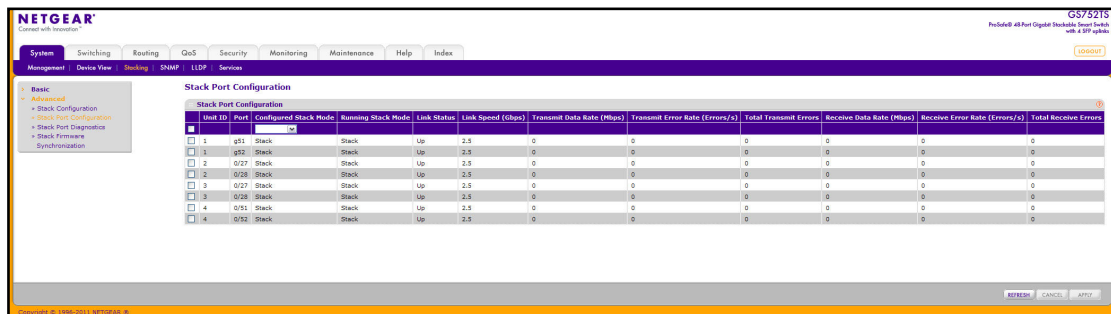
The following table describes the Basic Stack Status fields.

Field	Description
Unit ID	The unit ID of the specific switch.
Switch Description	The description for the unit can be configured by the user.
Serial Number	The unique box serial number for this switch.
Uptime	The displays the relative time since the last reboot of the switch.
Preconfigured Model Identifier	This field displays the model type assigned by the device manufacturer to identify the device.
Plugged-in Model Identifier	This field displays the model type assigned by the device manufacturer to identify the plugged-in device.
Expected Code Type	This field indicates the expected code type on this unit.
Detected Code Version	This field indicates the detected version of code on this unit.
Detected Code Version in Flash	The displays the Release number and version number of the code stored in flash.
SFS Last Attempt Status	This displays the status of last tried stack firmware synchronisation. "None" is the default value if SFS has not been tried.

Stack Port Configuration

By default, the stack ports on each switch are configured for stacking. However, you can use these ports as standard Ethernet ports. Use the Stack Port configuration page to configure the mode of the stack ports and to view information about the ports.

To display the Stack Port Configuration page, click **System > Stacking > Advanced > Stack Port Configuration**. A screen similar to the following is displayed.



To configure the mode of the stack ports:

1. Select the check box associated with the unit and port to configure:
2. From the **Configured Stack Mode** field, select the operating mode:
 - **Stack.** The port connects to the stack port on another stack member. This is the default value.
 - **Ethernet.** The port operates as a standard switch port that receives and transmits network traffic
3. Click **Apply** to apply the new settings to the system.
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 **Refresh** to update the screen with the current information.

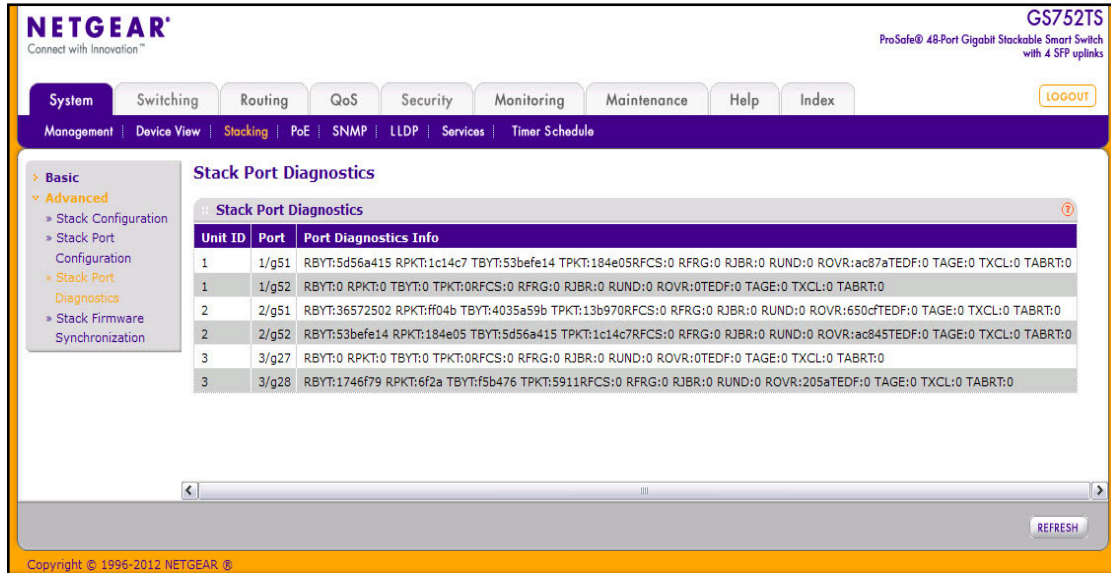
The following table describes Stack Port Configuration fields.

Field	Description
Unit ID	Displays the unit.
Port	Displays the stackable interfaces on the given unit.
Running Stack Mode	Displays the run-time mode of the stackable interface.
Link Status	Displays the link status (UP/DOWN) of the port.
Link Speed (Gbps)	Displays the maximum speed of the stacking port.
Transmit Data Rate (Mbps)	Displays the approximate transmit rate on the stacking port.
Transmit Error Rate	Displays the number of errors in transmit packets per second.
Total Transmit Errors	Displays the total number of errors in transmit packets since boot. The counter may wrap.
Data Rate (Mbps)	Displays the approximate receive rate on the stacking port.
Receive Error Rate	Displays the number of errors in receive packets per second.
Total Receive Errors	Displays the total number of errors in receive packets since boot. The counter may wrap.

Stack Port Diagnostics

This page displays the diagnostics for all the stackable interfaces in the given stack.

To display the Stack Port Diagnostics page, click **System > Stacking > Advanced > Stack Port Diagnostics**. A screen similar to the following is displayed.

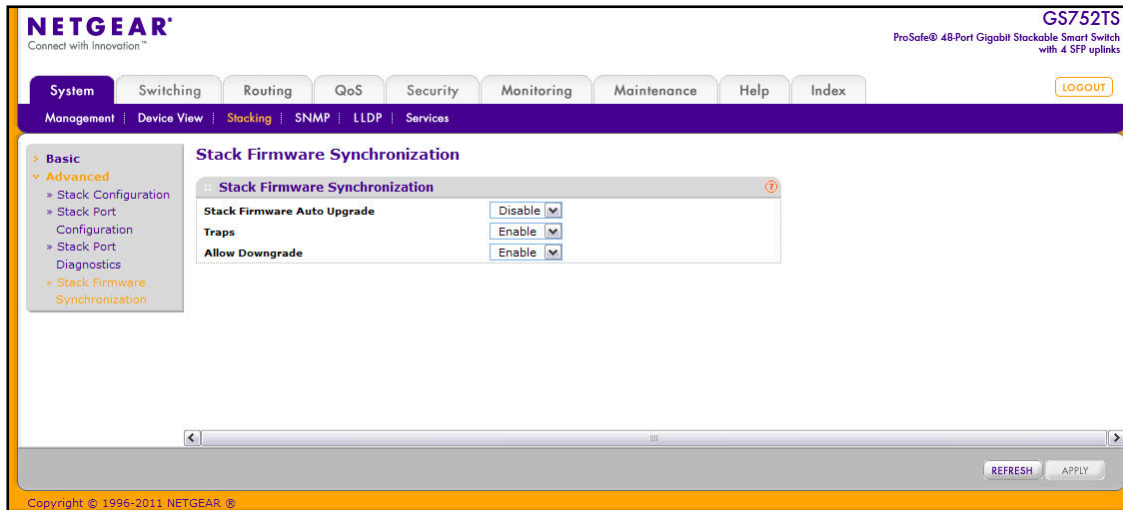


The following table describes the Stack Port Diagnostics fields.

Field	Definition
Unit ID	Displays the unit.
Port	Displays the stackable interface on the given unit.
Port Diagnostics Info	Displays three text fields (80 character strings) populated by the driver containing debug and status information.

Stack Firmware Synchronization

To display the stack firmware synchronization configurations from the Stack Firmware Synchronization page, click **System** > **Stacking** > **Advanced** > **Stack Firmware Synchronization**. A screen similar to the following is displayed.



To configure the Stack Firmware Synchronization features:

1. Specify whether **Stack Firmware Auto Upgrade** is enabled or disabled. This feature determines what to do when a new member attempts to join the stack, and its firmware does not match the version running on the master.
 - **Enable**. The stack master upgrades the version on the new member to match the version running on the rest of the stack.
 - **Disable**. The new member is not allowed to join.
2. Use the **Traps** field to enable or disable sending of traps during Stack Firmware Synchronization Start, Failure, or Finish.
3. Use the **Allow Downgrade** field to determine whether the stack master should downgrade the firmware version on a new member that attempts to join the stack if the new member has a firmware version that is more recent than the stack.
4. Click **Refresh** to update the page with the latest information from the switch.
5. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

PoE/PoE+ (GS728TPS and GS752TPS Only)

Ports g1–g8 on the GS728TPS and GS752TPS are PoE+ (IEEE 802.3at) compliant ports. Each port is capable of delivering up to 30W of reliable, uninterrupted power to connected PoE-powered devices (PD). Ports g9–g24 on the GS728TPS and ports g9–g48 on the GS752TPS are PoE (IEEE 802.3af) ports that are capable of delivering up to 15W of power to connected PDs.

The GS728TPS can provide a total of 192W of power to all connected devices. The GS752TPS can provide a total of 384W of power to all connected devices. You can configure per-port priority settings, timers, and power limits to manage the power supplied to the connected PDs and to ensure that the power budget for each switch is used effectively.

From the PoE link under the System tab, you can view and configure PoE settings for the switch and for ports.

From the PoE link, you can access the following pages:

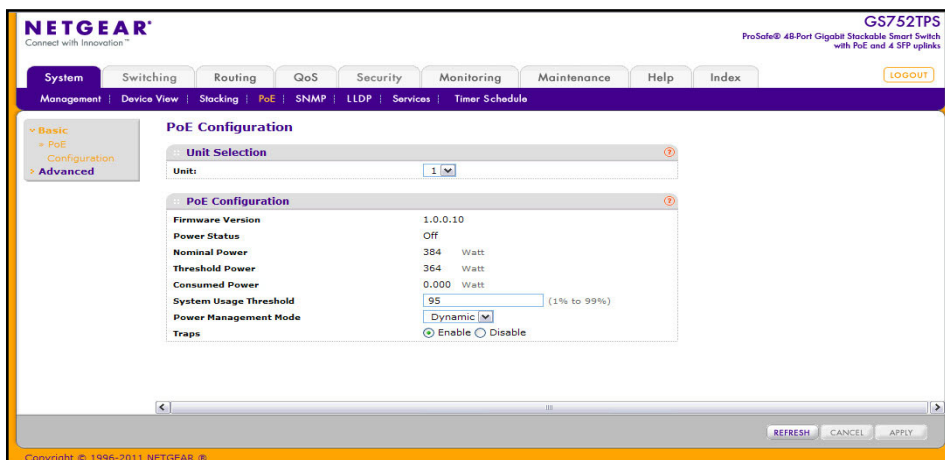
- [PoE Configuration](#) on page 70
- [PoE Port Configuration](#) on page 72

PoE Configuration

Use the PoE Configuration page to view global PoE power information and to configure PoE settings.

To display the PoE Configuration page, click **System > PoE > Basic > PoE Configuration**.

Note: You can also access the PoE Configuration page by clicking **System > PoE > Advanced > PoE Configuration**.



To configure PoE trap settings:

1. If you are managing a stack of switches, select the ID of the stack member to configure from the **Unit** menu.
2. Specify the percentage of the threshold power that must be consumed before a trap is sent.
3. Select the power management algorithm the switch uses to deliver power to the requesting PDs.
 - **Static.** The Power allocated for each port depends on the type of power threshold configured on the port.
 - **Dynamic.** The power consumption of each port is measured and calculated in real-time.
4. Select the appropriate radio button to enable or disable SNMP traps for PoE.
5. Click **Apply** to apply the new settings to the system.
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. Click **Refresh** to update the screen with the current information.

The PoE Configuration page also provides the following information:

Field	Description
Firmware Version	Version of the PoE controller's FW image.
Power Status	Indicates whether the PoE capability is on or off.
Nominal Power	Indicates the nominal amount of power the switch can provide to all ports.
Threshold Power	Shows the amount of power the system can consume before the system will not provide power to an additional port.
Consumed Power	Shows the total amount of power currently being delivered to all ports.

PoE Port Configuration

Use the PoE Port Configuration page to configure per-port PoE settings.

To display the PoE Port Configuration page, click **System > PoE > Advanced > PoE Port Configuration**.

Port	Admin Mode	High Power	Max Power	Port Priority	High Power Mode	Power Limit Type	Power Limit (Watts)	Detection Type	Class	Timer Schedule	Output Voltage (Volts)	Output Current (mA)	Output Power (Watts)	Status	Fault Status
<input type="checkbox"/> 1/01	Enable	Yes	32.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error
<input type="checkbox"/> 1/02	Enable	Yes	32.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error
<input type="checkbox"/> 1/03	Enable	Yes	32.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error
<input type="checkbox"/> 1/04	Enable	Yes	32.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error
<input type="checkbox"/> 1/05	Enable	Yes	32.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error
<input type="checkbox"/> 1/06	Enable	Yes	32.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error
<input type="checkbox"/> 1/07	Enable	Yes	32.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error
<input type="checkbox"/> 1/08	Enable	Yes	32.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error
<input type="checkbox"/> 1/09	Enable	No	18.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error
<input type="checkbox"/> 1/10	Enable	No	18.0	Low	Disable	User	15,200	ieee	Unknown	None	0	0	0.000	Searching	No Error

To configure PoE Port settings:

1. Select the check box next to the port to configure. Select multiple check boxes to apply the same settings to each selected port. Select the check box in the heading row to apply the same settings to all ports.
2. Configure or view the settings:
 - **Admin Mode.** Enable or disable the ability of the port to deliver power.
 - **High Power.** Indicates whether the port supports High Power Mode.
 - **Max Power.** Shows the maximum power, in Watts, the port can provide.
 - **Port Priority.** Determine which ports can deliver power if the total power delivered by the switch crosses a certain threshold. The switch may not be able to supply power to all connected devices. Priority is used to determine which ports can supply power. When ports have the same priority, the lower numbered port is given a higher priority. The possible priority levels are Critical (highest priority), High, and Low.

- **High Power Mode.** Select the power-up mode for the port
 - **Disable:** A port is powered in the IEEE 802.3af mode. (Default)
 - **Legacy:** A port is powered using high-inrush current, which is used by legacy powered devices (PDs) with a power requirement greater than 15W from power up.
 - **Pre-802.3at.** A port is powered in the IEEE 802.3af mode initially and switched to the high-power IEEE 802.3at mode before 75 msec. Use this mode if the PD is *not* performing Layer 2 classification, or if the switch is performing two-event Layer 1 classification.
 - **802.3at.** A port is powered in IEEE 802.3at mode. If the PD class detected by the switch is not Class 4 (type 2), the port will power up the PD, but only Class 4 PDs can be powered up in the IEEE 802.3at mode.
- **Power Limit Type.** Select the type of power limit to use on the port, which is one of the following:
 - **Class:** Select this option to base the power limit on the detected class value. When this value is selected, the user-configured value configured in the Power Limit field is ignored.
 - **User:** Select this option to base the power limit on the value configured in the Power Limit field.
 - **None.** Select this option to indicate that no power limit type is used on the port.
- **Power Limit.** Set the maximum amount of power that can be delivered by a port when the Power Limit Type is *User*.
- **Detection Mode.** Select the PD detection mode the PSE port uses to detect an attached device. The detection mode can be one of the following modes:
 - **Auto.** The port performs four-point resistive detection (802.3af4point) followed by legacy detection.
 - **Pre-ieee.** The port performs legacy detection.
 - **ieee.** The port performs four-point resistive detection (802.3af4point).
- **Class.** View the class of the PD connected to the port. The class defines the range of power a PD is drawing from the system. The class is defined as:
 - **0:** 0.44–12.95W
 - **1:** 0.44–3.83W
 - **2:** 3.84–6.48W
 - **3:** 6.49–12.95W
 - **4:** 12.95–25.50W (802.3at Type 2 devices only)
- **Timer Schedule.** Select the timer schedule to use for the port. By default, no timer schedules are configured. To create a timer schedule, use the Timer Schedule Global Configuration page.
- **Output Voltage.** Shows the current voltage being delivered to device in Volts.
- **Output Current.** Shows the current being delivered to device in mA.
- **Output Power.** Shows the current power being delivered to device in Watts.

- **Status.** View the operational status of the port PD detection.
 - **Disabled.** Indicates no power is being delivered.
 - **DeliveringPower.** Indicates power is being drawn by a connected device.
 - **Fault.** Indicates a problem with the port.
 - **Test.** Indicates the port is in test mode.
 - **OtherFault.** Indicates the port is idle due to an error condition.
 - **Searching.** Indicates the port is not in one of the above states.
 - **Requesting Power.** Indicates that a valid PD has been detected, but the device is not able to deliver power to the PD due to a power management decision.
- **Fault Status.** Describes the error description when the PSE port is in fault status, which can be one of the following:
 - **No Error.** Specifies that the PSE port is not in any error state.
 - **MPS Absent.** Specifies that the PSE port has detected an absence of main power supply.
 - **Short.** Specifies that the PSE port has detected a short circuit condition.
 - **Overload.** Specifies that the PD connected to the PSE port had tried to provide more power than it is permissible by the hardware.
 - **Power Denied.** Specifies that the PSE port has been denied power because of shortage of power or due to administrative action.
- 3. Click **Apply** to apply the new settings to the system.
- 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 **Reset** to forcibly reset the selected port(s).

SNMP

From SNMP link under the System tab, you can configure SNMP settings for SNMPv1/v2 and SNMPv3.

From the SNMP link, you can access the following pages:

- [SNMPv1/v2](#) on page 75
- [Trap Flags](#) on page 78
- [SNMP v3 User Configuration](#) on page 79

SNMPv1/v2

The pages under the SNMPv1/v2 menu allow you to configure SNMP community information, traps, and trap flags.

Community Configuration

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

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.

The screenshot shows the Netgear web interface for a GS728TPS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The current page is 'Community Configuration' under the 'SNMP V1/V2' menu. The page title is 'Community Configuration'. Below the title is a table with the following data:

	Management Station IP	Management Station IP Mask	Community String	Access Mode	Status
<input type="checkbox"/>	0.0.0.0	0.0.0.0	public	ReadOnly	Enable
<input type="checkbox"/>	0.0.0.0	0.0.0.0	private	ReadWrite	Enable

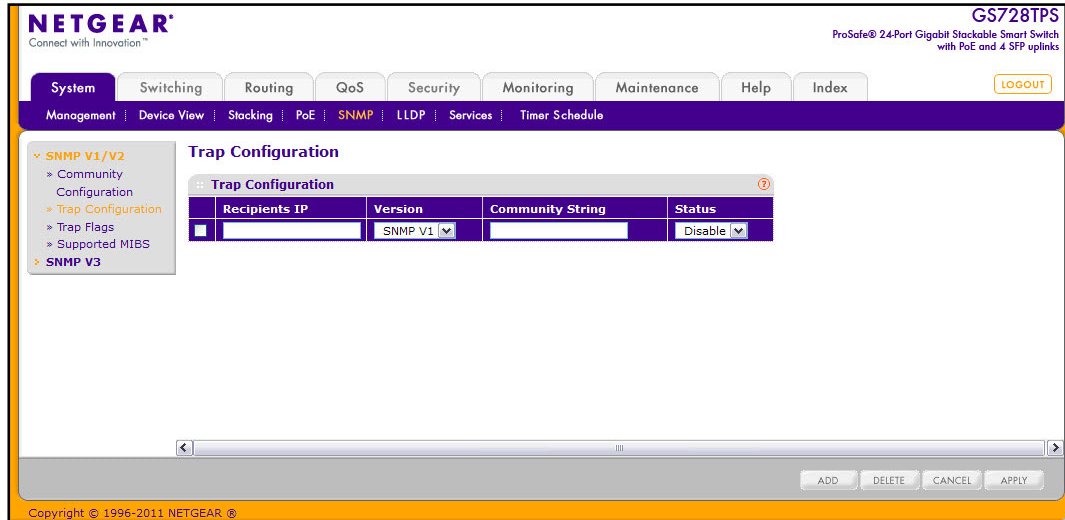
At the bottom of the page, there are buttons for ADD, DELETE, CANCEL, and APPLY. The footer contains the copyright information: Copyright © 1996-2011 NETGEAR ®.

To configure SNMP communities:

1. To add a new SNMP community, enter community information in the available fields described below, and then click **Add**.
 - **Management Station IP.** Specify the IP address of the management station. 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.** Specify the subnet mask to associate with the management station IP address.
 - **Community String.** Specify a community name. 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 menu.
 - **Status.** Specify the status of this community by selecting Enable or Disable from the pull down 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.
2. To modify an existing community, select the check box next to the community, change the desired fields, and then click **Apply**. Configuration changes take effect immediately.
3. To delete a community, select the check box next to the community 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.

Trap Configuration

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



To configure SNMP trap settings:

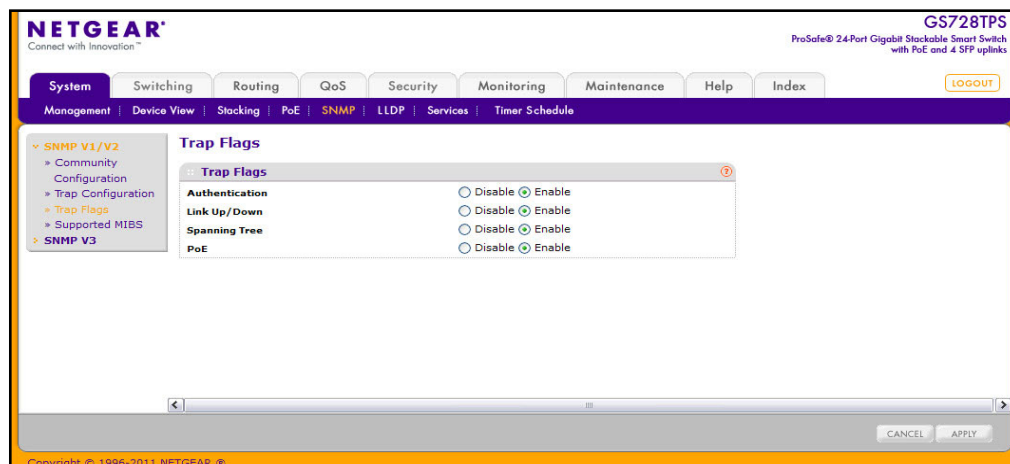
- To add a host that will receive SNMP traps, enter trap configuration information in the available fields described below, and then click **Add**.
 - Recipients IP.** The address in x.x.x.x format to receive SNMP traps from this device.
 - Version.** The trap version to be used by the receiver from the 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.** 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 menu:
 - Enable: Send traps to the receiver.
 - Disable: Do not send traps to the receiver.
- To modify information about an existing SNMP recipient, select the check box next to the recipient, change the desired fields, and then click **Apply**. Configuration changes take effect immediately.
- To delete a recipient, select the check box next to the recipient and click **Delete**.
- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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 send 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, click **System > SNMP > SNMP V1/V2 > Trap Flags**.



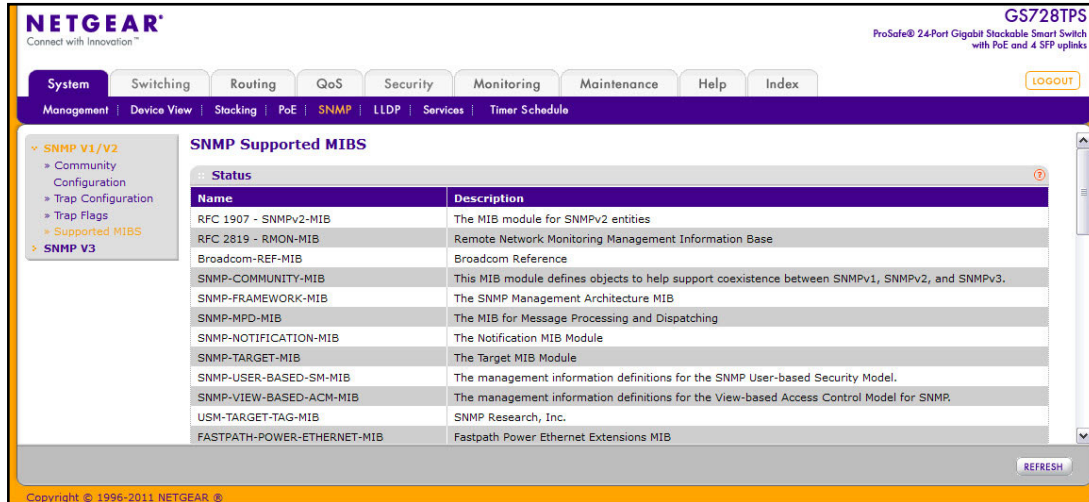
To configure the trap flags:

1. From the **Authentication** field, enable or disable activation of authentication failure traps by selecting the corresponding button. The factory default is Enable.
2. From the **Link Up/Down** field, enable or disable activation of link status traps by selecting the corresponding button. The factory default is Enable.
3. From the **Spanning Tree** field, enable or disable activation of spanning tree traps by selecting the corresponding button. The factory default is Enable.
4. For the GS728TPS and GS752TPS switches, use the **PoE** field to enable or disable activation of PoE traps. The factory default is Enable.
5. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

SNMP Supported MIBs

The SNMP Supported MIBs page lists the MIBs available for management by using a SNMP-based network management system.

To access the page, click **System > SNMP > SNMP V1/V2 > Supported MIBs**.

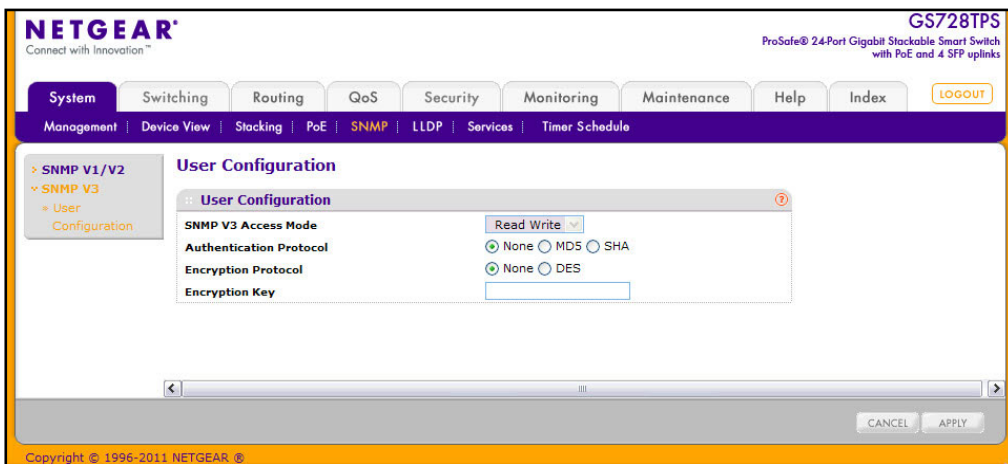


The page displays the name of each supported MIB file and provides a description of the module.

SNMP v3 User Configuration

This is the configuration for SNMP v3.

To access this page, click **System > SNMP > SNMP V3 > User Configuration**.



The SNMPv3 Access Mode is a read-only field that shows the access privileges for the user account. The admin account always has Read/Write access, and all other accounts have Read Only access.

To configure SNMPv3 settings for the user account:

1. In the Authentication Protocol field, 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.
2. In the Encryption Protocol field, choose whether to encrypt SNMPv3 packets transmitted by the switch.
 - **None.** Do not encrypt the contents of SNMPv3 packets transmitted from the switch.
 - **DES.** Encrypt SNMPv3 packets using the DES encryption protocol.
3. 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.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

LLDP

The IEEE 802.1AB-defined standard, Link Layer Discovery Protocol (LLDP), allows stations 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.

From the LLDP link, you can access the following pages:

- [LLDP Configuration](#) on page 81
- [LLDP Port Settings](#) on page 82
- [LLDP-MED Network Policy](#) on page 83
- [LLDP-MED Port Settings](#) on page 85
- [Local Information](#) on page 86
- [Neighbors Information](#) on page 88

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 enabled 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 Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP with the following features:

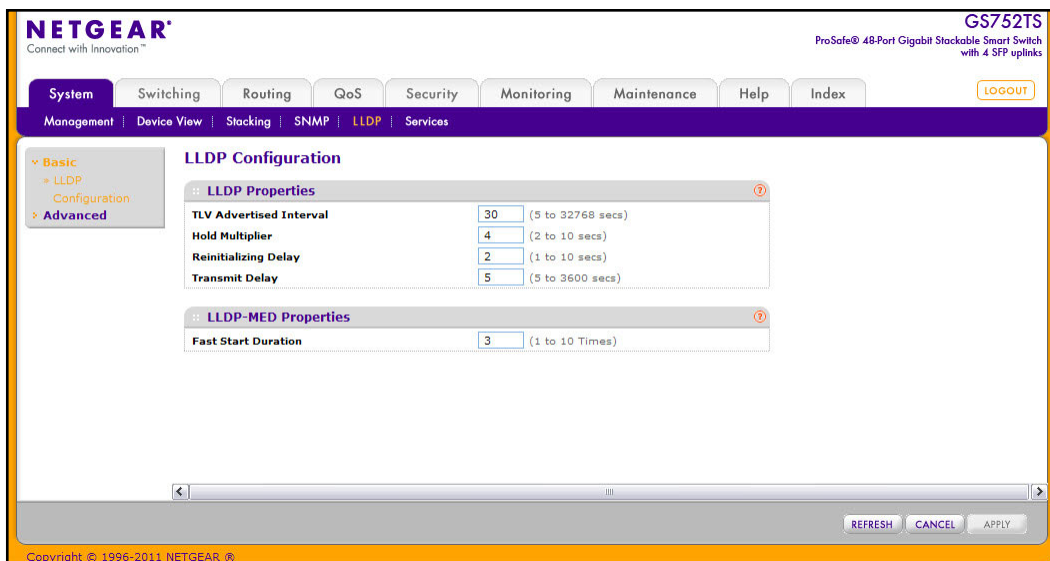
- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority, and DiffServ settings), enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet endpoints.
- Inventory management, enabling network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

LLDP Configuration

Use the LLDP Configuration page to specify LLDP and LLDP-MED parameters that are applied to the switch.

To display the LLDP Configuration page, click **System > LLDP > Basic > LLDP Configuration**.

Note: You can also access the LLDP Configuration page by clicking **System > LLDP > Advanced > LLDP Configuration**.



To configure global LLDP settings:

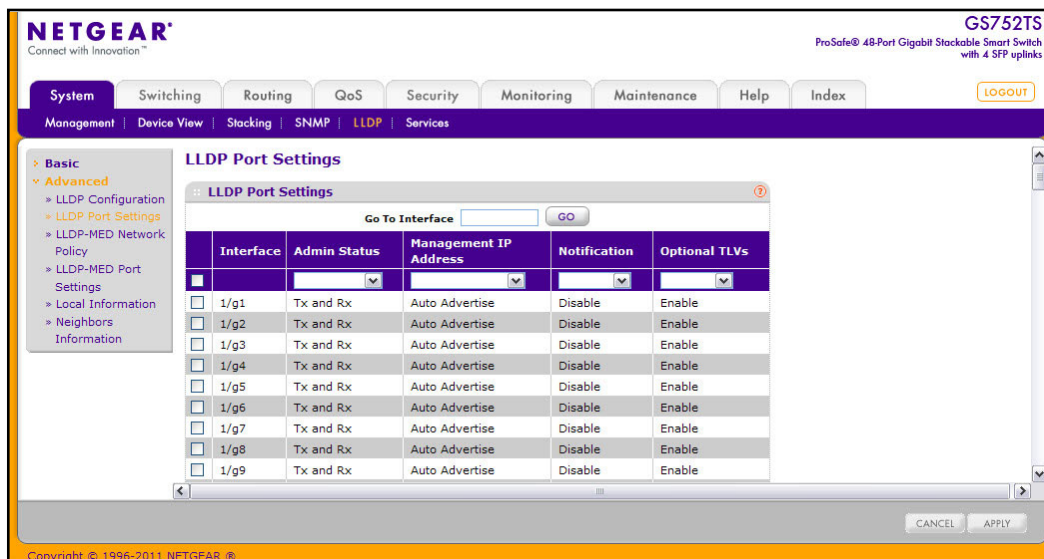
1. Configure the following LLDP properties.

- **TLV Advertised Interval.** Specify the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32768 seconds.
 - **Hold Multiplier.** Specify multiplier on the transmit interval to assign to Time-to-Live (TTL). The default is 4 seconds, and the range is 2–10.
 - **Reinitializing Delay.** Specify the delay before a reinitialization. The default is 2 seconds, and the range is 1–10 seconds.
 - **Transmit Delay.** Specify the interval for the transmission of notifications. The default is 5 seconds, and the range is 5–3600 seconds.
2. To change the LLDP-MED properties in the **Fast Start Duration** field, specify the number of LLDP packets sent when the LLDP-MED Fast Start mechanism is initialized, which occurs when a new endpoint device links with the LLDP-MED network connectivity device. The default value is 3 times, and the range is from 1–10.
 3. Click **Apply** to apply the new settings to the system.
 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 **Refresh** to update the screen with the current information.

LLDP Port Settings

Use the LLDP Port Settings page to specify LLDP parameters that are applied to a specific interface.

To display the LLDP Port Settings page, click **System > LLDP > Advanced > LLDP Port Settings**.



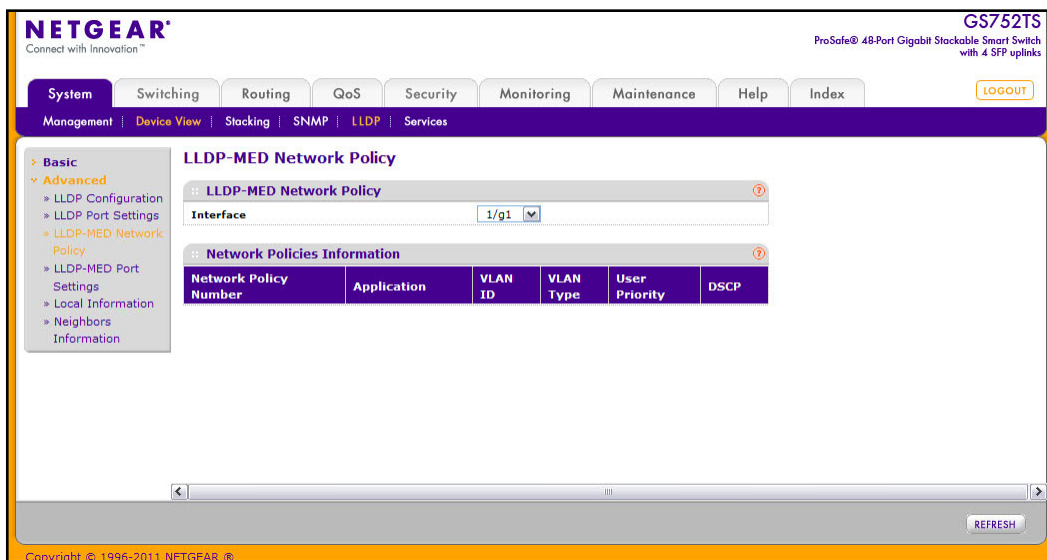
To configure LLDP port settings:

1. Change the LLDP port settings described below:
 - **Interface.** Specifies the port to be affected by these parameters.
 - **Admin Status.** Select the status for transmitting and receiving LLDP packets:
 - **Tx Only:** Enable only transmitting LLDP PDUs on the selected ports.
 - **Rx Only:** Enable only receiving LLDP PDUs on the selected ports.
 - **Tx and Rx:** Enable both transmitting and receiving LLDP PDUs on the selected ports. This is the default value.
 - **Disabled:** Do not transmit or receive LLDP PDUs on the selected ports.
 - **Management IP Address.** Choose whether to advertise the management IP address from the interface. The possible field values are:
 - **Stop Advertise:** Do not advertise the management IP address from the interface.
 - **Auto Advertise:** Advertise the current IP address of the device as the management IP address.
 - **Notification.** When notifications are enabled, LLDP interacts with the Trap Manager to notify subscribers of remote data change statistics. The default is Disabled.
 - **Optional TLV(s).** Enable or disable the transmission of optional type-length value (TLV) information from the interface. The TLV information includes the system name, system description, system capabilities, and port description. The default is Enabled. To configure the System Name, see [Management](#) on page 31. To configure the Port Description, see [Ports](#) on page 102.
2. If you make any changes to the page, click **Apply** to apply the new settings to the system.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

LLDP-MED Network Policy

This page displays information about the LLDP-MED network policy TLV transmitted in the LLDP frames on the selected local interface.

To display this page, click **System > LLDP > Advanced > LLDP-MED Network Policy**.



From the **Interface** menu, select the interface with the information to view. The following table describes the LLDP-MED network policy information that displays on the screen.

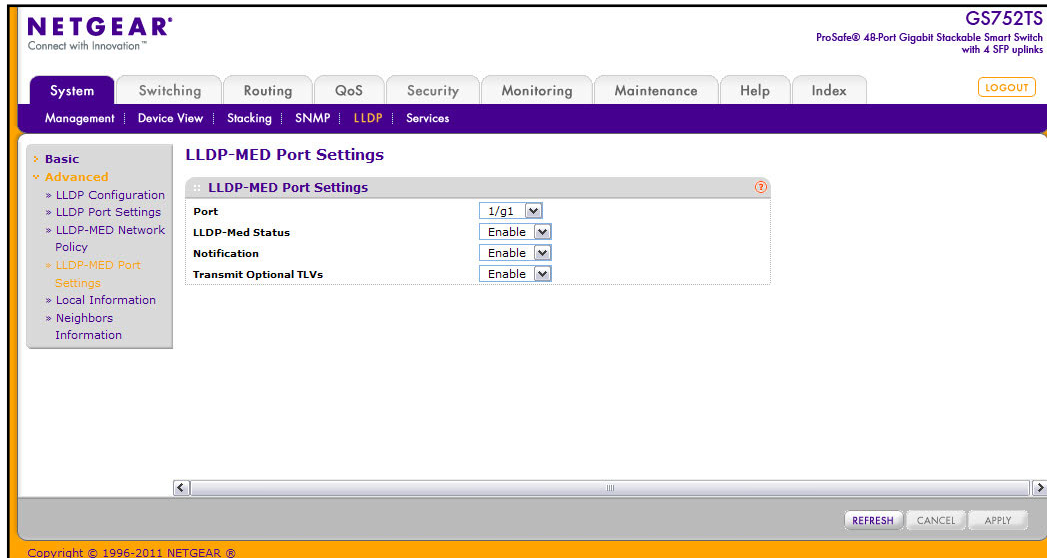
Field	Description
Device Information	
Chassis ID Subtype	Identifies the type of data the local switch displays in the Chassis ID field.
Chassis ID	Identifies the local 802 LAN switch.
System Name	Identifies the system name associated with the switch.
System Description	Provides a description of the switch, which is its model number.
System Capabilities	Specifies the system capabilities of the switch.
Port Information	
Network Policy Number	Specifies the policy number.
Application	Specifies the media application type associated with the policy. Only the Voice application type is supported. The application type that is received on the interface has the VLAN ID, priority, DSCP, <i>tagged</i> bit status and <i>unknown</i> bit status. This information is displayed only if a network policy TLV has been transmitted.
VLAN ID	Specifies the VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	Specifies the priority associated with the policy.
DSCP	Specifies the DSCP associated with a particular policy type.

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

LLDP-MED Port Settings

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

To display this page, click **System > LLDP > Advanced > LLDP-MED Port Settings**.



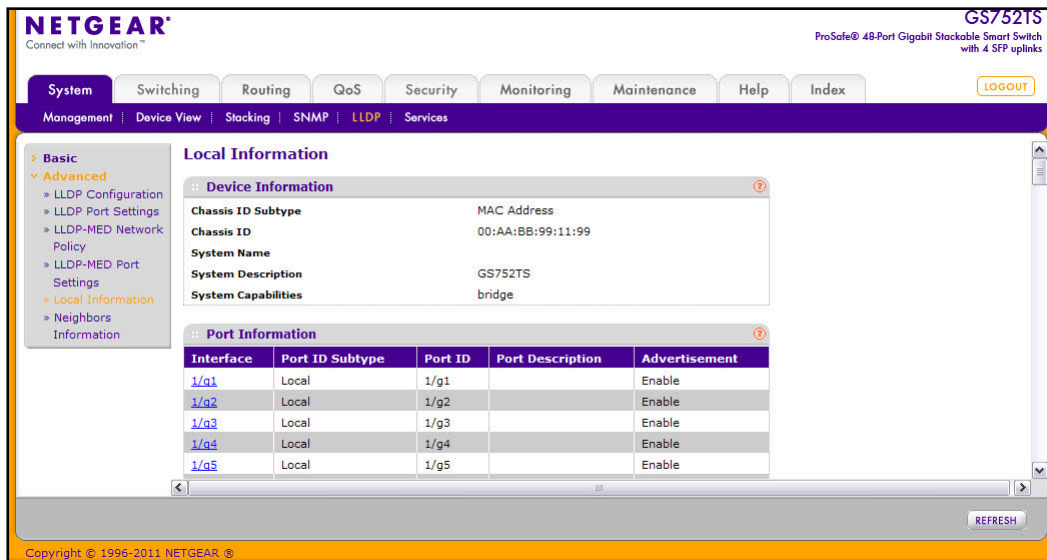
To configure LLDP-MED settings for a port:

1. From the **Port** field, select the port to configure.
2. From the **LLDP-MED Status** field, enable or disable the LLDP-MED mode for the selected interface.
3. From the **Notification** field, specify whether the port should send a topology change notification if a device is connected or removed.
4. From the **Transmit Optional TLVs** field, specify whether the port should transmit optional type length values (TLVs) in the LLDP PDU frames. If enabled, the following LLDP-MED TLVs are transmitted:
 - MED Capabilities
 - Network Policy
 - Location Identification
 - Extended Power via MDI: PSE
 - Extended Power via MDI: PD
 - Inventory
5. Click **Apply** to send the updated configuration to the switch. These changes occur immediately and the configuration will be saved.
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. Click **Refresh** to update the screen with the current information.

Local Information

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

To display the LLDP Local Device Information page, click **System > Advanced > LLDP > Local Information**.



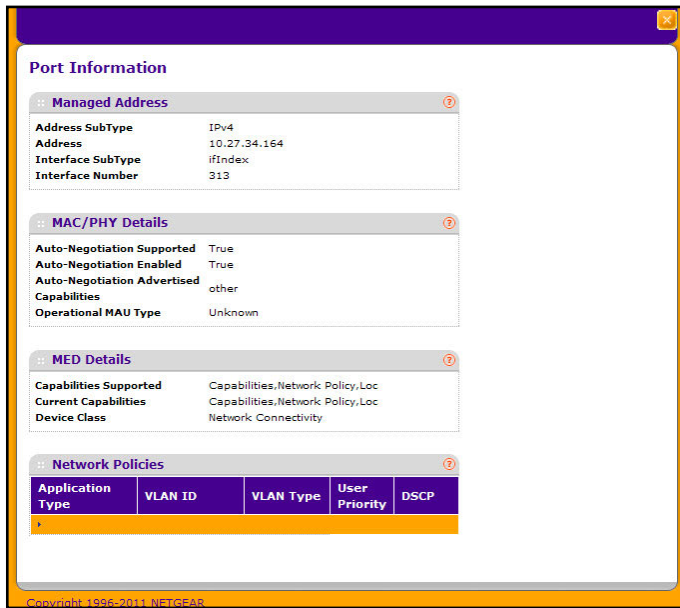
The following table describes the LLDP local information that displays for each port.

Field	Description
Interface	Select the interface with the information to display.
Port ID Subtype	Identifies the type of data displayed in the Port ID field.
Port ID	Identifies the physical address of the port.
Port Description	Identifies the user-defined description of the port. To configure the Port Description, see Ports on page 102.
Advertisement	Displays the advertisement status of the port.

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

To view additional details about a port, click the name of the port in the Interface column of the Port Information table.

A popup window displays information for the selected port.



The following table describes the detailed local information that displays for the selected port.

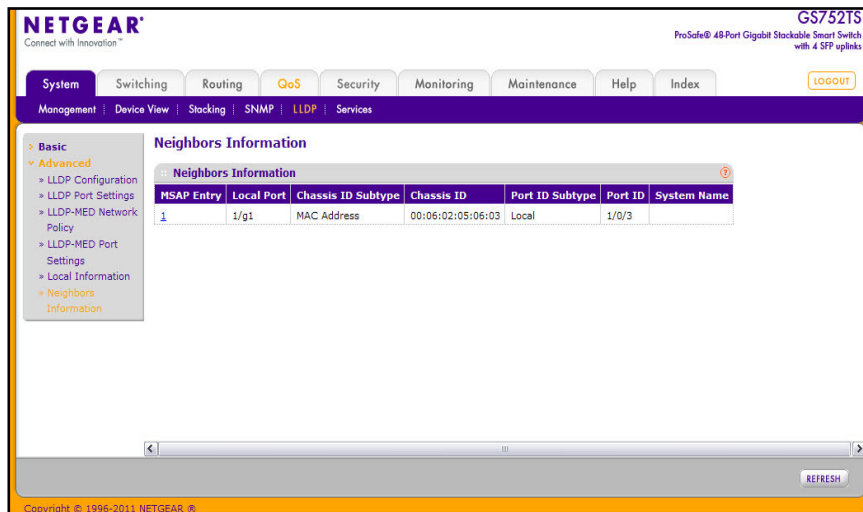
Field	Description
Managed Address	
Address SubType	Displays the type of address the management interface uses, such as an IPv4 address.
Address	Displays the address used to manage the device.
Interface SubType	Displays the port subtype.
Interface Number	Displays the number that identifies the port.
MAC/PHY Details	
Auto-Negotiation Supported	Specifies whether the interface supports port-speed auto-negotiation. The possible values are True or False.
Auto-Negotiation Enabled	Displays the port speed auto-negotiation support status. The possible values are True (enabled) or False (disabled).
Auto Negotiation Advertised Capabilities	Displays the port speed auto-negotiation capabilities such as 1000BASE-T half-duplex mode or 100BASE-TX full-duplex mode.
Operational MAU Type	Displays the Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network.

Field	Description
MED Details	
Capabilities Supported	Displays the MED capabilities enabled on the port.
Current Capabilities	Displays the TLVs advertised by the port.
Device Class	Network Connectivity indicates the device is a network connectivity device.
Network Policies	
Application Type	Specifies the media application type associated with the policy.
VLAN ID	Specifies the VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	Specifies the priority associated with the policy.
DSCP	Specifies the DSCP associated with a particular policy type.

Neighbors Information

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

To display the LLDP Neighbors Information page, click **System > LLDP > Advanced > Neighbors Information**.



The following table describes the information that displays for all LLDP neighbors that have been discovered.

Field	Description
MSAP Entry	Displays the Media Service Access Point (MSAP) entry number for the remote device.
Local Port	Displays the interface on the local system that received LLDP information from a remote system.
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. If the field is blank, the name might not be configured on the remote system.

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

To view additional information about the remote device, click the link in the MSAP Entry field.

The image displays two screenshots of a network management interface showing LLDP neighbor details.

Left Screenshot: Neighbors Information

- Port Details:** Local Port: 1/g1, MSAP Entry: 1
- Basic Details:** Chassis ID SubType: MAC Address, Chassis ID: 00196102105106103, Port ID SubType: Local, Port ID: 1/0/3, Port Description: , System Name: , System Description: GSM7352S - NetGear GSM7352S - 48 GE, 4 TENGIG, System Capabilities: bridge, router
- Managed Address:** Table with columns: Address SubType, Address, Interface SubType, Interface Number.
- MAC/PHY Details:** Auto-Negotiation Supported: N/A, Auto-Negotiation Enabled: N/A, Auto-Negotiation Advertised: N/A, Capabilities: , Operational MAU Type: N/A

Right Screenshot: Expanded Details

- MED Details:** Capabilities Supported: N/A, Current Capabilities: N/A, Device Class: N/A, PoE Device Type: N/A, PoE Power Source: N/A, PoE Power Priority: N/A, PoE Power Value: N/A, Hardware Revision: N/A, Firmware Revision: N/A, Software Revision: N/A, Serial Number: N/A, Model Name: N/A, Asset ID: N/A
- Location Information:** Civic: N/A, Coordinates: N/A, ECS ELIN: N/A, Unknown: N/A
- Network Policies:** Table with columns: Application Type, VLAN ID, VLAN Type, User Priority, DSCP.
- LLDP Unknown TLVs:** Table with columns: Type, Value.

Copyright 1996-2011 NETGEAR

A popup window displays information for the selected port. The following table describes the fields in the popup window.

Field	Description
Port Details	
Local Port	Displays the interface on the local system that received LLDP information from a remote system.
MSAP Entry	Displays the Media Service Access Point (MSAP) entry number for the remote device.
Basic Details	
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.
Port Description	Identifies the user-defined description of the port.
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.
System Capabilities	Specifies the system capabilities of the remote system.
Managed Addresses	
Address SubType	Specifies the type of the management address.
Address	Specifies the advertised management address of the remote system.
Interface SubType	Specifies the port subtype.
Interface Number	Identifies the port on the remote device that sent the information.
MAC/PHY Details	
Auto-Negotiation Supported	Specifies whether the remote device supports port-speed auto-negotiation. The possible values are True or False
Auto-Negotiation Enabled	Displays the port speed auto-negotiation support status. The possible values are True or False
Auto Negotiation Advertised Capabilities	Displays the port speed auto-negotiation capabilities.
Operational MAU Type	Displays the Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network.

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

Field	Description
MED Details	
Capabilities Supported	Specifies the supported capabilities that were received in MED TLV from the device.
Current Capabilities	Specifies the advertised capabilities that were received in MED TLV from the device.
Device Class	Displays the LLDP-MED endpoint device class. The possible device classes are: <ul style="list-style-type: none"> • Endpoint Class 1 Indicates a generic endpoint class, offering basic LLDP services. • Endpoint Class 2 Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features. • Endpoint Class 3 Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support and device information management capabilities.
PoE Device Type	Displays the port PoE type. For example, PSE or PD.
PoE Power Source	Displays the port's power source.
PoE Power Priority	Displays the port's power priority.
PoE Power Value	Displays the port's power value.
Hardware Revision	Displays the hardware version advertised by the remote device.
Firmware Revision	Displays the firmware version advertised by the remote device.
Software Revision	Displays the software version advertised by the remote device.
Serial Number	Displays the serial number advertised by the remote device.
Model Name	Displays the model name advertised by the remote device.
Asset ID	Displays the asset ID advertised by the remote device.
Location Information	
Civic	Displays the physical location, such as the street address, the remote device has advertised in the location TLV. For example, 123 45th St. E. The field value length range is 6–160 characters.
Coordinates	Displays the location map coordinates the remote device has advertised in the location TLV, including latitude, longitude and altitude.
ECS ELIN	Displays the Emergency Call Service (ECS) Emergency Location Identification Number (ELIN) the remote device has advertised in the location TLV. The field range is 10–25.
Unknown	Displays unknown location information for the remote device.

Field	Description
Network Policies	
Application Type	Specifies the media application type associated with the policy advertised by the remote device.
VLAN ID	Specifies the VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	Specifies the priority associated with the policy.
DSCP	Specifies the DSCP associated with a particular policy type.
LLDP Unknown TLVs	
Type	Displays the unknown TLV type field.
Value	Displays the unknown TLV value field.

Services — DHCP Snooping

DHCP Snooping is a useful feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network. 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.

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also provides way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

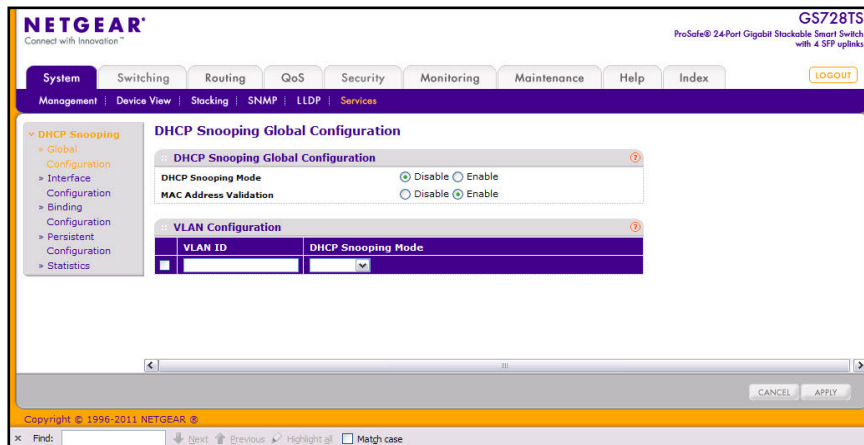
From the Services link, you can access the following pages:

- [DHCP Snooping Global Configuration](#) on page 93
- [Interface Configuration](#) on page 94
- [Binding Configuration](#) on page 95
- [Persistent Configuration](#) on page 97
- [Statistics](#) on page 98

DHCP Snooping Global Configuration

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

To access the DHCP Snooping Configuration page, click **System > Services > DHCP Snooping > Global Configuration**.



To configure global DHCP Snooping settings:

1. In the **Admin Mode** field, select **Enable** or **Disable** to turn the DHCP Snooping feature on or off. DHCP snooping is globally disabled by default.
2. In the MAC Address Validation field, select **Enable** to allow the switch to validate the sender MAC address for DHCP snooping. If **Disable** is selected, the switch will not check the source MAC address. MAC address validation is enabled by default.
3. Configure the DHCP snooping mode for VLANs. Enter the VLAN ID and specify whether to enable or disable DHCP snooping:
 - **Enable**. When a DHCP packet is received on a routing VLAN, the DHCP snooping application applies its filtering rules and updates the bindings database. If a client message passes filtering rules, the message is placed into the software forwarding path, where it may be processed by the DHCP relay agent, the local DHCP server, or forwarded as an IP packet.
 - **Disable**. Traffic in the VLAN is not snooped for DHCP messages.
4. Click **Apply** to apply the change to the system. The changes take effect immediately.
5. 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 Snooping Interface Configuration page to view and configure each port or LAG as trusted or untrusted. 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 Snooping Interface Configuration page, click **System > Services > DHCP Snooping > Interface Configuration**.

The screenshot shows the Netgear web interface for a GS728TS switch. The main navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar shows the DHCP Snooping configuration tree. The main content area is titled 'DHCP Snooping Interface Configuration' and contains a table with the following data:

Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
<input type="checkbox"/> 1/g1	Disable	Disable	N/A	N/A
<input type="checkbox"/> 1/g2	Disable	Disable	N/A	N/A
<input type="checkbox"/> 1/g3	Disable	Disable	N/A	N/A
<input type="checkbox"/> 1/g4	Disable	Disable	N/A	N/A
<input type="checkbox"/> 1/g5	Disable	Disable	N/A	N/A
<input type="checkbox"/> 1/g6	Disable	Disable	N/A	N/A
<input type="checkbox"/> 1/g7	Disable	Disable	N/A	N/A
<input type="checkbox"/> 1/g8	Disable	Disable	N/A	N/A

To configure DHCP snooping settings for an interface:

1. To configure DHCP snooping settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure DHCP snooping settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure DHCP snooping settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Choose the **Trust Mode** for the selected port(s) or LAG(s).
 - **Enable:** Any DHCP responses received on this port are forwarded. The port connected downstream from 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.
 - **Disable:** Any DHCP (or BootP) responses received on this port are discarded. Ports connected to hosts should be configured as untrusted. This is the default value.
6. Use the **Logging Invalid Packets** menu to choose whether to log invalid packets. When enabled, the DHCP snooping application sends a log message to the buffered log to record invalid packets received on this interface. The factory default is disabled.

7. Use the **Rate Limit (pps)** field to specify the rate limit value for DHCP Snooping purpose. If the incoming rate of DHCP packets exceeds the value of this object for consecutively burst interval seconds, the port will be shutdown. If this value is N/A, then burst interval has no meaning, hence it is disabled. The default value is N/A. The range of Rate Limit is (0 to 300).
8. Use the **Burst Interval (secs)** field to specify the burst interval value for rate limiting purpose on this interface. If the rate limit is N/A, then the burst interval has no meaning and it is not applicable. The default value is N/A. The range of Burst Interval is (1 to 15).
9. Click **Apply** to apply the change to the system. Configuration changes take effect immediately.
10. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Binding Configuration

The DHCP snooping application uses DHCP messages to build and maintain the binding's database. The binding's database only includes data for clients on untrusted ports. You can create static binding by manually configuring information in the bindings database. The DHCP snooping feature dynamically creates a tentative binding from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to a port (the port where the DHCP client message was received). Tentative bindings are completed when DHCP snooping learns the client's IP address from a DHCP ACK message on a trusted port. DHCP snooping removes bindings in response to DECLINE, RELEASE, and NACK messages. The DHCP snooping application ignores the ACK messages as a reply to the DHCP Inform messages received on trusted ports. You can also enter static bindings into the binding database.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database.

To access the DHCP Snooping Binding Configuration page, click **System > Services > DHCP Snooping > Binding Configuration**.

The screenshot shows the Netgear web interface for a GS728TS switch. The main content area is titled "DHCP Snooping Binding Configuration". It features two configuration sections:

- Static Binding Configuration:** A table with columns for Interface, MAC Address, VLAN ID, and IP Address. There is a checkbox in the first row.
- Dynamic Binding Configuration:** A table with columns for Interface, MAC Address, VLAN ID, IP Address, and Lease Time.

At the bottom of the configuration area, there are buttons for ADD, DELETE, CLEAR, REFRESH, and CANCEL. The footer of the page indicates "Copyright © 1996-2011 NETGEAR".

To configure static DHCP bindings in the database:

1. Select the interface to add a static binding to into the DHCP snooping database.
2. Specify the MAC address for the binding to be added. This is the key to the binding database.
3. In the **VLAN ID** field, select the from the VLANs that exist on the switch for the binding rule. The range of the VLAN ID is (1 to 4093).
4. In the **IP Address** field, specify a valid IP Address for the binding rule.
5. Click **Add** to add the DHCP snooping binding entry into the database.
6. Click **Delete** to delete the selected static entries from the database.
7. Click **Clear** to delete all DHCP Snooping binding entries.
8. Click **Refresh** to refresh the data on the screen with the latest DHCP Snooping Dynamic Binding information.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

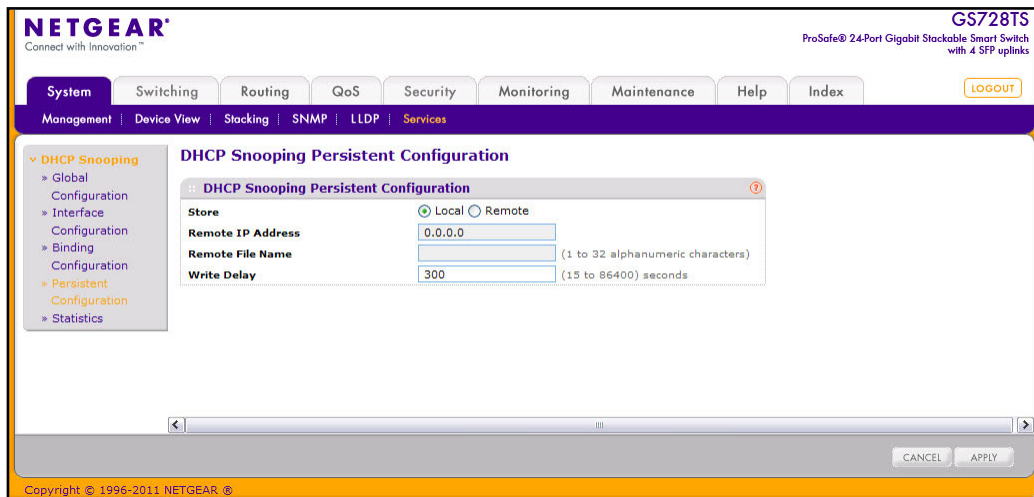
For DHCP Snooping Dynamic Binding Configuration table shows the bindings that have been learned on the switch through DHCP snooping. The following table describes the available fields.

Field	Description
Interface	Displays the interface on which the binding was learned.
MAC Address	Displays the MAC address for the binding in the binding database.
VLAN ID	Displays the VLAN for the binding entry in the binding database. The range of the VLAN ID is 1 to 4093.
IP Address	Displays the IP Address for the binding entry in the binding database.
Lease Time	Displays the remaining Lease time for the Dynamic entries.

Persistent Configuration

Use the DHCP Snooping Persistent Configuration page to configure the persistent location of the DHCP snooping database. Bindings that are not written to the persistent file are lost when the system reboots.

To access the DHCP Snooping Persistent Configuration page, click **System > Services > DHCP Snooping > Persistent Configuration**.



To configure DHCP snooping persistent settings:

1. Specify where to store the persistent binding file:
 - **Local**. The binding table will be stored locally in a file on the switch. Selecting this option disables the **Remote File Name** and **Remote IP Address** fields.
 - **Remote**. The binding table will be stored on the remote TFTP server.
2. If the database is stored in a remote location, specify the IP address of the TFTP server on which the snooping database will be stored.
3. If the database is stored in a remote location, specify the name of the file on the TFTP server that will store the bindings database entries. The name can contain up to 32 alphanumeric characters.
4. In the **Write Delay** field, specify how often to write entries from the local database into the local or remote file. The default value is 300 seconds, and the range is 15 to 86400 seconds.
5. Click **Apply** to apply the change to the system. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Statistics

Use this page to view per-interface DHCP snooping statistics.

To access the DHCP Snooping Statistics page, click **System** > **Services** > **DHCP Snooping** > **Statistics**.

The screenshot shows the Netgear web interface for a GS728TS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar shows the DHCP Snooping configuration tree, with Statistics selected. The main content area displays the DHCP Snooping Statistics page, which includes a table of statistics for various interfaces.

Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs Received
1/g1	0	0	0
1/g2	0	0	0
1/g3	0	0	0
1/g4	0	0	0
1/g5	0	0	0
1/g6	0	0	0
1/g7	0	0	0

At the bottom of the page, there are buttons for CLEAR and REFRESH, and a copyright notice for 1996-2011 NETGEAR.

Use the DHCP Snooping Statistics page to view the DHCP Snooping statistics.

- To view settings for a physical port, click the unit ID of the stack member with the ports to view.
- To view settings for a Link Aggregation Group (LAG), click **LAGS**.
- To view settings for both physical ports and LAGs, click **ALL**.
- View the following DHCP snooping statistics:
 - The **Interface** field shows the untrusted and snooping enabled interface for which statistics to be displayed.
 - The **MAC Verify Failures** field shows the number of packets that were dropped by DHCP Snooping as there is no matching DHCP Snooping binding entry found.
 - The **Client Ifc Mismatch** field shows the number of DHCP messages that are dropped based on source MAC address and client HW address verification.
 - The **DHCP Server Msgs Received** field shows the number of Server messages that are dropped on an untrusted port.
- Click **Clear** to clear all interfaces statistics.
- Click **Refresh** to refresh the data on the screen with the latest statistics.

Timer Schedule (GS728TPS and GS752TPS Only)

Timers control when power can and cannot be delivered to the port. Use the following general steps to add a timer to a port:

1. Create the timer on the Timer Global Configuration page.
2. Configure the timer settings on the Timer Schedule Configuration page.
3. Assign the timer to the port on the PoE Port Configuration page.

Note: The Timer Schedule feature must be enabled for the settings to be applied to the ports.

From the Timer Schedule link under the System tab, you can view and configure Timer Schedule settings for the switch and for the PoE ports.

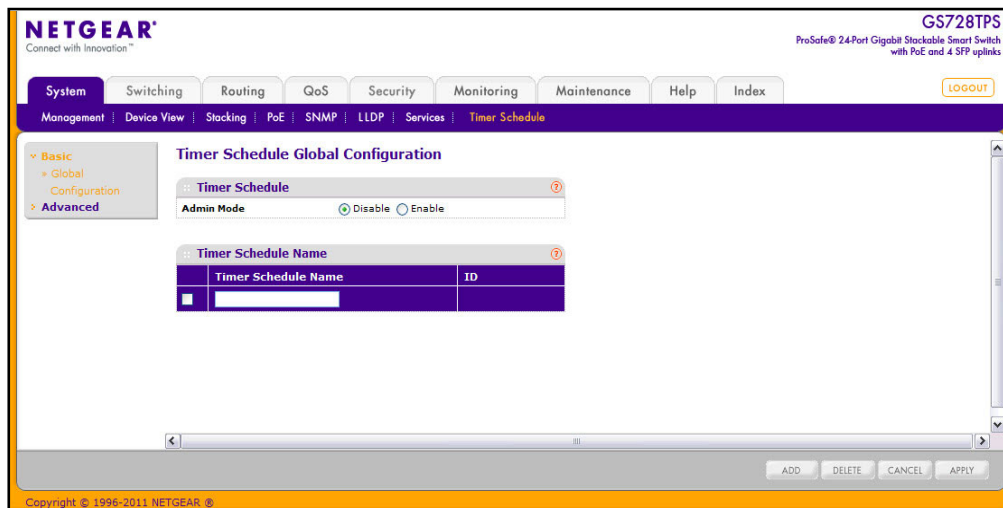
From the Timer Schedule link, you can access the following pages:

- [Timer Global Configuration](#) on page 99
- [Timer Schedule Configuration](#) on page 100

Timer Global Configuration

Use the Timer Global Configuration page to create or remove timers and to control the administrative status of the timer feature.

To display the Timer Global Configuration page, click **System > Timer Global Configuration**.



To configure global timer settings:

1. To add a timer, enter a name in the Timer Schedule Name field, and click **Add**.
2. To remove a timer, select the check box associated with the timer and click **Delete**.
3. To enable or disable the timer feature, select the appropriate radio button and click **Apply**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Timer Schedule Configuration

Use the Timer Schedule Configuration page to configure when the power to a port is turned off. For example, you can specify that the power is turned off every night, during the weekend, or during the same one-week period every year.

To display the Timer Schedule Configuration page, click **System > Timer Schedule > Advanced > Timer Schedule Configuration**.

To configure timer schedules:

1. Select the name of the schedule created on the Timer Global Configuration page.
2. Specify the type of timer to configure:
 - **Absolute**. The timer occurs once.
 - **Periodic**. The timer occurs periodically at regular intervals.

The fields available for the timer schedule configuration depend on the selected timer type.

3. In the Timer Schedule Entry menu, select *new* to configure a new schedule, or select an existing entry to change its settings.
4. Specify the start and end times for the timer in the appropriate fields. The time range is from 00:00 to 23:59.
5. Specify the start and end dates for the timer by clicking the calendar icon and selecting the date. If the timer schedule is periodic, you can specify that there is no end date.

6. If required, use the Recurrence Pattern and Daily Mode fields to customize the power shutdown schedule. These fields are available only if the scheduler type is periodic.
7. Click **Add** to add the new entry to the selected timer schedule.
8. Click **Delete** to remove the selected entry from the timer schedule.
9. Click **Apply** to update the settings for an entry.
10. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Note: Each timer can contain a maximum of one Absolute schedule entry and ten Periodic schedule entries.

Configuring Switching Information

3

Use the features in the Switching tab to define Layer 2 features. The **Switching** tab contains links to the following features:

- [Ports](#) on page 102
- [Link Aggregation Groups](#) on page 105
- [VLANs](#) on page 110
- [Voice VLAN](#) on page 118
- [Auto-VoIP](#) on page 121
- [Spanning Tree Protocol](#) on page 122
- [Multicast](#) on page 135
- [Forwarding Database](#) on page 156

Ports

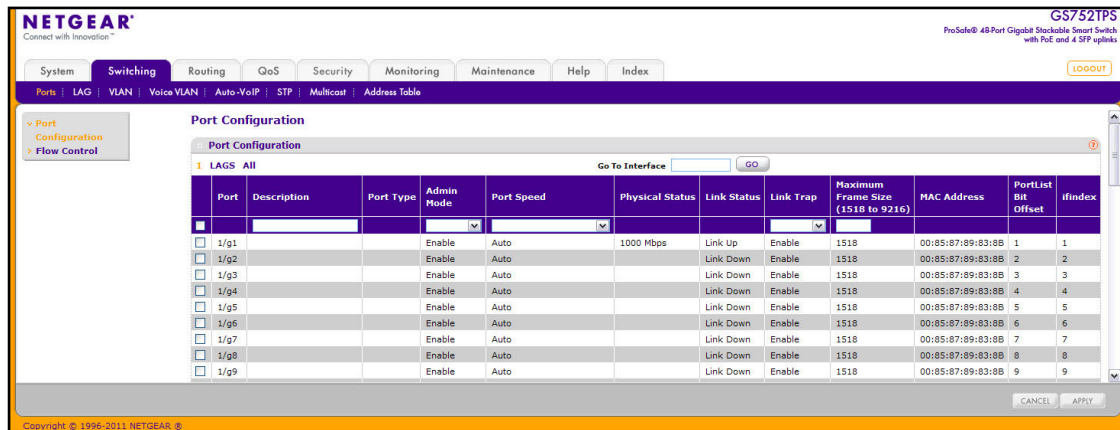
The pages on the Ports tab allow you to view and monitor the physical port information for the ports available on the switch. From the Ports link, you can access the following pages:

- [Port Configuration](#) on page 102
- [Flow Control](#) on page 104

Port Configuration

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

To access the Port Configuration page, click **Switching > Ports > Port Configuration**.



To configure port settings:

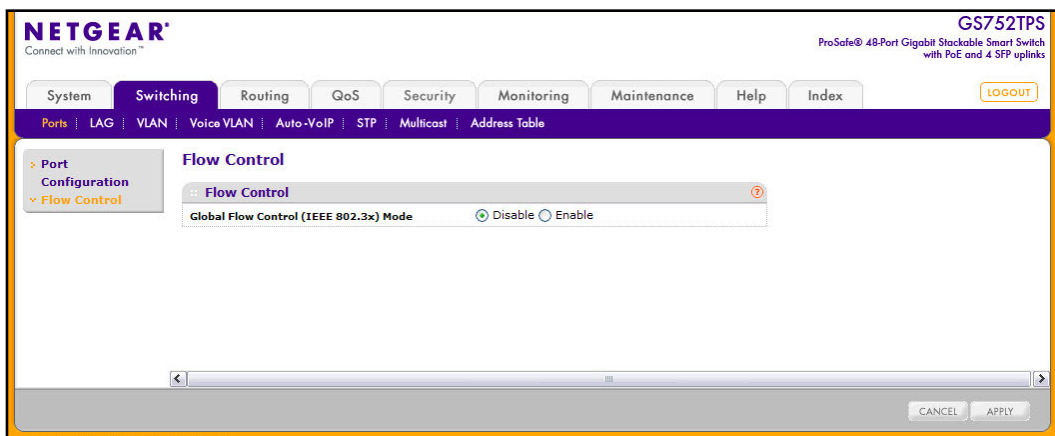
1. To configure settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure settings for both physical ports and LAGs, click **ALL**.
4. Alternatively, to configure settings for a specific interface, enter the interface ID in the **Go To Interface** and click **Go**.
5. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
6. Configure or view the settings:
 - **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:
 - Probe: Indicates that the port is a monitoring (destination) port. For additional information about port monitoring see [Port Mirroring](#) on page 278.
 - Mirrored: The port is a source port and mirrors traffic to the probe port. For additional information about port monitoring see [Port Mirroring](#) on page 278.
 - LAG: Indicates that the port is a member of a Link Aggregation trunk. For more information see [Link Aggregation Groups](#) on page 105.
 - **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. 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 physical port's speed and duplex mode

- **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 Enable.
 - 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.** Specify the maximum Ethernet frame size the interface supports or is configured to support. The frame size includes the Ethernet header, CRC, and payload. (1518–9216). The default maximum frame size is 1518.
 - **MAC Address.** Displays the physical address of the specified interface.
 - **PortList Bit Offset.** Displays 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.
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 changes to the system.

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



To configure global flow control settings:

1. From the Global Flow Control (IEEE 802.3x) Mode field, enable or disable IEEE 802.3x flow control on the system. The factory default is Disable.
 - **Enable.** The switch sends pause packets if the port buffers become full.
 - **Disable.** The switch does not send pause packets if the port buffers become full.
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 the mode, click **Apply** to apply the changes to the system.

Link Aggregation Groups

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. By default, the LAG becomes a member of the management VLAN.

A LAG interface can be either static or dynamic, but not both. Dynamic LAGs use Link Aggregation Control Protocol (LACP) Protocol Data Units (PDUs) to exchange information with their link partners to help maintain the link state. A static port-channel interface does not require a partner system to be able to aggregate its member ports. When a port is added to a LAG as a static member, it neither transmits nor receives LACP PDUs.

The GS728TS, GS728TPS, GS752TS, and GS752TPS Smart Switches each support four LAGs.

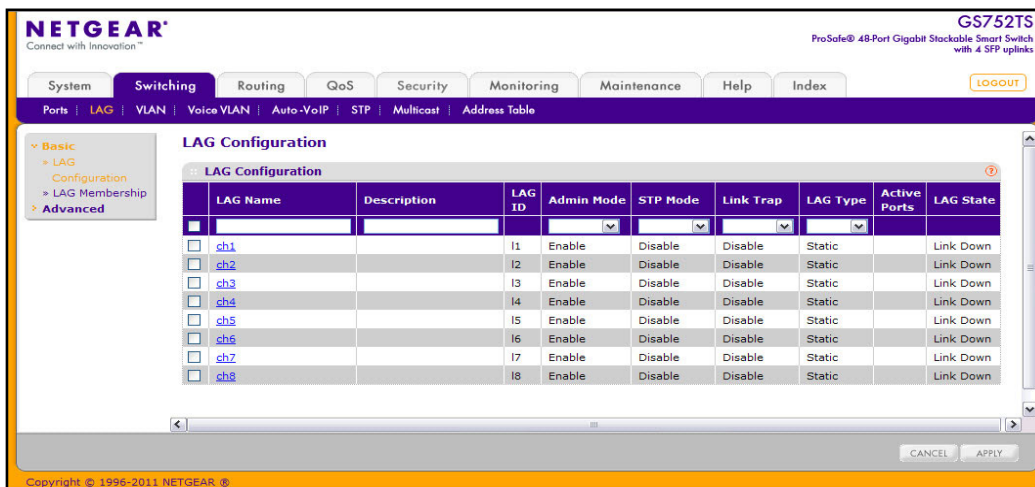
From the LAGs link, you can access the following pages:

- [LAG Configuration](#) on page 105
- [LAG Membership](#) on page 107
- [LACP Configuration](#) on page 108
- [LACP Port Configuration](#) on page 109

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, click **Switching > LAG > Basic > LAG Configuration**.



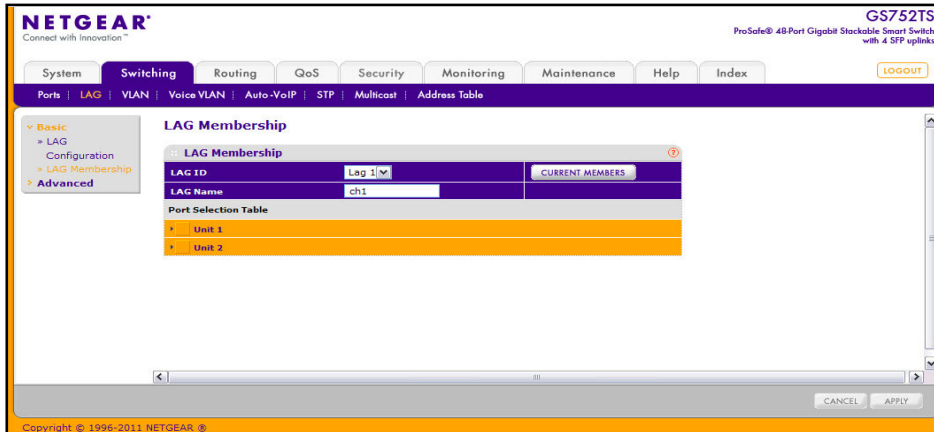
To configure LAG settings:

1. Select the check box next to the LAG to configure. You can select multiple LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
2. Configure or view the following settings:
 - **LAG Name.** Specify the name to assign to the LAG. You may enter any string of up to 15 alphanumeric characters.
 - **Description.** Specify the Description string to be attached to a LAG. It can be up to 64 characters in length.
 - **LAG ID.** Displays the number assigned to the LAG. This field is read-only.
 - **Admin Mode.** Select Enable or Disable from the menu. When the LAG (port channel) is disabled, no traffic will flow and LACP PDUs will be dropped, but the links that form the LAG (port channel) will not be released. The factory default is Enable.
 - **STP Mode.** Select the Spanning Tree Protocol Administrative Mode associated with the LAG.
 - **Link Trap.** Specify whether you want to have a trap sent when link status changes. The factory default is Disable, which will cause the trap to be sent.
 - **LAG Type.** Select Static or LACP. When the LAG is static, it does not transmit or process received LACP PDUs. The member ports do not transmit LACP PDUs, and all the LACP PDUs 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.
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.

LAG Membership

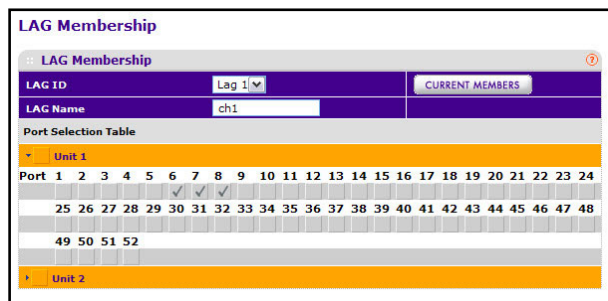
Use the LAG Membership page to select two or more full-duplex Ethernet links to be aggregated together to form a link aggregation group (LAG), which is also known as a port-channel. The switch can treat the port-channel as if it were a single link.

To access the LAG Membership page, click **Switching > LAG > Basic > LAG Membership**.



To create a LAG:

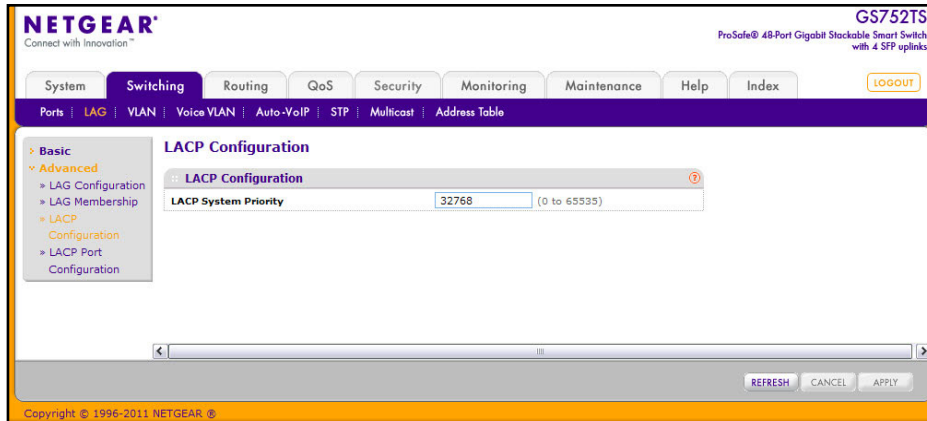
1. From the **LAG ID** field, select the LAG to configure.
2. In the **LAG Name** field, enter the name to assign the LAG. You may enter any string of up to 15 alphanumeric characters.
3. Click the orange bar to display the ports.
4. Click the box below each port to include in the LAG. The following figure shows an example of how to configure LAG1 with ports 6, 7 and 8 on Unit 1 as members.



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 this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. To view the ports that are members of the selected LAG, click **Current Members**.

LACP Configuration

To display the LACP Configuration page, click **Switching** > **LAG** > **Advanced** > **LACP Configuration**.

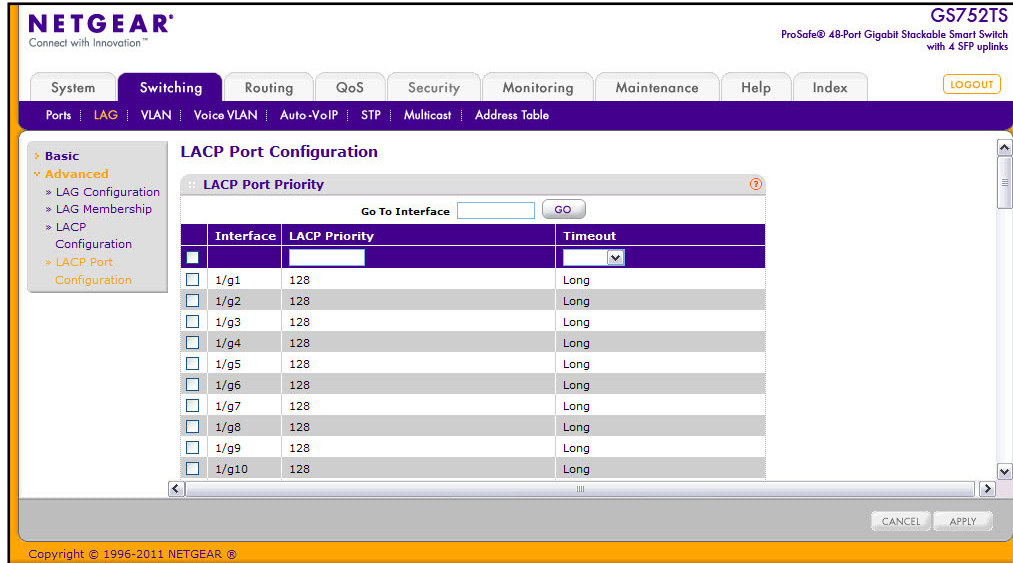


To configure LACP:

1. From the LACP System Priority field, specify 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 0–65535. 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, click **Switching** > **LAG** > **Advanced** > **LACP Port Configuration**.



To configure LACP port priority settings:

1. Select the check box next to the port to configure. You can select multiple ports to apply the same setting to all selected ports.

Note: You cannot select ports that are not participating in a LAG.

2. Configure the **LACP Priority** value for the selected port. The field range is 0–255. The default value is 128.
3. Configure the administrative LACP **Timeout** value.
 - **Long.** Specifies a long timeout value.
 - **Short.** Specifies a short timeout value.
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.

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.

By default, all ports on the switch are in the same broadcast domain. VLANs electronically separate ports on the same switch into separate broadcast domains so that broadcast packets are not sent to all the ports on a single switch. When you use a VLAN, users can be grouped by logical function instead of physical location.

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.

From the VLAN link, you can access the following pages:

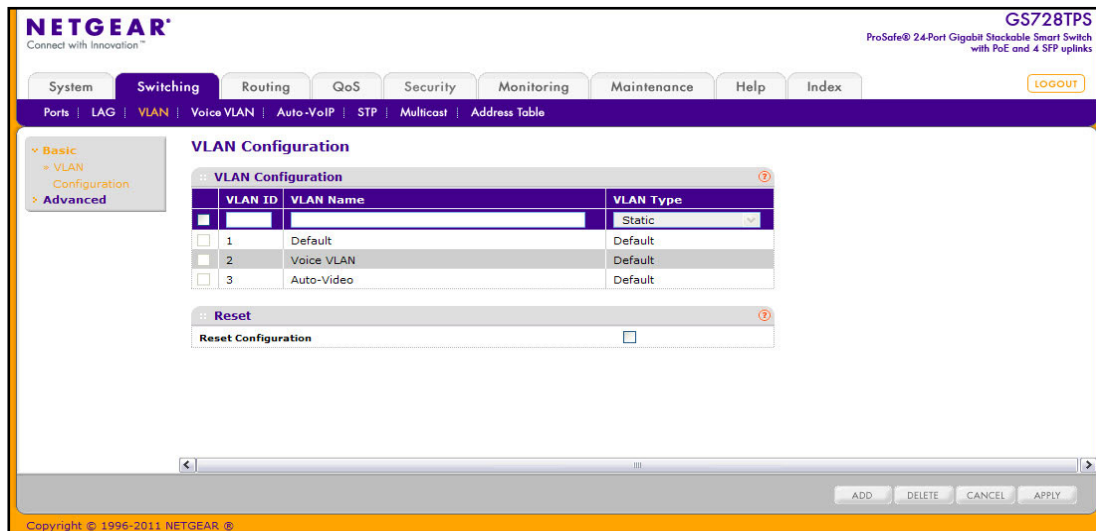
- [VLAN Configuration](#) on page 110
- [VLAN Membership Configuration](#) on page 112
- [Port VLAN ID Configuration](#) on page 113
- [MAC Based VLAN](#) on page 114
- [Protocol Based VLAN Group Configuration](#) on page 115
- [Protocol Based VLAN Group Membership](#) on page 116

VLAN Configuration

Use the VLAN Configuration page to define VLAN groups stored in the VLAN membership table. The GS728TS, GS728TPS, GS752TS, and GS752TPS each support up to 256 VLANs. Three VLANs are created by default:

- VLAN 1 is the default VLAN of which all ports are members.
- VLAN 2 is for voice traffic.
- VLAN 3 is for Auto-Video traffic.

To display the VLAN Configuration page, lick **Switching > VLAN > Basic > VLAN Configuration**.



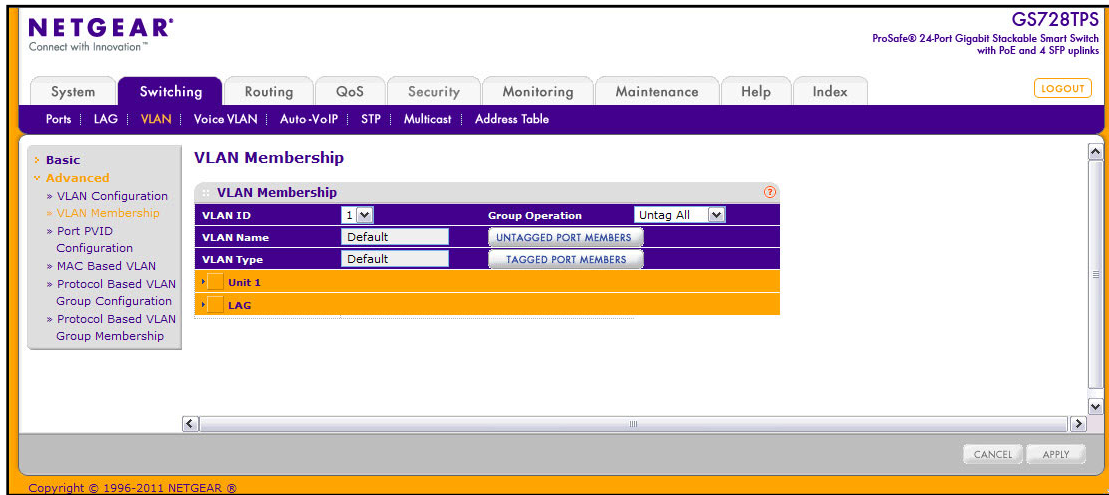
To configure VLANs:

- To add a VLAN, configure the VLAN ID, name, and type, and then click **Add**.
 - 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 1–4093.
 - 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) because the type is always Default. When you create a VLAN on this page, its type will always be Static.
- To delete a VLAN, select the check box next to the VLAN ID and click **Delete**. You cannot delete the default VLAN.
- To modify settings for a VLAN, select the check box next to the VLAN ID, change the desired information, and then click **Apply**. Configuration changes occur immediately.
- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
- To reset the VLAN settings on the switch to the factory defaults, select the **Reset Configuration** check box, and click OK in the popup message to confirm. If the Management VLAN is set to a non-default VLAN (VLAN 1), it is automatically set to 1 after a Reset Configuration.

VLAN Membership Configuration

Use this page to configure VLAN Port Membership for a particular VLAN. You can select the Group operation through this page.

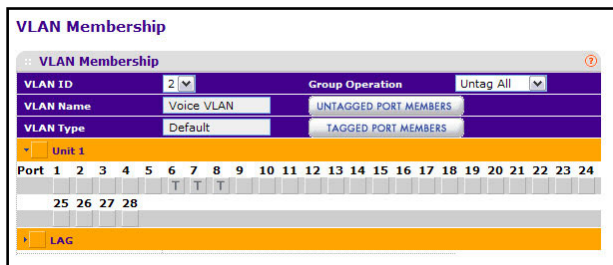
To display the VLAN Membership Configuration page, click **Switching > VLAN > Advanced > VLAN Membership**.



To configure VLAN membership:

1. From the VLAN ID field, select the VLAN to which you want to add ports.
2. Click the orange bar below the VLAN Type field to display the physical ports on the switch.
3. Click the lower orange bar to display the LAGs on the switch.
4. To select the port(s) or LAG(s) to add to the VLAN, click the square below each port or LAG. You can add each interface as a tagged (T) or untagged (U) VLAN member.
 - **Tagged:** Frames transmitted from this port are tagged with the port VLAN ID.
 - **Untagged:** Frames transmitted from this port are untagged. Each port can be an untagged member of only one VLAN. By default, all ports are an untagged member of VLAN 1.

In the following figure, ports g6, g7, and g8 are being added as tagged members to VLAN 2.



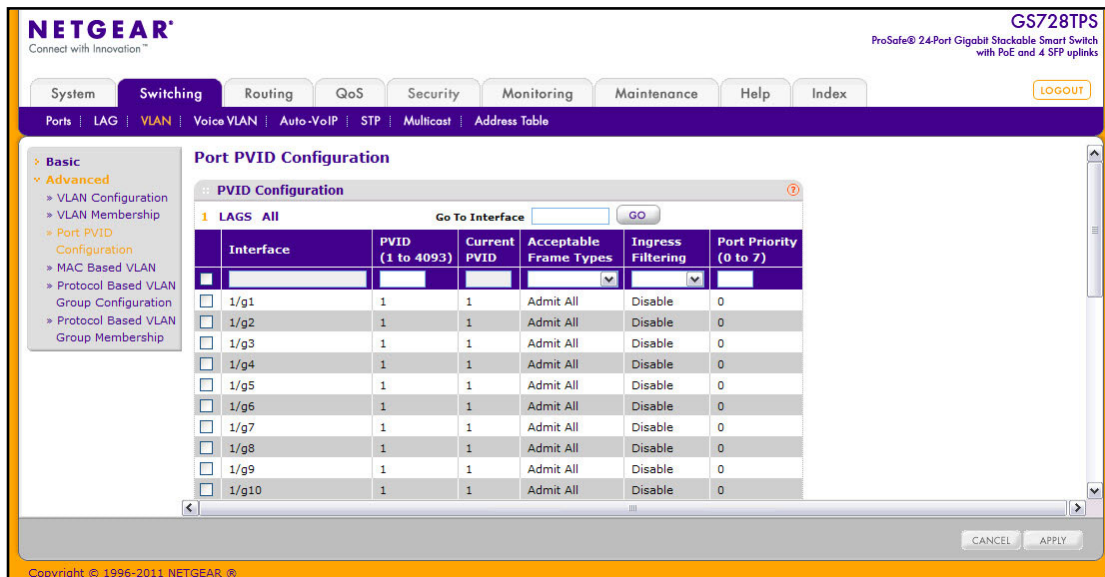
5. Use the **Group Operations** field to select all the ports and configure them. Possible values are:
 - **Untag All:** Select all the ports on which all frames transmitted from this VLAN will be untagged. All the ports will be included in the VLAN.
 - **Tag All:** Select the ports on which all frames 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.
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 any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

Port VLAN ID Configuration

The Port PVID Configuration screen lets you assign a port VLAN ID (PVID) to an interface. PVIDs have the following requirements:

- All ports must have a defined PVID.
- If no other value is specified, the default VLAN PVID is used.

To access the Port PVID Configuration page, click **Switching > VLAN > Advanced > Port PVID Configuration**.



To configure PVID information:

1. To configure PVID settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure PVID settings for a Link Aggregation Group (LAG), click **LAGS**.

3. To configure PVID settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the interfaces to configure. You can select multiple interfaces to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Configure the PVID to assign to untagged or priority tagged frames received on this port. The Current PVID field displays the PVID currently configured for the interface.
6. In the **Acceptable Frame Type** field, 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 accept only VLAN-tagged frames and 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.
7. In the **Ingress Filtering** field, 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.
8. Specify the default 802.1p priority assigned to untagged packets arriving at the port. Possible values are 0–7.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

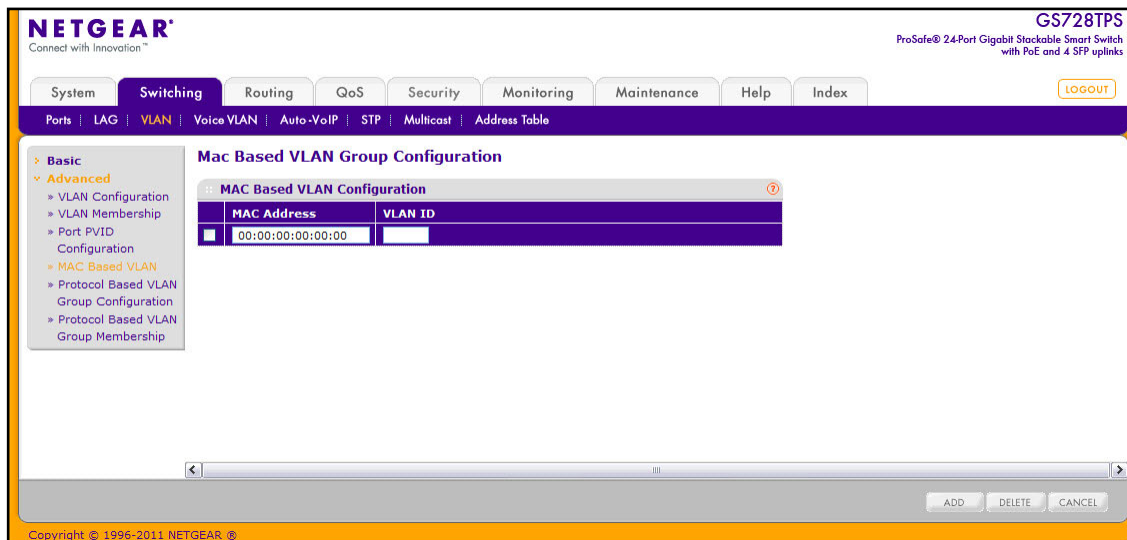
MAC Based VLAN

The MAC Based VLAN feature allows incoming untagged frames to be assigned to a VLAN and to classify traffic based on the source MAC address of the frame.

A MAC-to-VLAN mapping is defined by configuring an entry in the MAC to VLAN table. An entry is specified via a source MAC address and the desired VLAN ID. The MAC to VLAN configurations are shared across all ports of the device (i.e. there is a system wide table that has MAC address to VLAN ID mappings).

When untagged or priority tagged packets arrive at the switch and entries exist in the MAC to VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged it will maintain this value; otherwise the priority will be set to zero. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped. You can configure a MAC address mapping to a VLAN that has not been created on the system.

To access the MAC Based VLAN page, click **Switching > VLAN > Advanced > MAC Based VLAN**.



To configure a MAC-based VLAN:

1. In the **MAC Address** field, specify the valid MAC Address to be bound to a VLAN ID. This field is configurable only when a MAC Based VLAN is created. Select this entry.
2. The **VLAN ID** field shows the VLAN ID. A valid ID can be any number in the range of (1–4093).
3. To add the entry to the MAC address-to-VLAN mapping table, click **Add**.
4. To remove an entry from the table, select the check box associated with the entry to remove and 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.

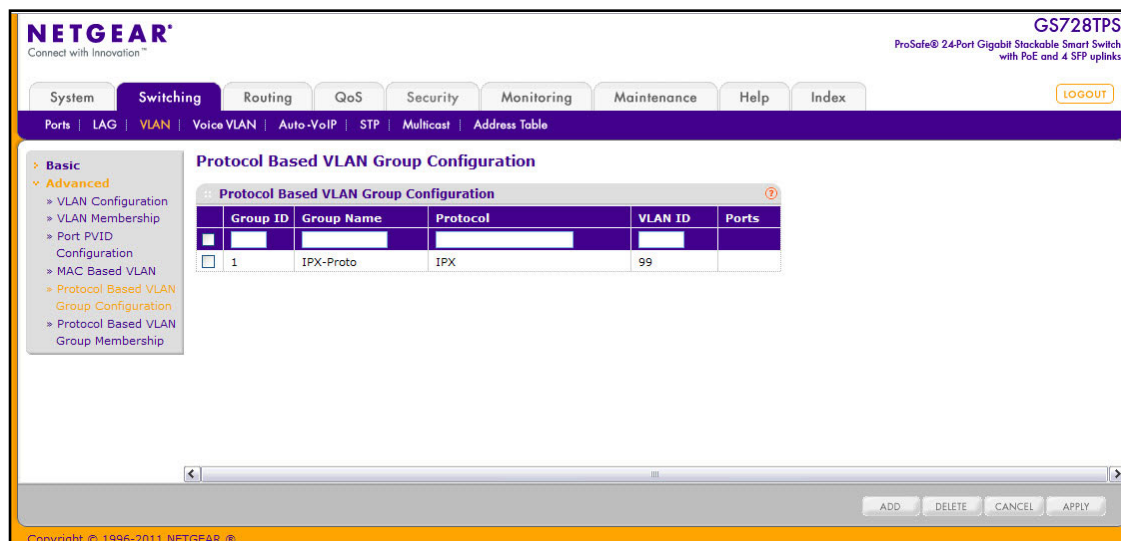
Protocol Based VLAN Group Configuration

Use the protocol-based VLAN feature to define filtering criteria for untagged packets of a specific protocol type. By default, if you do not configure any port- (IEEE 802.1Q) or protocol based VLANs, untagged packets will be assigned to VLAN 1. You can override this behavior by defining either port-based VLANs or protocol based VLANs, or both. Tagged packets are always handled according to the IEEE 802.1Q standard, and are not included in protocol based VLANs.

If you assign a port to a protocol based VLAN for a specific protocol, untagged frames received on that port for that protocol will be assigned the protocol-based VLAN ID you configure. Untagged frames received on the port for other protocols will be assigned the Port VLAN ID which is either the default PVID (1) or a PVID you have specifically assigned to the port using the Port VLAN Configuration screen.

You define a protocol-based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one to 16 protocol definitions, and can include multiple ports.

To access the Protocol Based VLAN page, click **Switching** > **VLAN** > **Advanced** > **Protocol Based VLAN Group Configuration**.



To configure a Protocol Based VLAN Group:

1. Enter a number used to identify the group created by the user. Group IDs should be assigned when a group is created by the user. The Group IDs range is 1–128.
2. Assign a name to a new group in the **Group Name** field. You may enter up to 16 characters.
3. Populate the **Protocol(s)** field - Protocol-list can be any valid comma(,) separated string with standard “arp”, “ip”, “ipx” keywords, hexadecimal, or decimal values in the range of 0x0600(1536) to 0xFFFF(65535).
4. Enter any number in the range of (1 to 4093) **VLAN ID** field. All the ports in the group will assign this VLAN ID to untagged packets received for the protocols you included in this group.

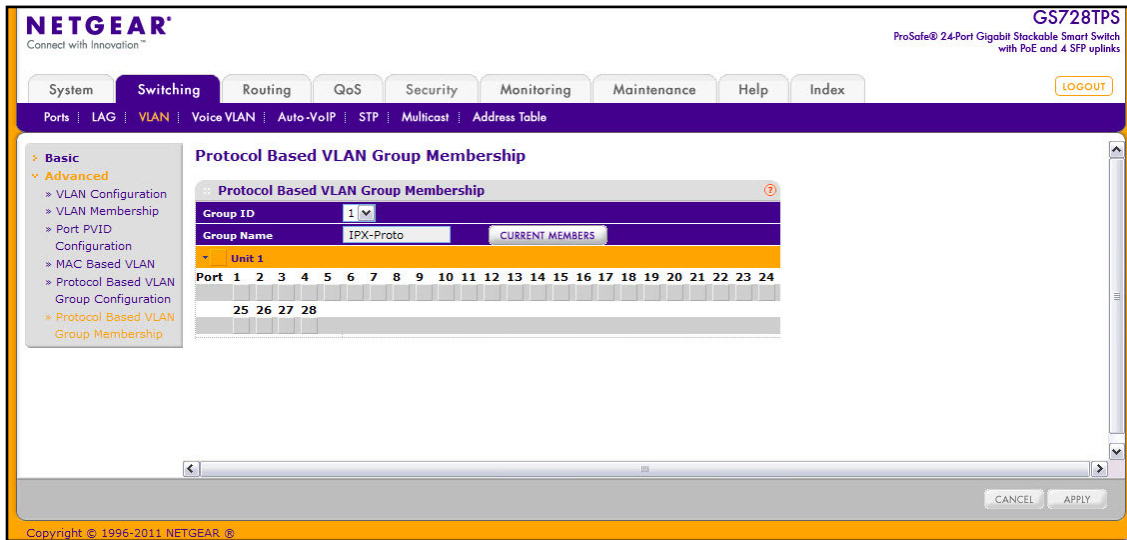
The **Ports** field displays all the member ports which belong to the group.

5. To add an entry of MAC Address to VLAN mapping, click **Add**.
6. To remove the Protocol Based VLAN group identified by the value in the **Group ID** field, click **Delete**.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

Protocol Based VLAN Group Membership

To access the MAC Based VLAN page, click **Switching** > **VLAN** > **Advanced** > **Protocol Based VLAN Group Membership**. In the following image, the port list has been expanded to display the available ports on the system.



To set up Protocol Based VLAN Group Membership:

1. Select the protocol-based VLAN Group ID for which you want to display or configure data in the **Group ID** drop-down menu.

The **Group Name** field identifies the name for the protocol-based VLAN you selected.

2. Click the orange bar to display the ports for a specific switch unit and click the box below a port number to add it to the protocol-based VLAN group.

Note that each interface can belong to only one group for a given protocol. For example, if you have already added a port to a group for IP, you cannot add it to another group that also includes IP, although you could add it to a new group for IPX.

3. Click the **Current Members** button view the current numbers in the selected protocol based VLAN Group.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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

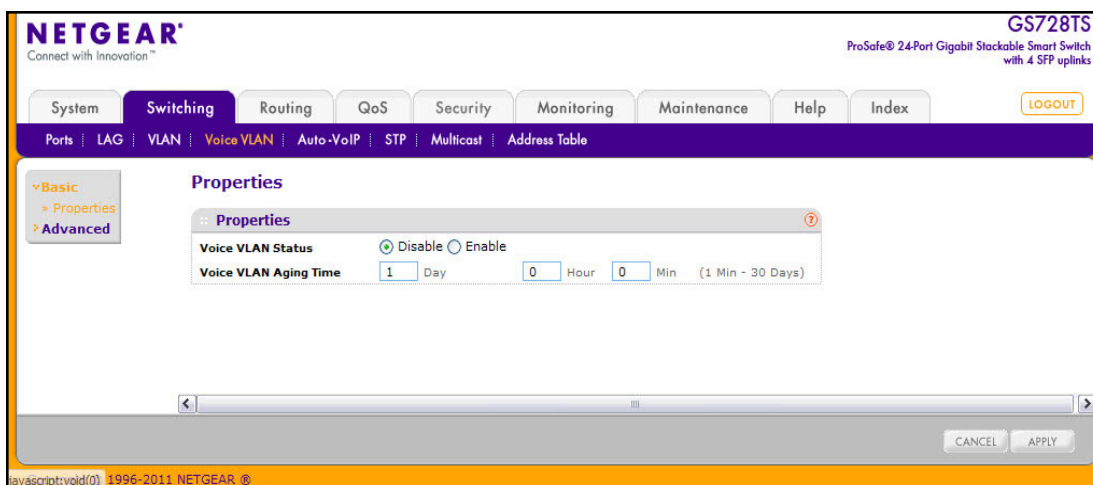
Configure the Voice VLAN settings for ports that carry traffic from IP phones. The Voice VLAN feature can help ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high.

From the VLAN link, you can access the following pages:

- [Voice VLAN Properties](#) on page 118
- [Voice VLAN Port Setting](#) on page 119
- [Voice VLAN OUI](#) on page 120

Voice VLAN Properties

To display the Voice VLAN Properties page, click **Switching** > **Voice VLAN** > **Basic** > **Properties**.

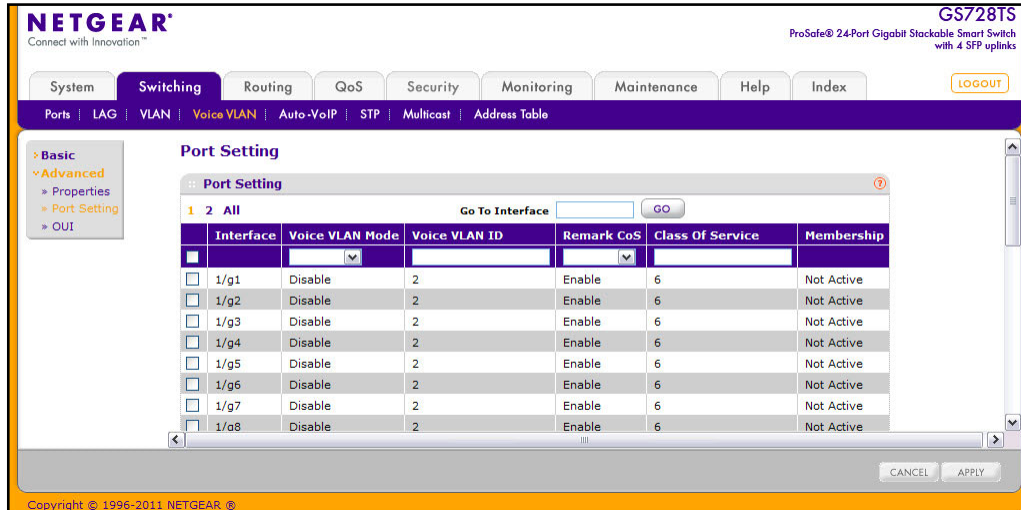


To configure Voice VLAN:

1. From the **Voice VLAN Status** field, enable or disable Voice VLAN on the switch. If the switch does not handle traffic from IP phones, the status should be disabled.
2. From the **Voice VLAN Aging Time** field, specify 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.
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.

Voice VLAN Port Setting

To display the Voice VLAN Port Setting page, click **Switching** > **Voice VLAN** > **Advanced** > **Port Setting**.



To configure Voice VLAN port settings:

1. Select the check box next to the port to configure. You can select multiple check boxes to apply the same setting to all selected ports.
2. From the Voice VLAN Mode menu, specify whether to enable or disable Voice VLAN on the selected port.
3. From the **Voice VLAN ID** menu, set the Voice VLAN ID to be used for voice traffic. The default value is 2.
4. From the **Remark CoS** menu, specify whether to enable or disable class of service remarks on the selected port.
5. From the **Class of Service** column, the CoS tag value to be reassigned for packets received on the voice VLAN when Remark CoS is displayed when this feature is enabled.
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 any changes to this page, click **Apply** to send the updated configuration to the switch.

Note: The **Membership** field displays whether a registered voice device (OUI or LLDP-MED) is currently active or not active on the interface.

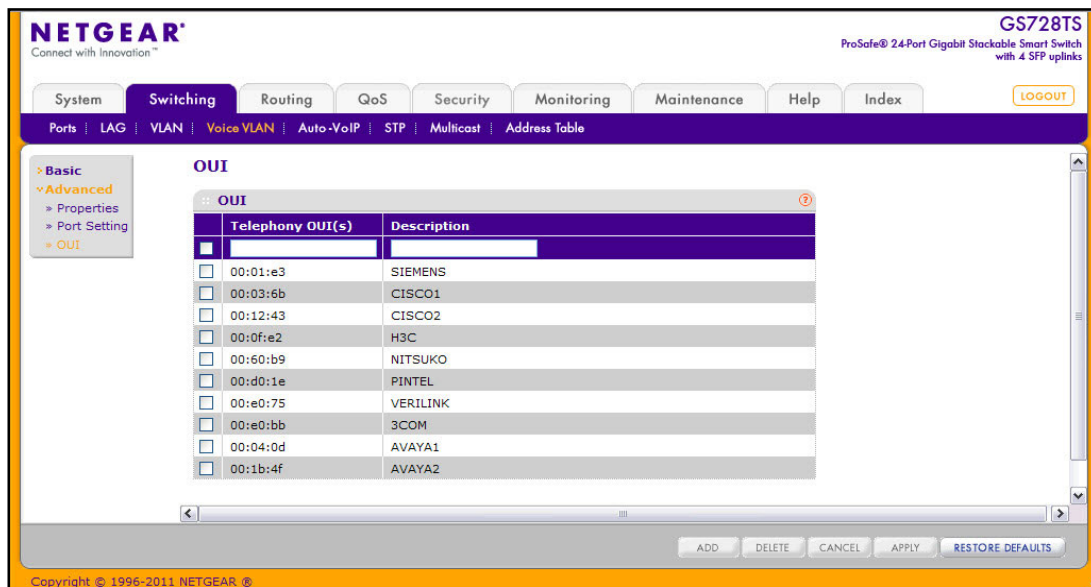
Voice VLAN OUI

The Organizational Unique Identifier (OUI) identifies the IP phone manufacturer. The switch comes preconfigured with the following OUIs:

- 00:01:E3: SIEMENS
- 00:03:6B: CISCO1
- 00:12:43: CISCO2
- 00:0F:E2: H3C
- 00:60:B9: NITSUKO
- 00:D0:1E: PINTEL
- 00:E0:75: VERILINK
- 00:E0:BB: 3COM
- 00:04:0D: AVAYA1
- 00:1B:4F: AVAYA2

You can select an existing OUI or add a new OUI and description to identify the IP phones on the network.

To display the Voice VLAN OUI page, click **Switching** > **Voice VLAN** > **Advanced** > **OUI**.



To configure OUI settings:

1. To add a new OUI prefix, type the VOIP OUI prefix in the **Telephony OUI(s)** field, provide a description of the prefix, and click **Add**. The OUI prefix must be in the format AA:BB:CC.
2. To delete an OUI prefix from the list, select the check box next to the OUI prefix and click **Delete**.

3. To modify information for an entry in the OUI list, select the check box next to the OUI prefix, update the OUI prefix or description, and then click **Apply**.
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 **Restore Defaults** to restore the list to the preconfigured OUIs.

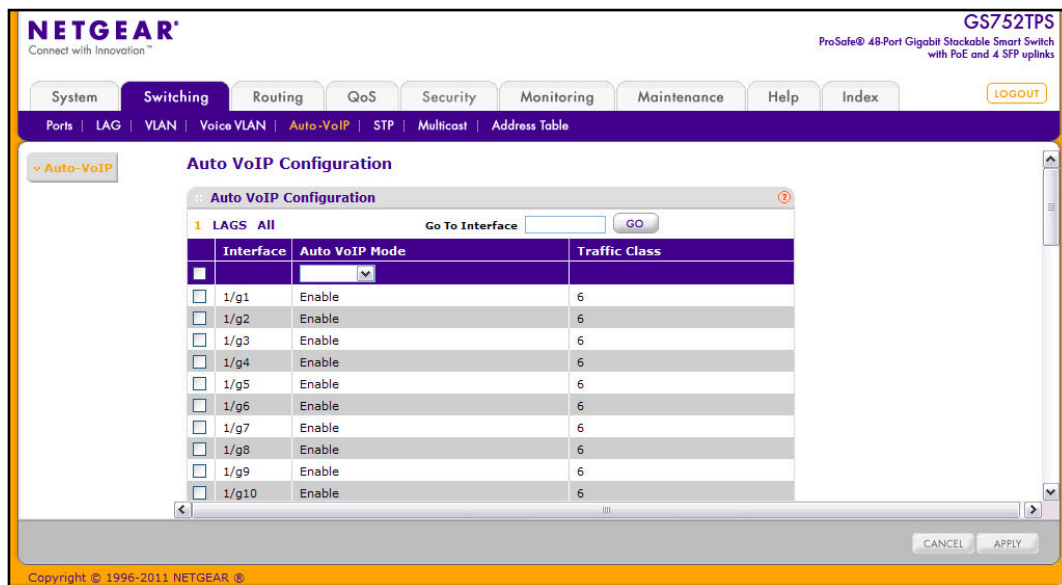
Auto-VoIP

The Auto-VoIP automatically makes sure that time-sensitive voice traffic is given priority over data traffic on ports that have this feature enabled. Auto-VoIP checks for packets carrying the following VoIP protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)
- Media Gateway Control Protocol (MGCP)

VoIP frames that are received on ports that have the Auto-VoIP feature enabled are marked with CoS traffic class 6.

To display the Auto-VoIP page, click **Switching > Auto-VoIP**.



To configure Auto-VoIP settings:

1. To configure Auto-VoIP settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure Auto-VoIP settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure Auto-VoIP settings for both physical ports and LAGs, click **ALL**.

4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. From the Auto-VoIP Mode menu, specify whether to enable or disable Auto-VoIP on the selected port(s) or LAG(s).
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 any changes to this page, click **Apply** to send the updated configuration to the switch.

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 126.

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 additional information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

From the STP link, you can access the following pages:

- [STP Switch Configuration](#) on page 123
- [CST Configuration](#) on page 125
- [CST Port Configuration](#) on page 126
- [CST Port Status](#) on page 128
- [Rapid STP](#) on page 129

- [MST Configuration](#) on page 130
- [MST Port Configuration](#) on page 131
- [STP Statistics](#) on page 134

STP Switch Configuration

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

To display the Spanning Tree Switch Configuration/Status page, click **Switching > STP > Basic > STP Configuration**.

NETGEAR
Connect with Innovation™

GS752TS
ProSafe® 48-Port Gigabit Stackable Smart Switch with 4 SFP uplinks

System | **Switching** | Routing | QoS | Security | Monitoring | Maintenance | Help | Index | LOGOUT

Ports | LAG | VLAN | Voice VLAN | Auto-VoIP | **STP** | Multicast | Address Table

Basic > STP > Configuration > Advanced

STP Configuration

Global Settings

Spanning Tree State: Disable Enable

STP Operation Mode: STP RSTP MSTP

Configuration Name: 00-85-87-89-83-86

Configuration Revision Level: 0 (0 to 65535)

Configuration Digest Key: 0xac36177f50283cd4b83821d8ab26de62

Forward BPDUs while STP Disabled: Disable Enable

STP Status

Bridge Identifier	80:00:00:85:87:89:83:86
Time Since Topology Change	1 day 8 hr 16 min 28 sec
Topology Change Count	0
Topology Change	False
Designated Root	80:00:00:85:87:89:83:86
Root Path Cost	0
Root Port	00:00
Max Age (secs)	20
Forward Delay (secs)	15
Hold Time (secs)	6
CST Regional Root	80:00:00:85:87:89:83:86
CST Path Cost	0

REFRESH CANCEL APPLY

Copyright © 1996-2011 NETGEAR, Inc.

To configure STP settings on the switch:

1. From the **Spanning Tree State** field, specify whether to enable or disable Spanning Tree operation on the switch.
2. From the **STP Operation Mode** field, 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

3. Specify the configuration name and revision level.
 - **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.
4. Specify the BPDU Flooding status for all ports or for individual ports. When this feature is enabled, BPDU packets arriving at this port are flooded to other ports if STP is disabled.
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 configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes occur immediately.

The following table describes the STP Status information displayed on the screen.

Field	Description
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. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Path cost to the Designated Root for the CST.
Root Port	Port to access the Designated Root for the CST.
Max Age (secs)	Specifies the bridge maximum age for CST. The value must be less than or equal to (2 X Bridge Forward Delay) – 1 and greater than or equal to 2 X (Bridge Hello Time +1).
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.

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

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, click **Switching > STP > Advanced > CST Configuration**.

The screenshot shows the NETGEAR web interface for a GS752TS switch. The main configuration area is titled "CST Configuration" and contains the following fields:

- Bridge Priority:** 32768 (range: 0 to 61440)
- Bridge Max Age (secs):** 20 (range: 6 to 40)
- Bridge Hello Time (secs):** 2
- Bridge Forward Delay (secs):** 15 (range: 4 to 30)
- Spanning Tree Maximum Hops:** 20 (range: 1 to 127)

Below the configuration fields is an "MSTP Status" table:

MST ID	VID	FID
0	1	1
0	2	2
0	3	3
0	99	99

At the bottom of the configuration area are buttons for "REFRESH", "CANCEL", and "APPLY".

To configure CST settings:

1. Specify values for CST in the appropriate fields:

- **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 $(2 * \text{Bridge Forward Delay}) - 1$ and greater than or equal to $2 * (\text{Bridge Hello Time} + 1)$. 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 value is fixed at 2 seconds.
- **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 $(\text{Bridge Max Age} / 2) + 1$. 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.
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 send the updated configuration to the switch. Configuration changes take place immediately.

The following table describes the MSTP status information displayed on the Spanning Tree CST Configuration page.

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.

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

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, click **Switching > STP > Advanced > CST Port Configuration**.

The screenshot shows the Netgear web interface for a GS752TS switch. The main content area is titled "CST Port Configuration" and contains a "Port Configuration" table. The table has the following columns: Interface, STP Status, Fast Link, BPDU Forwarding, Port State, Path Cost, Priority, External Port Path Cost, Port ID, and Hello Timer. The table lists 10 interfaces (1/g1 to 1/g10). For each interface, the STP Status is "Disable", Fast Link is "Disable", BPDU Forwarding is "Disable", and Port State is "Disabled". The Path Cost is 0, Priority is 128, and External Port Path Cost is 0. The Port ID and Hello Timer values are also listed for each interface.

Interface	STP Status	Fast Link	BPDU Forwarding	Port State	Path Cost	Priority	External Port Path Cost	Port ID	Hello Timer
1/g1	Disable	Disable	Disable	Manual forwarding	0	128	0	80:01	2
1/g2	Disable	Disable	Disable	Disabled	0	128	0	80:02	2
1/g3	Disable	Disable	Disable	Disabled	0	128	0	80:03	2
1/g4	Disable	Disable	Disable	Disabled	0	128	0	80:04	2
1/g5	Disable	Disable	Disable	Disabled	0	128	0	80:05	2
1/g6	Disable	Disable	Disable	Disabled	0	128	0	80:06	2
1/g7	Disable	Disable	Disable	Disabled	0	128	0	80:07	2
1/g8	Disable	Disable	Disable	Disabled	0	128	0	80:08	2
1/g9	Disable	Disable	Disable	Disabled	0	128	0	80:09	2
1/g10	Disable	Disable	Disable	Disabled	0	128	0	80:0a	2

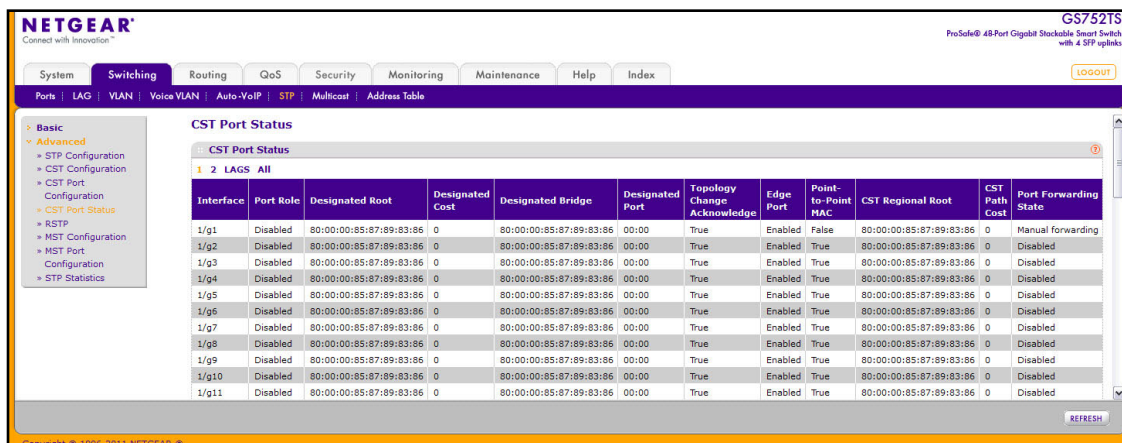
To configure CST port settings:

1. To configure CST settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure CST settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure CST settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Configure the CST values for the selected port(s) or LAG(s):
 - **STP Status.** Enable or disable the Spanning Tree Protocol Administrative Mode associated with the port or port channel.
 - **Fast Link.** Specifies if the specified port is an Edge Port with the CST. Possible values are Enable or Disable. The default is Disable.
 - **BPDU Forwarding.** When enabled, BPDU forwarding forward the BPDU traffic arriving on this port when STP is disabled on the port.
 - **Port State.** The Forwarding state of this port. This field is read-only.
 - **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 1–200000000.
 - **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 1–200000000.
 - **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 value is fixed at 2 seconds.
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 any configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.
8. Click **Refresh** to update the information on the screen with the most current data.

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, click **Switching > STP > Advanced > CST Port Status**.



The following table describes the CST Status information displayed on the screen.

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 <i>True</i> or <i>False</i> .
Edge Port	Indicates whether the port is enabled as an edge port. Possible values are Enabled or Disabled .
Point-to-point MAC	Derived value indicating whether the port is part of a point-to-point link.

Field	Description
CST Regional Root	Displays the bridge priority and base MAC address of the CST Regional Root.
CST Path Cost	Displays the path Cost to the CST tree Regional Root.
Port Forwarding State	Displays the Forwarding State of this port.

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

Rapid STP

Use the Rapid STP page to view information about Rapid Spanning Tree (RSTP) port status.

To display the Rapid STP page, click **Switching > STP > Advanced > RSTP**.

The screenshot shows the Netgear web interface for a GS752TS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under Switching, there are sub-menus for Ports, LAG, VLAN, Voice VLAN, Auto-VoIP, STP, Multicast, and Address Table. The STP menu is expanded to show Basic, Advanced, and RSTP. The RSTP page displays a table titled 'Rapid STP' with the following data:

Interface	Role	Mode	Fast Link	Status
1/g1	Disabled	MSTP	Disabled	Manual forwarding
1/g2	Disabled	MSTP	Disabled	Disabled
1/g3	Disabled	MSTP	Disabled	Disabled
1/g4	Disabled	MSTP	Disabled	Disabled
1/g5	Disabled	MSTP	Disabled	Disabled
1/g6	Disabled	MSTP	Disabled	Disabled
1/g7	Disabled	MSTP	Disabled	Disabled
1/g8	Disabled	MSTP	Disabled	Disabled
1/g9	Disabled	MSTP	Disabled	Disabled
1/g10	Disabled	MSTP	Disabled	Disabled

The following table describes the Rapid STP Status information displayed on the screen.

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 , and MSTP .
Fast Link	Indicates whether the port is enabled as an edge port.
Status	The Forwarding State of this port.

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, click **Switching > STP > Advanced > MST Configuration**.

The screenshot shows the Netgear web interface for a GS752TS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Switching menu is expanded to show Ports, LAG, VLAN, Voice VLAN, Auto-VoIP, STP, Multicast, and Address Table. The STP menu is further expanded to show Basic, Advanced, STP Configuration, CST Configuration, CST Port Configuration, CST Port Status, RSTP, MST Configuration, MST Port Configuration, and STP Statistics. The MST Configuration page displays a table with the following data:

MST ID	Priority	Vlan Id	Bridge Identifier	Time Since Topology Change	Topology Change Count	Topology Change	Designated Root	Root Path Cost	Root Port	
<input type="checkbox"/>	0	32768	1-3,99	80:00:00:85:87:89:83:86	1 day 8 hr 25 min 15 sec	0	False	80:00:00:85:87:89:83:86	0	00:00

Buttons for ADD, DELETE, CANCEL, and APPLY are located at the bottom right of the table.

To configure an MST instance:

- To add an MST instance, configure the MST values and click **Add**:
 - MST ID**. Specify the ID of the MST to create. 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**. The menu contains all VLANs configured on the switch. Select a VLAN to associate with the MST instance.
- To delete an MST instance, select the check box next to the instance and click **Delete**.
- To modify an MST instance, select the check box next to the instance to configure, update the values, and click **Apply**. You can select multiple check boxes to apply the same setting to all selected ports.
- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

For each configured instance, the information described in the following table displays on the page.

Field	Description
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.
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.

MST Port Configuration

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

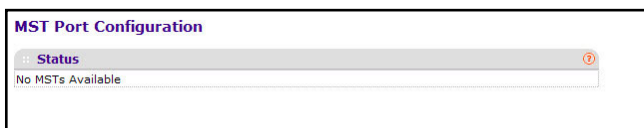
To display the Spanning Tree MST Port Status page, click **Switching > STP > Advanced > MST Port Configuration**. The following figures show the left and right portions of the Web page.

The screenshot shows the NETGEAR web interface for MST Port Configuration. The main content area displays a table with the following columns: Interface, Port Priority, Port Path Cost, Auto Calculated Port Path Cost, Port ID, Port Up Time Since Counters Last Cleared, and Port Mode. The table lists configurations for interfaces 1/g1 through 1/g10.

Interface	Port Priority	Port Path Cost	Auto Calculated Port Path Cost	Port ID	Port Up Time Since Counters Last Cleared	Port Mode
<input type="checkbox"/> 1/g1	128	0	Enabled	80:01	0 day 0 hr 0 min 10 sec	Disable
<input type="checkbox"/> 1/g2	128	0	Enabled	80:02	0 day 0 hr 0 min 10 sec	Disable
<input type="checkbox"/> 1/g3	128	0	Enabled	80:03	0 day 0 hr 0 min 10 sec	Disable
<input type="checkbox"/> 1/g4	128	0	Enabled	80:04	0 day 0 hr 0 min 10 sec	Disable
<input type="checkbox"/> 1/g5	128	0	Enabled	80:05	0 day 0 hr 0 min 10 sec	Disable
<input type="checkbox"/> 1/g6	128	0	Enabled	80:06	0 day 0 hr 0 min 10 sec	Disable
<input type="checkbox"/> 1/g7	128	0	Enabled	80:07	0 day 0 hr 0 min 10 sec	Disable
<input type="checkbox"/> 1/g8	128	0	Enabled	80:08	0 day 0 hr 0 min 10 sec	Disable
<input type="checkbox"/> 1/g9	128	0	Enabled	80:09	0 day 0 hr 0 min 10 sec	Disable
<input type="checkbox"/> 1/g10	128	0	Enabled	80:0a	0 day 0 hr 0 min 10 sec	Disable

Port Forwarding State	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00
Disabled	Disabled	80:01:00:85:87:89:83:86	0	80:01:00:85:87:89:83:86	00:00

Note: If no MST instances have been configured on the switch, the page displays a “No MSTs Available” message and does not display any fields.



To configure MST port settings:

1. To configure MST settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure MST settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure MST settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Configure the MST values for the selected port(s) or LAG(s):
 - **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 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. It takes a value in the range of 0–240.
- **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 1–200000000.
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 any configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

The following table describes the read-only MST port configuration information displayed on the Spanning Tree CST Configuration page.

Field	Description
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: <ul style="list-style-type: none"> • 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.

Click **Refresh** to update the screen with the latest MST information.

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, click **Switching > STP > Advanced > STP Statistics**.

The screenshot shows the NETGEAR web interface for a GS752TS switch. The 'Switching' tab is active, and the 'STP' sub-tab is selected. The 'Advanced' section is expanded to show 'STP Statistics'. A table displays statistics for 11 interfaces (1/g1 to 1/a11). All statistics are currently at 0. A 'REFRESH' button is located at the bottom right of the table area.

Interface	STP BPDUs Received	STP BPDUs Transmitted	RSTP BPDUs Received	RSTP BPDUs Transmitted	MSTP BPDUs Received	MSTP BPDUs Transmitted
1/g1	0	0	0	0	0	0
1/g2	0	0	0	0	0	0
1/g3	0	0	0	0	0	0
1/g4	0	0	0	0	0	0
1/g5	0	0	0	0	0	0
1/g6	0	0	0	0	0	0
1/g7	0	0	0	0	0	0
1/g8	0	0	0	0	0	0
1/g9	0	0	0	0	0	0
1/g10	0	0	0	0	0	0
1/a11	0	0	0	0	0	0

The following table describes the information available on the STP Statistics page.

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.

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

Multicast

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.

From the Multicast link, you can access the following pages:

- [MFDB](#) on page 135
- [Auto-Video Configuration](#) on page 137
- [IGMP Snooping](#) on page 138
- [IGMP Snooping Querier](#) on page 144
- [MLD Snooping](#) on page 147

MFDB

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.

MFDB Table

The MFDB table holds the port membership information for all active multicast address entries. 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, click **Switching** > **Multicast** > **MFDB** > **MFDB Table**.

The screenshot shows the Netgear web interface for a GS728TPS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Switching menu is expanded to show Ports, LAG, VLAN, Voice VLAN, Auto-VoIP, STP, Multicast, and Address Table. The Multicast menu is further expanded to show MFDB, MFDB Table, MFDB Statistics, Auto-Video, IGMP Snooping, IGMP Snooping Querier, and MLD Snooping. The MFDB Table page is displayed, featuring a search bar for MAC Address and a table with the following columns: MAC Address, VLAN ID, Component, Type, Description, Interfaces, and Forwarding Interfaces. The table is currently empty. There are CLEAR and REFRESH buttons at the bottom right of the table area.

The following table describes the fields in the MFDB Table.

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, and 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 , GMRP , MLD Snooping , and 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.

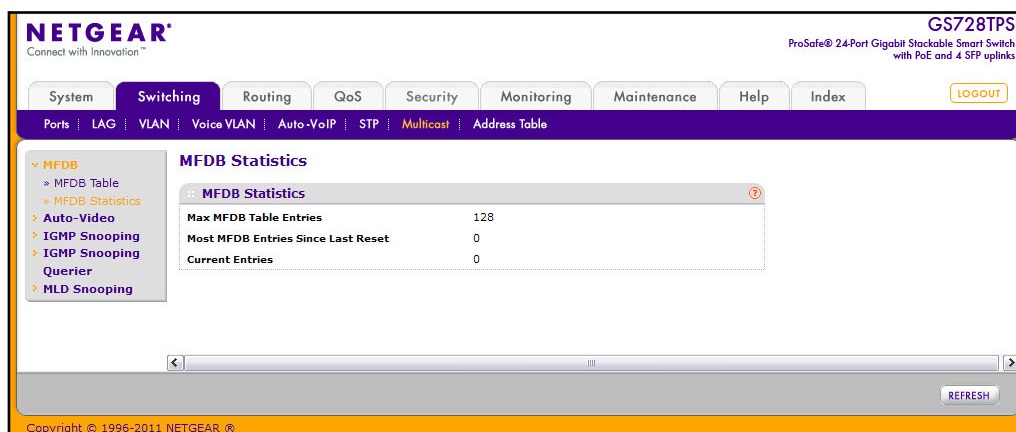
Click **Refresh** to update the information on the screen with the most current data.

Click **Clear** to clear all of the MFDB entries.

MFDB Statistics

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

To access the MFDB Statistics page, click **Switching > Multicast > MFDB > MFDB Statistics**.



The following table describes the information available on the MFDB Statistics page:

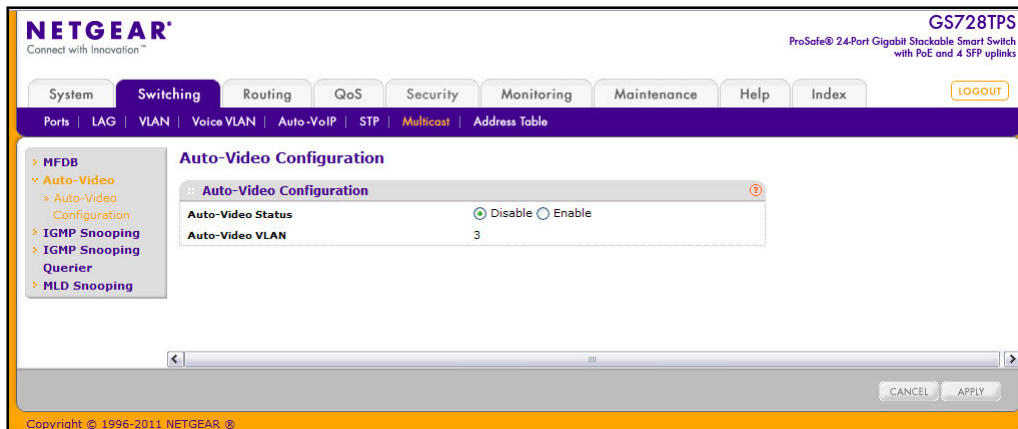
Field	Description
Max MFDB Table Entries	Displays the maximum number of entries that the Multicast Forwarding Database table can hold.
Most MFDB Entries Since Last Reset	The largest number of entries that have been present in the Multicast Forwarding Database table since the system was last reset. This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

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

Auto-Video Configuration

The Auto-Video feature simplifies IGMP Snooping Querier configuration if the switch supports devices or applications running multicast traffic, such as video surveillance cameras.

To access the Auto-Video Configuration page, click **Switching > Multicast > Auto-Video**.



To configure the Auto-Video feature:

1. Enable or disable the Auto-Video feature.
 - **Enable.** The IGMP Snooping Querier is automatically configured with the default VLAN ID for the Auto-Video VLAN
 - **Disable.** IGMP Snooping settings must be manually configured.
2. 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

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.

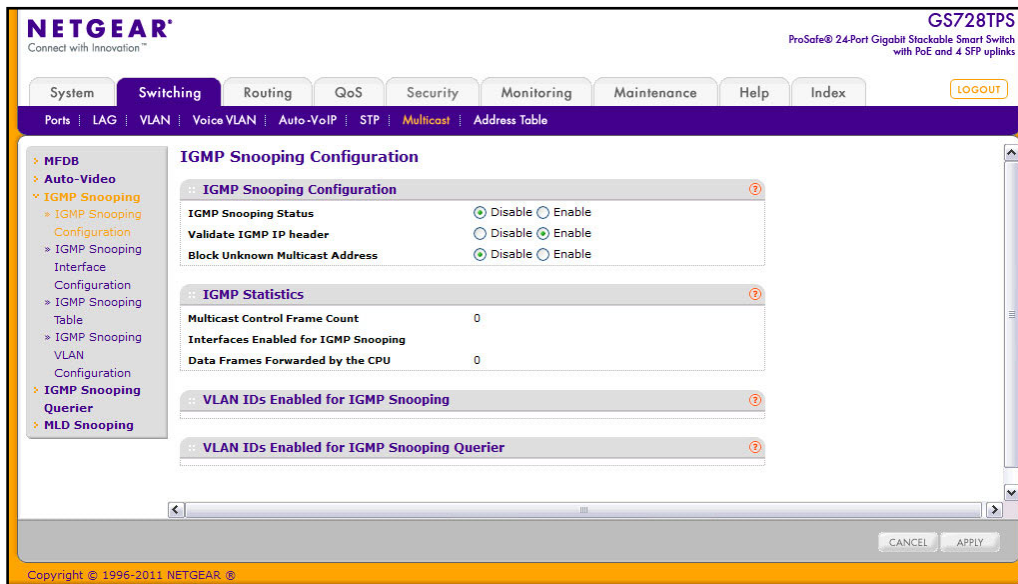
This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets 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 unrequested 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.

IGMP Snooping 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, click **Switching > Multicast > IGMP Snooping > IGMP Snooping Configuration**.



To configure IGMP Snooping:

1. Enable or disable IGMP Snooping on the switch.
 - **Enable.** The switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address.
 - **Disable.** The switch does not snoop IGMP packets.
2. Enable or disable the validation of IGMP IP headers.
 - **Enable.** The switch checks the IGMP IP header for valid Router Alert option, ToS, and TTL information.
 - **Disable.** The switch does not check the IGMP IP header for Router Alert option, ToS, and TTL information.
3. Specify whether to block unknown multicast addresses
 - **Enable.** The switch drops all packets with an unknown multicast MAC address in the destination field.
 - **Disable.** The switch forwards multicast packets with an unknown multicast MAC address in the destination field.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch

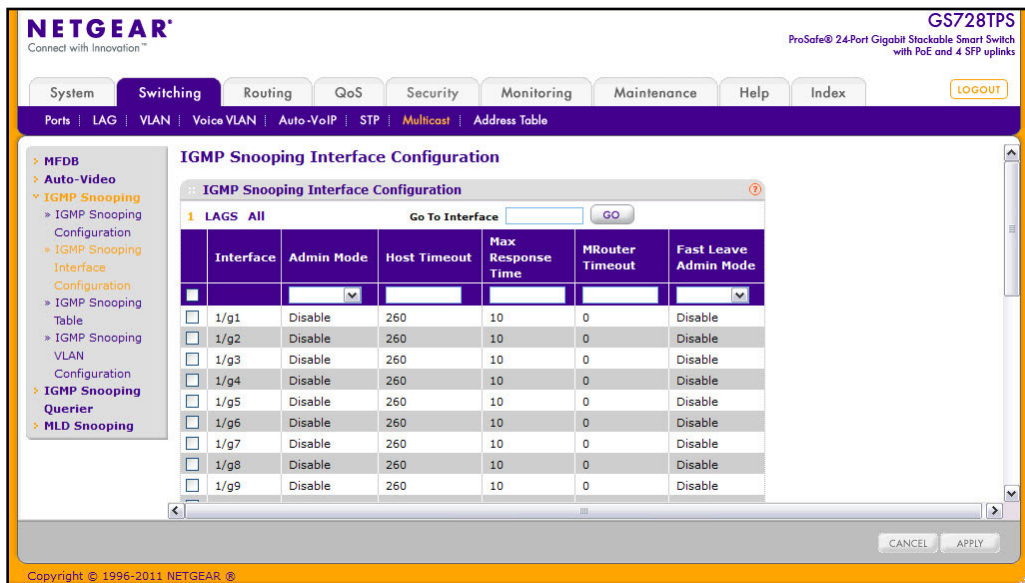
The following table displays information about the global IGMP snooping status and statistics on the page.

Field	Description
Multicast Control Frame Count	Displays 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 140.
Data Frames Forwarded by the CPU	Displays 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 142.
VLAN Ids Enabled For IGMP Snooping Querier	Displays VLAN IDs enabled for IGMP snooping querier.

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, click **Switching > Multicast > IGMP Snooping > IGMP Snooping Interface Configuration**.



To configure IGMP Snooping interface settings:

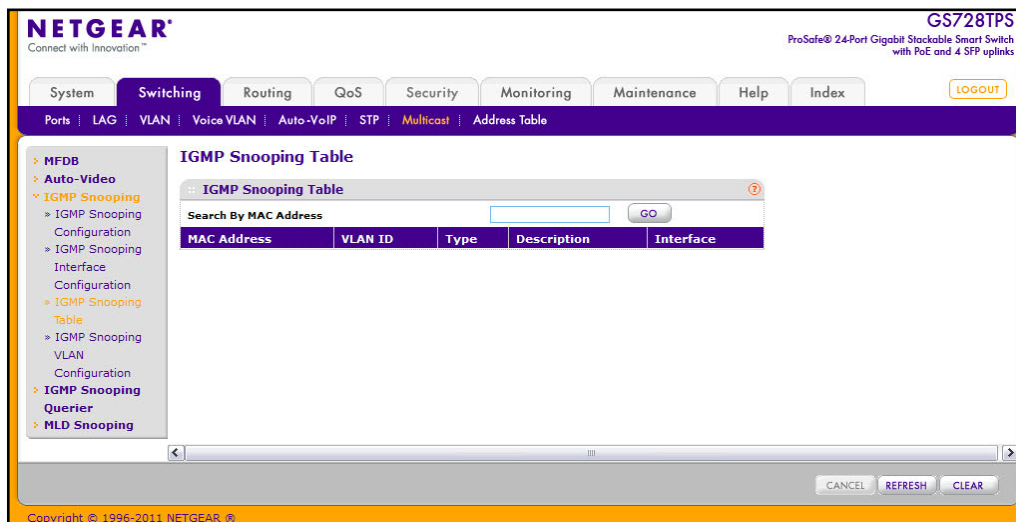
1. To configure IGMP Snooping settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure IGMP Snooping settings for a Link Aggregation Group (LAG), click **LAGS**.

3. To configure IGMP Snooping settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Configure the IGMP Snooping values for the selected port(s) or LAG(s):
 - **Admin Mode.** Use the menu to enable or disable the administrative mode of IGMP snooping on the selected interface(s). The default is Disable.
 - **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 2 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 Host Timeout, in seconds. The default is 10 seconds.
 - **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; no expiration.
 - **Fast Leave Admin Mode.** Select the Fast Leave mode for a particular interface from the menu. The default is Disable.
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 any configuration changes, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

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, click **Switching > Multicast > IGMP Snooping > IGMP Snooping Table**.



The following table describes the fields in the IGMP Snooping Table.

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 filtering information.
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 (Fit) for the associated address.

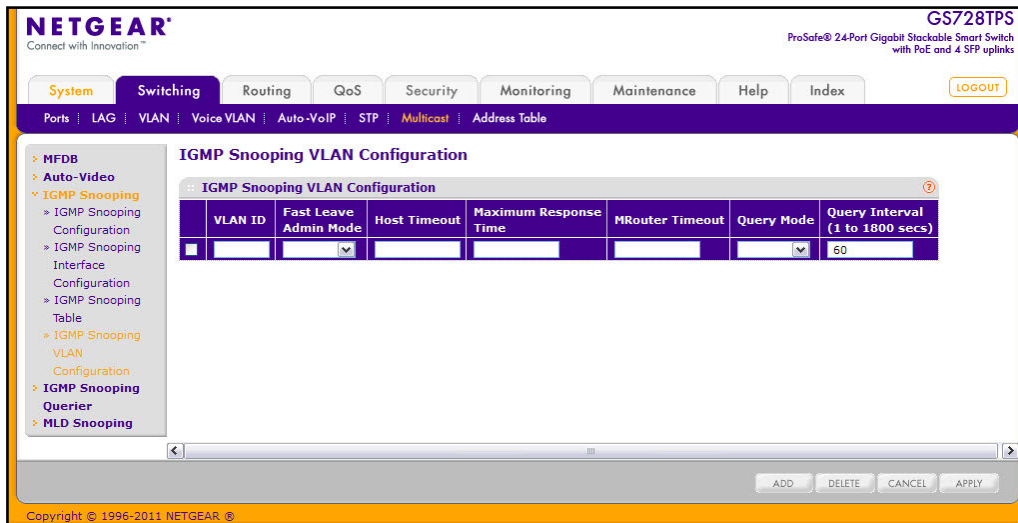
Use the buttons at the bottom of the page to perform the following actions:

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

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, click **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.



To configure IGMP snooping settings for VLANs:

- To enable IGMP snooping on a VLAN, enter the VLAN ID in the appropriate field and configure the IGMP Snooping values:
 - 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.
 - Maximum Response Time.** Enter the amount of time in seconds that a switch will wait after sending a query on the VLAN because it did not receive a report for a particular group in that interface. The valid range is 1 to 25 seconds. The Maximum Response Time value must be less than the Host Timeout value.
 - MRouter Timeout.** Enter the amount of time that a switch will wait to receive a query on the VLAN before removing it from the list of VLANs with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds, which means there is no expiration.
 - 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. The valid range is 1–1800 seconds. The default is 60 seconds.
- 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 disable IGMP snooping on a VLAN and remove it from the list, select the check box next to the VLAN ID and click **Delete**.
4. To modify IGMP snooping settings for a VLAN, select the check box next to the VLAN ID, update the desired values, and click **Apply**.

IGMP Snooping Querier

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 feature contains links to the following pages:

- [IGMP Snooping Querier Configuration](#) on page 144
- [IGMP Snooping Querier VLAN Configuration](#) on page 145
- [IGMP Snooping Querier VLAN Status](#) on page 146

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 the related parameters.

To access this page, click **Switching** > **Multicast** > **IGMP Snooping Querier** > **IGMP Snooping** > **Querier Configuration**.

The screenshot shows the Netgear web interface for a GS752TPS switch. The main navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Switching menu is expanded to show Ports, LAG, VLAN, Voice VLAN, Auto-VoIP, STP, Multicast, and Address Table. The Multicast menu is further expanded to show Querier Configuration, Querier VLAN Configuration, and Querier VLAN Status. The Querier Configuration page is displayed, showing the following settings:

Querier Configuration	
Querier Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Snooping Querier Address	<input type="text" value="0.0.0.0"/>
IGMP Version	<input type="text" value="2"/> (1 to 2)
Query Interval(secs)	<input type="text" value="60"/> (1 to 1800)
Querier Expiry Interval(secs)	<input type="text" value="125"/> (60 to 300)

At the bottom of the page, there are buttons for REFRESH, CANCEL, and APPLY. The footer indicates Copyright © 1996-2012 NETGEAR.

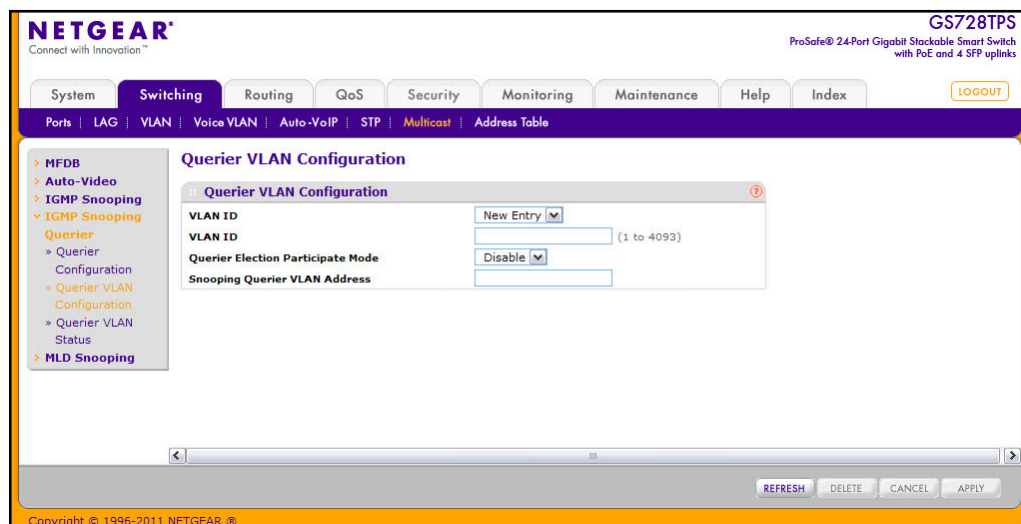
To configure IGMP Snooping Querier settings:

1. From the **Querier Admin Mode** field, enable or disable the administrative mode for IGMP Snooping Querier.
2. In the **Snooping Querier Address** field, specify the IP 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.
3. In the **IGMP Version** field, specify the IGMP protocol version used in periodic IGMP queries. The supported IGMP versions are 1 and 2. The default value is 2.
4. In the **Query Interval** field, 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 1–1800 seconds. The default value is 60.
5. In the **Querier Expiry Interval** field, 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 60–300 seconds. The default value is 125.
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. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately
8. Click **Refresh** to update the page with the latest information from the switch.

IGMP Snooping Querier VLAN Configuration

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

To access this page, click **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration**.



To configure Querier VLAN settings:

1. To create a new VLAN ID for IGMP Snooping, select New Entry from the VLAN ID field and complete the following fields:
 - **VLAN ID.** Specifies the VLAN ID for which the IGMP Snooping Querier is to be enabled.
 - **Querier Election Participate Mode.** Enable or disable Querier Participate Mode.
 - **Disabled.** Upon seeing another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
 - **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 IP Address to be used as the source address in periodic IGMP queries sent on the specified VLAN.
2. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately
3. To disable Snooping Querier on a VLAN, select the VLAN ID 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. Click **Refresh** to update the page with the latest information from 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, click **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status**.

The screenshot shows the Netgear web interface for a GS728TPS switch. The main content area is titled "Querier VLAN Status" and contains a table with the following data:

VLAN ID	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time(sec)
100	Disable	2			

The interface also features a sidebar with a navigation tree under "IGMP Snooping" and a "REFRESH" button at the bottom right of the table area.

The following table describes the information available on the Querier VLAN Status page.

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: <ul style="list-style-type: none"> • 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.

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

MLD Snooping

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2 and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

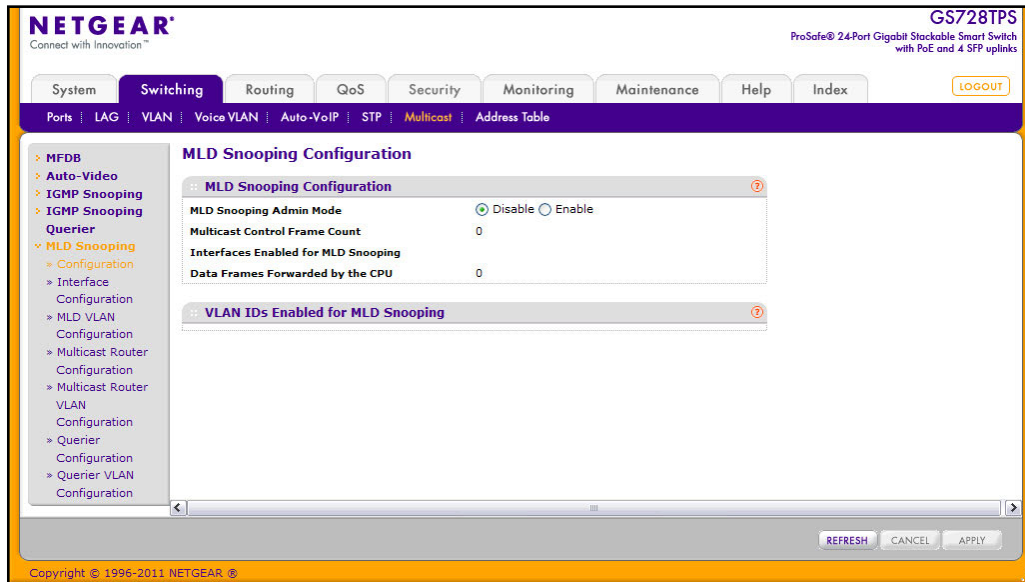
The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 Multicast MAC Addresses. The switch can be configured to perform MLD Snooping and IGMP Snooping simultaneously.

MLD Snooping Configuration

In IPv4, Layer 2 switches can use IGMP Snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports

that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

To access the MLD Snooping Configuration page, click **Switching > Multicast > MLD Snooping > MLD Snooping Configuration**.



To configure MLD Snooping:

1. Enable or disable the MLD Snooping Admin Mode, the administrative mode for MLD Snooping for the switch. The default is disable.
 - **Multicast Control Frame Count** - This displays the number of multicast control frames that are processed by the CPU.
 - **Interfaces Enabled for MLD Snooping** - This displays a list of all the interfaces currently enabled for MLD Snooping.
 - **Data Frames Forwarded by the CPU** - This displays the number of data frames forwarded by the CPU.
2. **VLAN IDs Enabled For MLD Snooping** - This displays VLAN IDs enabled for MLD snooping.
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 the page, click **Apply** to apply the changes to the system.
5. Click **Refresh** to update the page with the latest information from the switch.

MLD Interface Configuration

MLD snooping can be enabled on the interfaces (physical and lag).

To access the MLD Snooping Configuration page, click **Switching** > **Multicast** > **MLD Snooping** > **Interface Configuration**.

The screenshot shows the Netgear web interface for a GS728TPS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Switching menu is expanded to show Ports, LAG, VLAN, Voice VLAN, Auto-VoIP, STP, Multicast, and Address Table. The Multicast menu is further expanded to show MLD Snooping, and the MLD Snooping menu is expanded to show Interface Configuration. The MLD Snooping Interface Configuration page is displayed, showing a table of interfaces and their MLD snooping settings.

Interface	Admin Mode	Group Membership Interval (secs)	Max Response Time (secs)	Present Expiration Time (secs)	Fast Leave Admin Mode
<input type="checkbox"/> 1/g1	Disable	260	10	0	Disable
<input type="checkbox"/> 1/g2	Disable	260	10	0	Disable
<input type="checkbox"/> 1/g3	Disable	260	10	0	Disable
<input type="checkbox"/> 1/g4	Disable	260	10	0	Disable
<input type="checkbox"/> 1/g5	Disable	260	10	0	Disable
<input type="checkbox"/> 1/g6	Disable	260	10	0	Disable
<input type="checkbox"/> 1/g7	Disable	260	10	0	Disable
<input type="checkbox"/> 1/g8	Disable	260	10	0	Disable
<input type="checkbox"/> 1/g9	Disable	260	10	0	Disable

To configure the MLD interface:

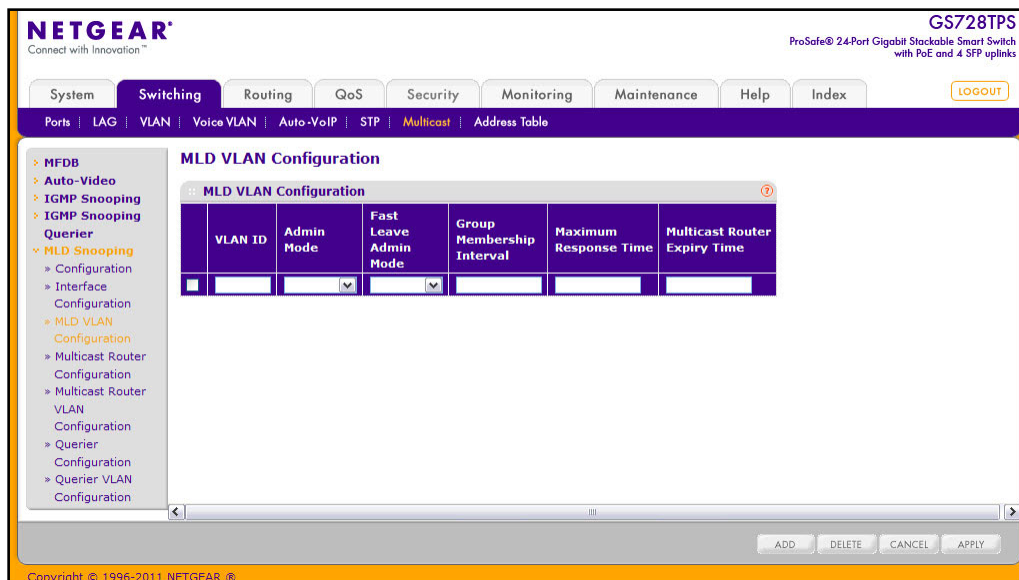
1. To configure MLD Snooping settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure MLD Snooping settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure MLD Snooping settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Use the **Admin Mode** menu to specify whether to enable or disable MLD snooping on the selected interface(s). The default is disable.
6. Use the **Group Membership Interval (secs)** field to 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. The valid range is from (2 to 3600) seconds. The configured value must be greater than Max Response Time. The default is 260 seconds.
7. Use the **Max Response Time (secs)** field to 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.
8. Use the **Present Expiration Time (secs)** field to 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, that is, no expiration.

9. Use the **Fast Leave Admin Mode** field to select the Fast Leave mode for a particular interface from the menu. The default is Disable.
10. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately
11. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

MLD VLAN Configuration

MLD Snooping can be enabled on a per VLAN basis. It is necessary to keep track of the interfaces that are participating in a VLAN in order to apply or remove configurations.

To access the MLD VLAN Configuration page, click **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.



To configure the MLD VLAN:

1. Set the VLAN IDs for which MLD Snooping is enabled in the **VLAN ID** field.
2. Enable MLD Snooping for the specified VLAN ID in the **Admin Mode** field.
3. Enable or disable the MLD Snooping Fast Leave Mode for the specified VLAN ID in the **Fast Leave Admin Mode** field.
4. Use the **Group Membership Interval** field to set the value for group membership interval of MLD Snooping for the specified VLAN ID. Valid range is (Maximum Response Time + 1) to 3600.
5. Use the **Maximum Response Time** field to set the amount of time, in seconds, that a switch will wait after sending a query on the VLAN because it did not receive a report for a particular group in that interface. The minimum response time value is 1, and the maximum value must be at least one second less than the value configured for the Group Membership Interval.

6. Use the **Multicast Router Expiry Time** field to set the value for multicast router expiry time of MLD Snooping for the specified VLAN ID. Valid range is 0 to 3600.
7. Click **Add** to enable MLD Snooping on the specified VLAN.
8. Click **Delete** to disable MLD Snooping on the specified VLAN.
9. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately
10. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
11. Click **Refresh** to update the page with the latest information from the switch.

Multicast Router Configuration

In addition to building and maintaining lists of multicast group memberships, the Snooping switch also maintains a list of multicast routers. When forwarding multicast packets, they should be forwarded on ports that have joined using MLD/IGMP and also on ports on which multicast routers are attached. In MLD/IGMP, there is only one active querier. This means that all other routers on the network are suppressed and are not detectable by the switch. If a query is not received on an interface within a specified length of time (multicast router present expiration time), then that interface is removed from the list of interfaces with multicast routers attached. The multicast router present expiration time is configurable via management. The default value for the multicast router expiration time is zero, which indicates an infinite timeout, that is, no expiration.

To access the Multicast Router Configuration page, click **Switching > Multicast > MLD Snooping > Multicast Router Configuration**.

The screenshot shows the Netgear web interface for a GS728TPS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The current page is 'Multicast Router Configuration' under the 'Multicast' section. The page title is 'Multicast Router Configuration' and it shows a table of interfaces and their multicast router status. The table has columns for 'Interface' and 'Multicast Router'. The status for all interfaces is 'Disable'.

Interface	Multicast Router
<input type="checkbox"/> 1/g1	Disable
<input type="checkbox"/> 1/g2	Disable
<input type="checkbox"/> 1/g3	Disable
<input type="checkbox"/> 1/g4	Disable
<input type="checkbox"/> 1/g5	Disable
<input type="checkbox"/> 1/g6	Disable
<input type="checkbox"/> 1/g7	Disable
<input type="checkbox"/> 1/g8	Disable
<input type="checkbox"/> 1/g9	Disable
<input type="checkbox"/> 1/g10	Disable
<input type="checkbox"/> 1/g11	Disable

At the bottom of the page, there are 'CANCEL' and 'APPLY' buttons. The footer shows 'Copyright © 1996-2011 NETGEAR'.

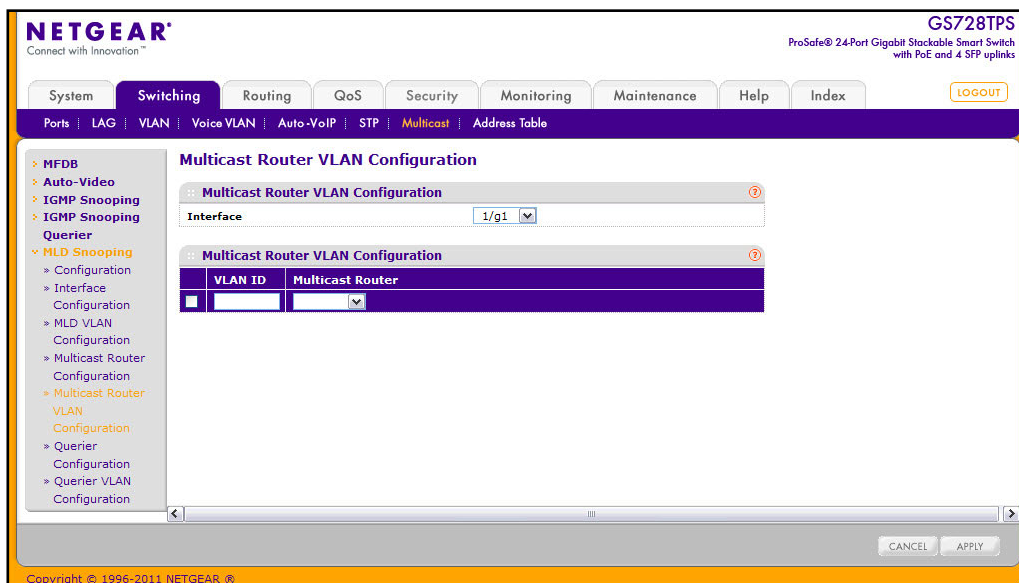
To configure the Multicast Router:

1. To configure multicast router settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure multicast router settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure multicast router settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Use the **Multicast Router** field to enable or disable Multicast Router on the selected interface.
6. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Multicast Router VLAN Configuration

The statically configured router attached (VLAN, Interface) is added to the learned multicast router attached interface list if the interface is active and is a member of the VLAN. Snooping dynamic learning mode (snooping interface mode or snooping VLAN mode) does not need to be enabled on the interface. The dynamic learning mode is applicable only for dynamically learned multicast router information (Queries from an attached true Querier).

To access the Multicast Router VLAN Configuration page, click **Switching > Multicast > MLD Snooping > Multicast Router Configuration VLAN Configuration**.



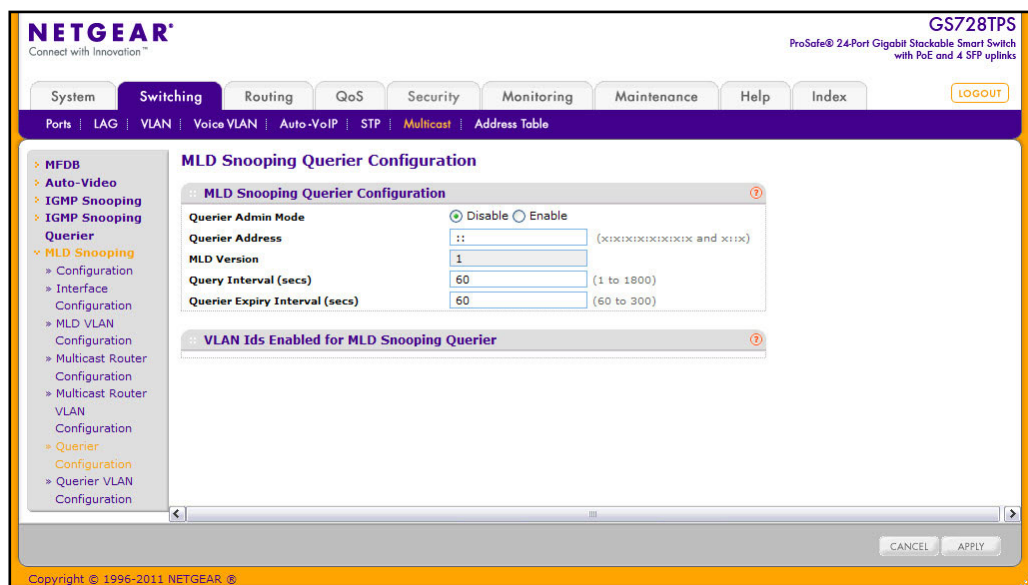
To configure the Multicast Router VLAN:

1. Use the **Interface** menu to select the interface to configure.
2. Enter the VLAN ID in the **VLAN ID** field for which the Multicast Router Mode is to be Enabled or Disabled.
3. Use the **Multicast Router** field to enable or disable Multicast Router on the selected interface.
4. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Querier Configuration

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

To access this page, click **Switching > Multicast > MLD Snooping > Querier Configuration**.



To configure the Querier settings:

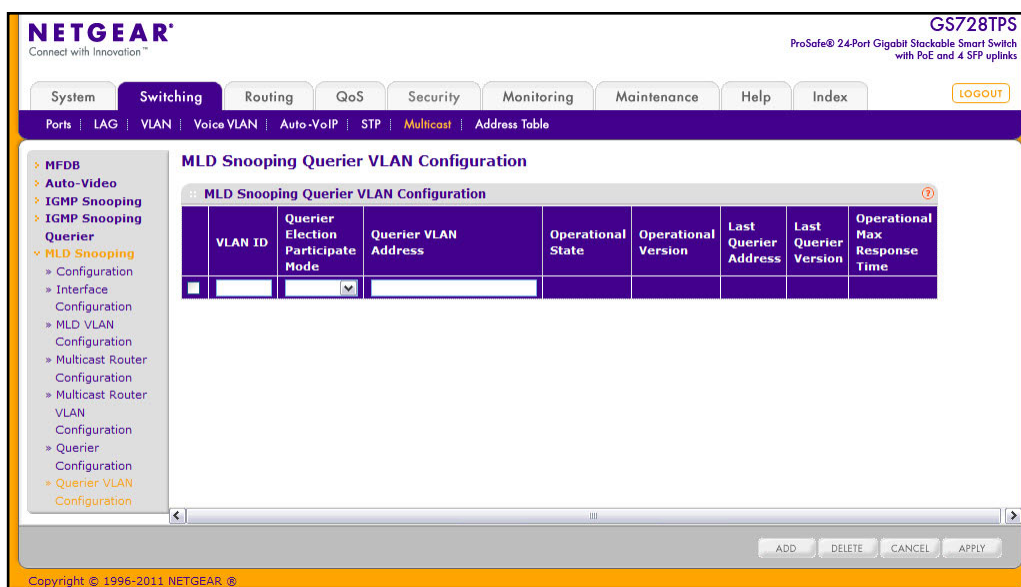
1. From the **Querier Admin Mode** field, enable or disable the administrative mode for MLD Snooping Querier.
2. In the **Querier Address** field, specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent. The supported IPv6 formats are x:x:x:x:x:x and x::x.
3. In the **MLD Version** field, the MLD protocol version used in periodic MLD queries is displayed. The supported MLD Version is 1.

4. In the **Query Interval** field, 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 1–1800 seconds. The default value is 60.
5. In the **Querier Expiry Interval** field, 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 60–300 seconds. The default value is 60.
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. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately

Querier VLAN Configuration

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

To access this page, click **Switching > Multicast > MLD Snooping Querier > Querier VLAN Configuration**.



The following table describes the information available on the Querier VLAN Status page.

Field	Description
VLAN ID	Specifies the VLAN ID on which MLD Snooping Querier is administratively enabled and VLAN exists in the VLAN database.
Querier Election Participate Mode	Enable or Disable the MLD Snooping Querier participate in election mode. When this mode is disabled, up on seeing other querier of same version in the VLAN, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least IP address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

Field	Description
Querier VLAN Address	Specify the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.
Operational State	Specifies the operational state of the IGMP Snooping Querier on a VLAN: <ul style="list-style-type: none"> • 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 MLD Snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.
Operational Version	Displays the MLD 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 MLD 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.

1. Click **Add** to add a Querier on the specified VLAN.
2. Click **Delete** to delete a Querier on the specified VLAN.
3. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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:

- [MAC Address Table](#) on page 156
- [Dynamic Address Configuration](#) on page 158
- [Static MAC Address](#) on page 159

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. Use the search function of the MAC Address Table page to display information about the entries in the table.

To access this page, click **Switching > Address Table > Basic > Address Table**.

The screenshot shows the Netgear web interface for a GS728TS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The 'Switching' menu is expanded to show Ports, LAG, VLAN, Voice VLAN, Auto-VoIP, STP, Multicast, and Address Table. The 'Address Table' page is displayed, showing a search bar for VLAN ID and a 'GO' button. Below the search bar, it indicates 'Total MAC Addresses: 7'. A table lists the following entries:

VLAN ID	MAC Address	Interface	status
99	00:01:F4:11:22:45	1/g1	Learned
99	00:01:FC:51:10:01	1/g1	Learned
99	00:04:0D:01:01:04	1/g1	Learned
99	00:1E:C9:AA:AC:02	1/g1	Learned
99	00:40:41:42:43:44	c1	Management
99	00:85:87:89:83:86	1/g1	Learned
99	E8:04:62:C0:4F:C1	1/g1	Learned

At the bottom of the page, there are 'CLEAR' and 'REFRESH' buttons, and a copyright notice: Copyright © 1996-2011 NETGEAR ®.

To search for an entry in the MAC Address Table:

1. 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 and click **Go**. The interface format is <unit>/g<port>. If any entries learned on that interface exist, they are displayed.
2. Click **Clear** to clear Dynamic MAC Addresses in the table.
3. Click **Refresh** to redisplay the page to show the latest MAC Addresses.

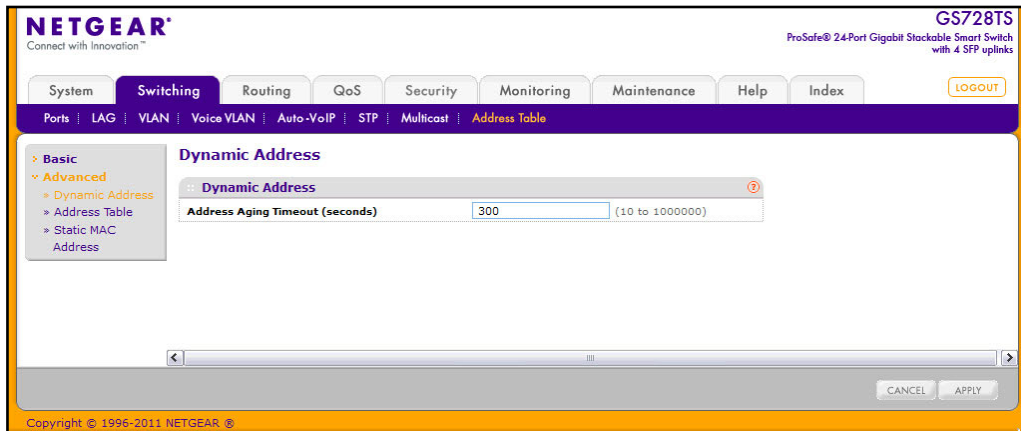
The following table describes the information available for each entry in the address table.

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 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: that is, this field displays the port through which the MAC address can be reached.
Status	The status of this entry. The possible values are: <ul style="list-style-type: none"> • 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.

Dynamic Address Configuration

Use the 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, click **Switching > Address Table > Advanced > Dynamic Addresses**.



To configure the Dynamic Address setting:

1. Specify the number of seconds the forwarding database should wait before deleting a learned entry that has not been updated. IEEE 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.

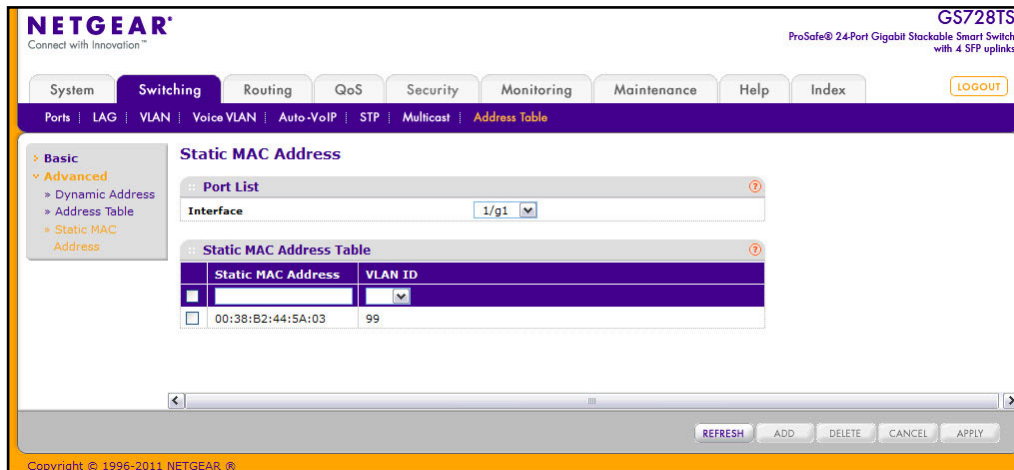
Note: IEEE 802.1D recommends a default of 300 seconds, which is the factory default.

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.

Static MAC Address

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

To access the Static MAC Address Configuration page, click **Switching > Address Table > Advanced > Static MAC Address**.



To configure a static MAC address:

1. To add a static MAC address entry:
 - a. From the **Interface** menu, select the port or LAG on which to configure the static MAC address.
 - b. Specify the MAC address to add.
 - c. Select the VLAN ID corresponding to the MAC address to add.
 - d. Click **Add**.
2. To delete a static MAC address, select the check box next to the entry and click **Delete**.
3. To modify the settings for a static MAC address, select the check box next to the entry, update the desired values, and click **Apply**.
4. Click **Refresh** to reload the page and display the latest MAC address learned on a specific port.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Configuring Routing

4

The GS728TS, GS728TPS, GS752TS, and GS752TPS switches support IP routing. Use the links in the Routing menu to manage and monitor routing on the system. This section contains the following information:

- [Configuring IP Settings](#) on page 160
- [Configuring VLAN Routing](#) on page 165
- [Configuring Router Discovery](#) on page 168
- [Configuring and Viewing Routes](#) on page 169
- [Configuring ARP](#) on page 171

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

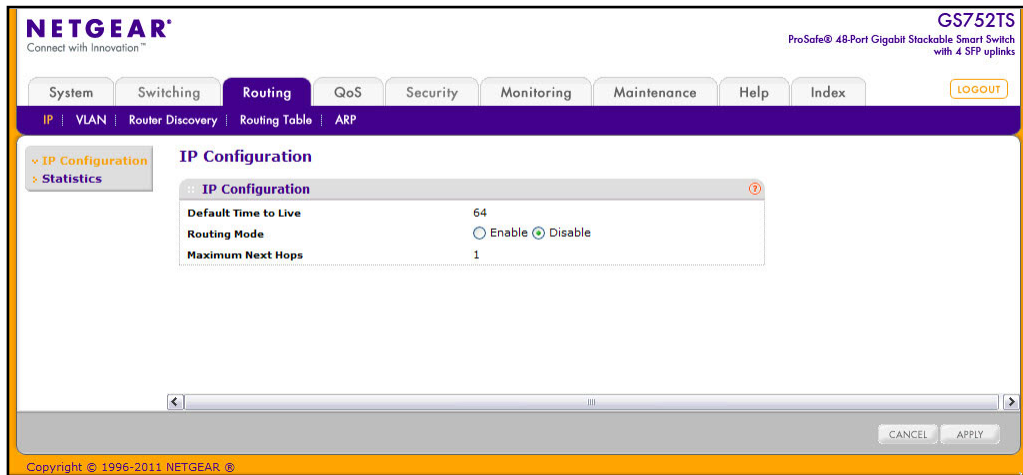
The pages available from the IP tab allow you to globally enable routing and view information about the packets received and transmitted by the switch. From the IP link, you can access the following pages:

- [IP Configuration](#) on page 161
- [IP Statistics](#) on page 162

IP Configuration

Use the IP Configuration page to enable routing on the switch and to view global routing settings.

To access the IP Configuration page click **Routing** > **IP**, then click the **IP Configuration** link.



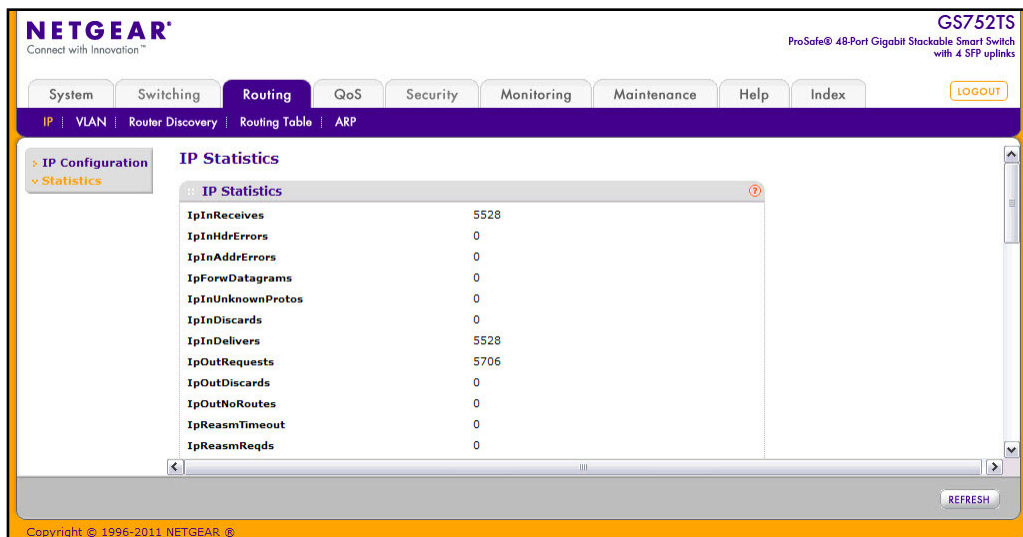
To configure or view the global routing settings on the switch:

1. View the default time to live, which is the 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.
2. From the **Routing Mode** field, 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.
3. View the maximum next hops, which is the maximum number of hops supported by the switch. This is a read-only value.
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 changes to the system.

IP Statistics

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

To access the page click **Routing** > **IP**, then click the **Statistics** link. The following image shows some, but not all, of the fields the page displays.



The following table describes the information available on the IP Statistics page

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.
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.

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

Field	Description
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.
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.

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

Field	Description
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.
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.

Field	Description
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
IcmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

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

Configuring VLAN Routing

You can configure GS728TS, GS728TPS, GS752TS, and GS752TPS switches 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 GS728TS, GS728TPS, GS752TS, and GS752TPS switches 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.

From the VLAN link, you can access the following pages:

- [VLAN Routing Wizard](#) on page 165
- [VLAN Routing Configuration](#) on page 167

VLAN Routing Wizard

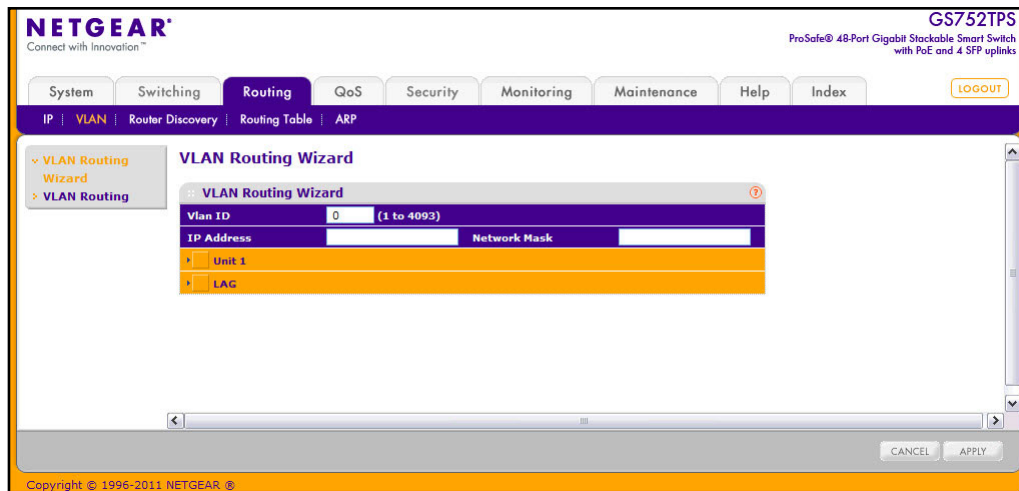
The VLAN Routing Wizard allows you to create a VLAN routing interface, configure the IP address and subnet mask for the interface, and add selected ports or LAGs to the VLAN.

With this wizard, you can:

- Create a VLAN.
- Add selected ports to the newly created VLAN and remove selected ports from the default VLAN.
- Add selected LAGs to the newly created VLAN.
- Enable tagging on selected ports if the port is in another VLAN. Disable tagging if a selected port does not exist in another VLAN.

- Exclude ports not selected from the VLAN.
- Enable routing on the VLAN using the IP address and subnet mask entered.

To display the page, click **Routing** > **VLAN**, and then click the **VLAN Routing Wizard** link.



To use the wizard to configure VLAN routing:

1. Specify the VLAN ID in the appropriate field. The VLAN Identifier (VID) associated with this VLAN. The range of the VLAN ID is (1 to 4093).
2. Specify the IP address of the VLAN routing interface.
3. In the **Network Mask** field, specify the subnet mask to associate with the IP address.
4. Select the physical ports or LAGs to add as members to the VLAN interface.

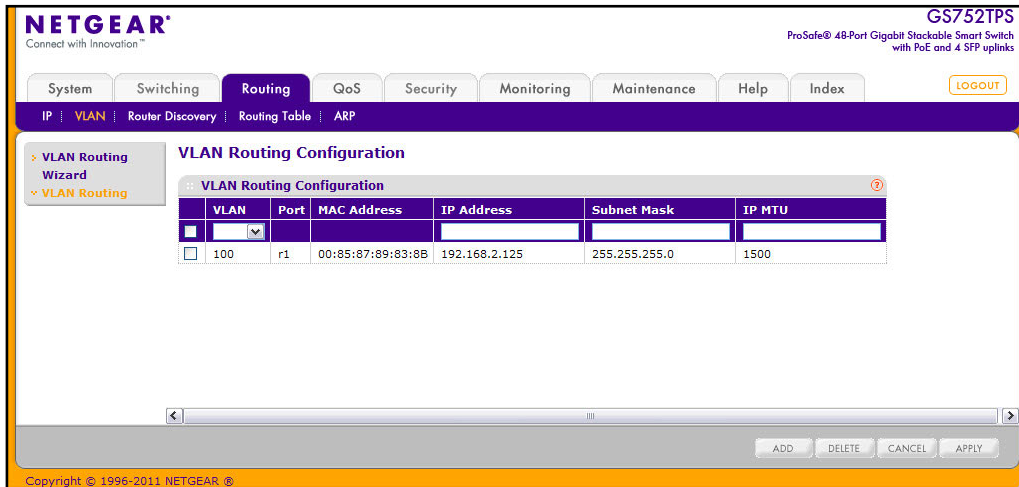
To display the ports, click the unit number of the stack member with the ports to add to the VLAN interface. Click **LAG** to display the LAGs to add to the VLAN interface. Click the box below each port or LAG to add or remove it as a member. You can add each port or LAG as one of the following member types:

- **T (Tagged)** - All frames transmitted for this VLAN will be tagged.
 - **U (Untagged)** - All frames transmitted for this VLAN will be untagged.
 - **BLANK (Autodetect)** - Ports or LAGs may be dynamically registered in this VLAN via GVRP. This selection has the effect of excluding a port from the selected VLAN.
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 change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

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, click **Routing** > **VLAN**, and then click the **VLAN Routing** link.



To configure VLANs for routing:

1. Select the VLAN you want to configure for VLAN Routing. The VLAN field displays the IDs of all VLANs configured on this switch. To change the settings for a VLAN routing interface that has already been configured, select the appropriate check box.
2. Enter an IP address for the VLAN Routing Interface.
3. Enter a subnet mask for the VLAN Routing Interface.
4. Specify the maximum size of IP packets sent on an interface. A valid range is from 68 bytes to the link MTU. The default value is 1500. A value of 0 indicates that the IP MTU is unconfigured. When the IP MTU is unconfigured, the router uses the link MTU as the IP MTU. The link MTU is the maximum frame size minus the length of the layer 2 header.
5. View additional information about configured VLAN routing interfaces:
 - Port. The logical interface number assigned to the VLAN routing interface.
 - MAC Address. The MAC Address assigned to the VLAN routing interface.
6. Click **Add** to add the VLAN routing interface.
7. Click **Delete** to remove the selected VLAN routing interface.
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.

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 click **Routing**, and then click the **Router Discovery** link.

The screenshot shows the Netgear web interface for a GS728TPS switch. The 'Routing' tab is active, and the 'Router Discovery' sub-tab is selected. The 'Router Discovery Configuration' page displays a table with the following data:

Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval	Minimum Advertise Interval	Advertise Lifetime	Preference Level
<input type="checkbox"/> r1	Disable	224.0.0.1	600	450	1800	0

Buttons for 'CANCEL' and 'APPLY' are visible at the bottom right of the configuration area.

To configure the router discovery settings:

1. 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.
2. From the **Advertise Mode** field, select Enable or Disable from the drop-down menu. If you select Enable, Router Advertisements are transmitted from the selected interface.
3. In the **Advertise Address** field, enter the IP Address to be used to advertise the router.
4. In the **Maximum Advertise Interval** field, enter the maximum time (in seconds) allowed between router advertisements sent from the interface. The allowed range for this field is 4 to 1800.
5. In the **Minimum Advertise Interval** field, enter the minimum time (in seconds) allowed between router advertisements sent from the interface. The allowed range for this field is 3 to 1800.

6. In the **Advertise Lifetime** field, 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.
7. In the **Preference Level** field, 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.
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.

Configuring and Viewing Routes

From the **Routing Table** page, you can configure static and default routes and view the routes that the GS728TS, GS728TPS, GS752TS, and GS752TPS has already learned.

To display the page click the **Routing > Routing Table** link.

The screenshot shows the Netgear web interface for a GS728TS switch. The 'Routing' tab is selected, and the 'Routing Table' page is displayed. The 'Route Configuration' section is active, showing a table for 'Configure Routes' with the following data:

Route Type	Network Address	Subnet Mask	Next Hop IP Address	Preference	Identifier
Static	192.168.3.0	255.255.255.0	192.168.7.31	100	file server

Below this table is a 'Route Status' section with a table that is currently empty. At the bottom of the page, there are buttons for CLEAR, REFRESH, ADD, DELETE, CANCEL, and APPLY.

To configure a route:

1. In the **Route Type** field, specify whether the route is to be a Default route or a Static route. If creating a default route, you need to specify only the next hop IP address; otherwise, you need to specify each field.
2. In the **Network Address** field, specify the IP route prefix for the destination. 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.
3. In the **Subnet Mask** field, specify the network mask to indicate the portion of the IP address that identifies the attached network.
4. In the **Next Hop IP Address** field, specify 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.

5. In the **Preference** field, specify 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.

6. In the **Identifier** field, optionally specify a description to identify the route.
7. To add a route, enter the route information into the appropriate fields and click **Add**.
8. 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 GS728TS, GS728TPS, GS752TS, and GS752TPS already has in its routing table.

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: <ul style="list-style-type: none"> • Local • Static
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
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. GS728TS, GS728TPS, GS752TS, and GS752TPS switches 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 GS728TS, GS728TPS, GS752TS, and GS752TPS switches support 1024 ARP entries, which includes dynamic and static 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 172
- [ARP Create](#) on page 173
- [Global ARP Configuration](#) on page 174
- [ARP Entry Management](#) on page 175

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, click the **Routing** > **ARP**, then click the **Basic** > **ARP Cache** link.

The Management VLAN ARP Cache table displays the following information:

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

The Routing VLANs ARP Cache table displays the following information:

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.

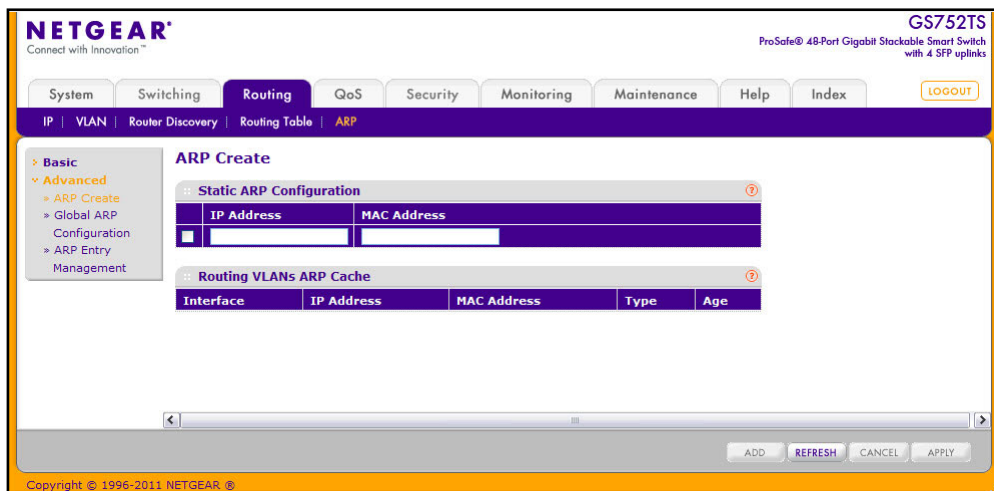
Field	Description
Type	The type of the ARP entry. Possible values are: <ul style="list-style-type: none"> • Local. An ARP entry associated with one of the switch's routing interface's MAC addresses. • Gateway. A dynamic ARP entry whose IP address is that of a router. • Static. An ARP entry configured 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.

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

ARP Create

Use this page to add a static entry to the ARP table.

To display the page, click **Routing** > **ARP**, then click the **Advanced** > **ARP Create** link.



To configure a static ARP entry:

1. In the **IP Address** field, 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.
2. In the **MAC Address** field, enter 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.
3. Click **Add** to add an ARP Entry.
4. If you made any changes to existing entries, click **Apply** to update the settings.
5. To delete an entry, select the box associated with the entry and click **Delete**.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

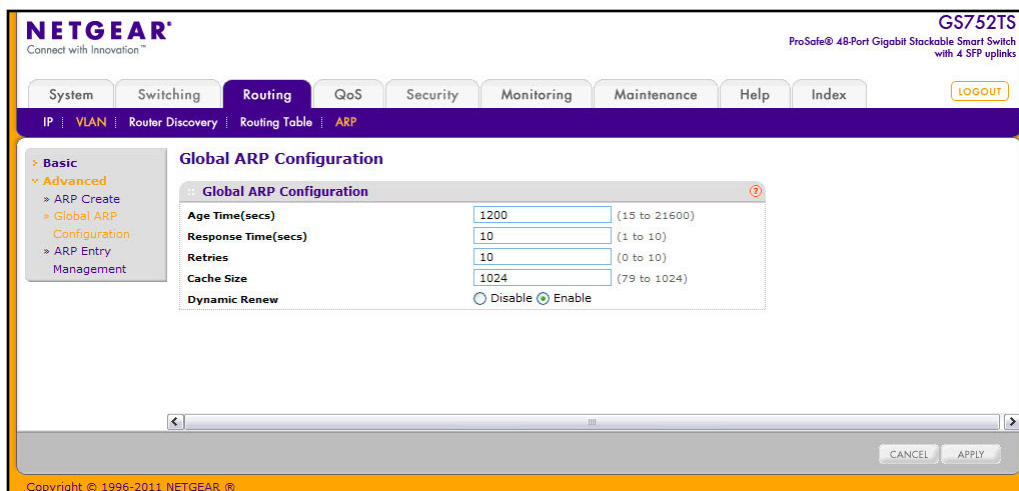
The Routing VLANs ARP Cache table displays the following information:

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: <ul style="list-style-type: none"> • 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

Global ARP Configuration

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

To display the page, click **Routing > ARP**, and then click the **Advanced > Global ARP Configuration** link.



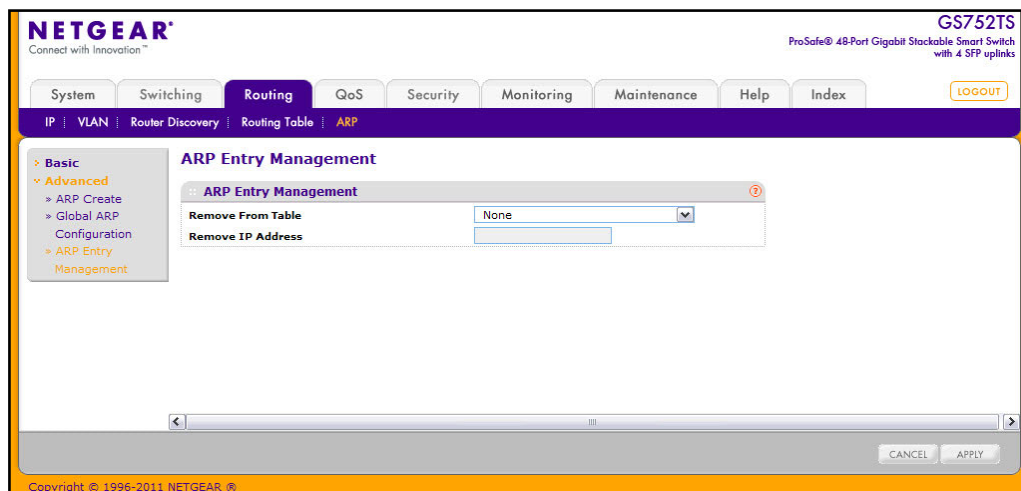
To configure the global ARP settings:

1. In the **Age Time** field, 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.
2. In the **Response Time** field, 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.
3. In the **Retries** field, 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.
4. In the **Cache Size** field, enter an integer which specifies the maximum number of entries for the ARP cache. The range is 79 to 1024. The default value is 1024.
5. In the Dynamic Renew field, select whether the ARP component automatically attempts to renew ARP entries of type Dynamic when they age out. The default setting is Enable.
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 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, click **Routing** > **ARP**, then click the **Advanced** > **ARP Entry Management** link.



To manage the ARP entries:

1. To move certain type of entries, select the type of entries to remove from the **Remove From Table** menu. 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.
2. 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.
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.

Configuring Quality of Service

5

Use the features in the QoS tab to configure Quality of Service (QoS) settings on the switch. The QoS tab contains links to the following features:

- [Class of Service](#) on page 177
- [Differentiated Services](#) on page 184

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.

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, or transmission rate shaping are user-configurable at the queue (or port) level.

Four queues per port are supported.

From the Class of Service link under the QoS tab, you can access the following pages:

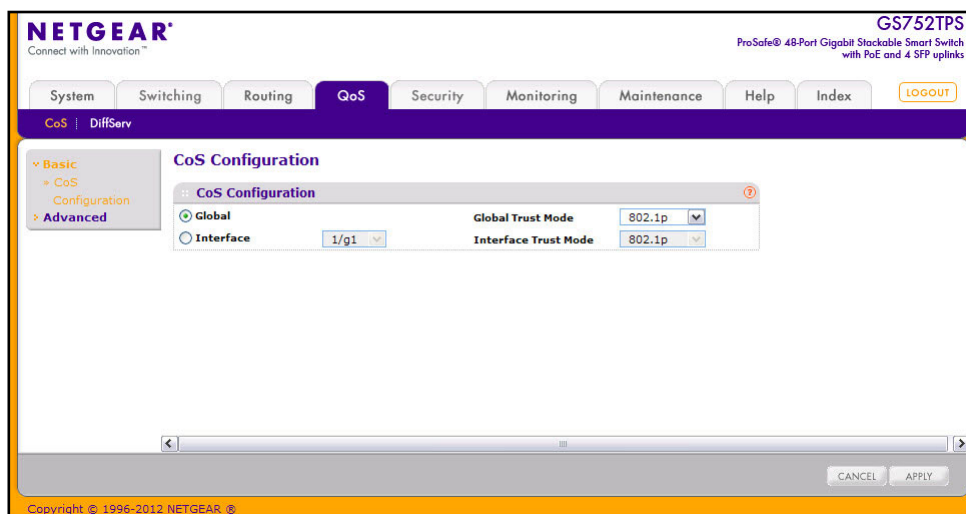
- [Basic CoS Configuration](#) on page 178
- [CoS Interface Configuration](#) on page 179
- [Interface Queue Configuration](#) on page 180
- [802.1p to Queue Mapping](#) on page 182
- [DSCP to Queue Mapping](#) on page 183

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, click **QoS > Basic > CoS Configuration**.



To configure global CoS settings:

1. Select the **Global** radio button to configure the trust mode settings that apply to all interfaces.
Alternatively, you can select the **Interface** radio button to apply trust mode settings to individual interfaces. The per-interface setting overrides the global settings.
2. Select the trust mode for all interfaces (**Global Trust Mode**) or the selected interface (**Interface Trust Mode**). This setting determines the type of CoS marking to trust when the frame enters the port.
 - **Untrusted**. Do not trust any CoS packet marking at ingress.
 - **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of four internal hardware priority queues: High, Normal, Low, and Lowest.
 - **DSCP**. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.
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.

CoS Interface Configuration

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

To display the CoS Interface Configuration page, click the **QoS > CoS** tab, and then click the **Advanced > CoS Interface Configuration** link.

The screenshot shows the Netgear web interface for a GS752TS switch. The main content area is titled "CoS Interface Configuration" and features a table with the following columns: "Interface", "Interface Trust Mode", and "Interface Shaping Rate (16 to 16384)". The table lists interfaces 1/g1 through 1/g8, each with a radio button for selection, a dropdown menu for the trust mode (currently set to "802.1p"), and a text input field for the shaping rate (currently set to "0"). A "Go To Interface" search box is located above the table. The interface also includes a "LOGOUT" button in the top right and "CANCEL" and "APPLY" buttons at the bottom right.

Interface	Interface Trust Mode	Interface Shaping Rate (16 to 16384)
<input type="checkbox"/> 1/g1	802.1p	0
<input type="checkbox"/> 1/g2	802.1p	0
<input type="checkbox"/> 1/g3	802.1p	0
<input type="checkbox"/> 1/g4	802.1p	0
<input type="checkbox"/> 1/g5	802.1p	0
<input type="checkbox"/> 1/g6	802.1p	0
<input type="checkbox"/> 1/g7	802.1p	0
<input type="checkbox"/> 1/g8	802.1p	0

To configure CoS settings for an interface:

1. To configure CoS settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure CoS settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure CoS settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces.
5. From the **Interface Trust Mode** field, specify whether or not the selected interface(s) trust a particular packet marking when the packet enters the port.
 - **Untrusted**. Do not trust any CoS packet marking at ingress.
 - **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of four internal hardware priority queues: High, Normal, Low, and Lowest.
 - **DSCP**. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.
6. From the **Interface Shaping Rate** field, specify the maximum bandwidth allowed on the selected interface(s). This setting is typically used to shape the outbound transmission rate in increments of 64 kbps. 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.

The expected shaping at egress interface is calculated as:

$(frameSize \times shaping \times 64) \div (frameSize + IFG)$, where *IFG* (Inter frame gap) is 20 bytes, *frameSize* is the configured frame size of the traffic, and *shaping* is the configured traffic shaping in the **Interface Shaping Rate** field.

For example, when a 64 byte frame size and 64 kbps interface shaping rate are configured, the expected shaping will be approximately 3121 kbps.

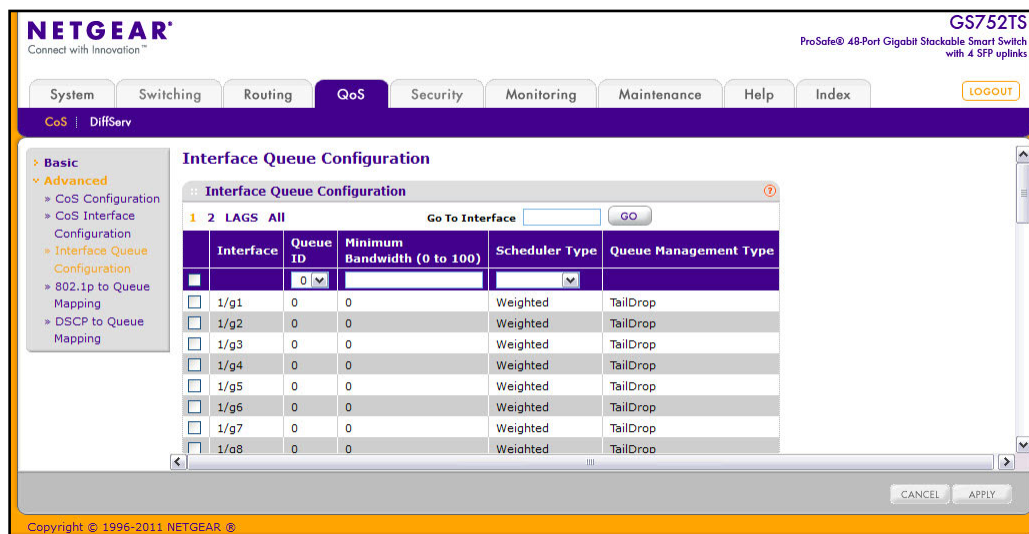
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
8. If you make changes to the page, click **Apply** to apply the changes to the system.

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

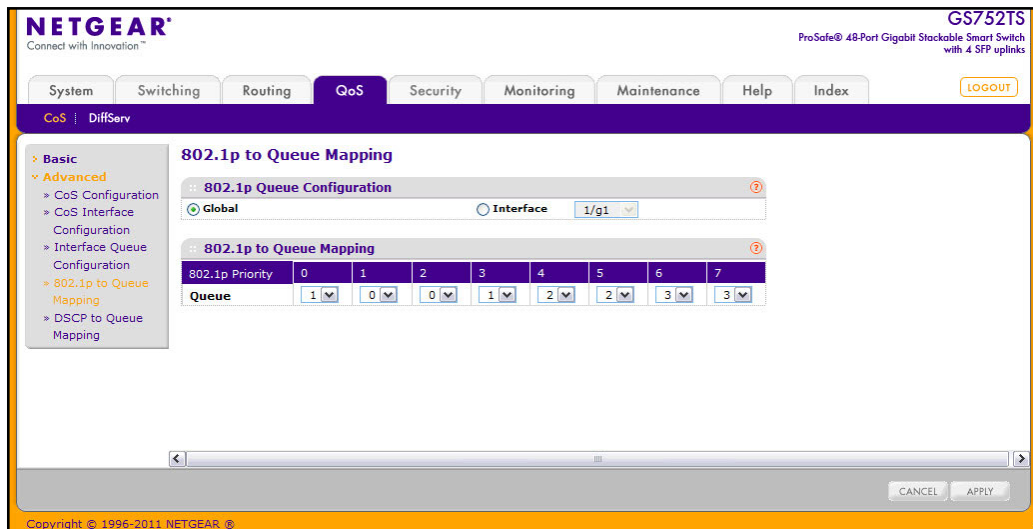


To configure CoS queue settings for an interface:

1. To configure CoS queue settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure CoS queue settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure CoS queue settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply a trust mode or rate to all interfaces.
5. Configure any of the following settings:
 - **Queue ID.** Use the menu to select the queue to be configured.
 - **Minimum Bandwidth.** Enter a percentage of the maximum negotiated bandwidth for the selected queue on the interface. Specify a percentage from 0–100, in increments of 1.
 - **Scheduler Type.** Selects the type of queue processing from the drop down 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.
 - **Strict:** 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.
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.

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, click **QoS > CoS > Advanced > 802.1p to Queue Mapping**.



To map 802.1p priorities to queues:

1. Select the Global radio button to apply the same 802.1p priority mapping to all CoS configurable interfaces or select the Interface radio button to apply 802.1p priority mapping to on a per-interface basis.

If you map 802.1p priorities to individual interfaces, select the Interface radio button and then select the interface from the drop-down menu. The interface settings override the global settings for 802.1p priority mapping.

2. Select the queue to map to the predefined 802.1p priority values.

The 802.1p Priority 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 7, might be time-sensitive traffic, such as voice or video.

The values in each drop down 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.

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.

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, click **QoS > CoS > Advanced > DSCP to Queue Mapping**.

NETGEAR GS752TS
ProSafe® 48-Port Gigabit Stackable Smart Switch with 4 SFP uplinks

System Switching Routing **QoS** Security Monitoring Maintenance Help Index LOGOUT

CoS | DiffServ

Basic
Advanced
CoS Configuration
CoS Interface Configuration
Interface Queue Configuration
802.1p to Queue Mapping
DSCP to Queue Mapping

DSCP to Queue Mapping

Class Selector (CS) PHB

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
CS 0 (000000)	1	CS 2 (010000)	0	CS 4 (100000)	2	CS 6 (110000)	3
CS 1 (001000)	0	CS 3 (011000)	1	CS 5 (101000)	2	CS 7 (111000)	3

Assured Forwarding (AF) PHB

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
AF 11 (001010)	0	AF 21 (010010)	0	AF 31 (011010)	1	AF 41 (100010)	2
AF 12 (001100)	0	AF 22 (010100)	0	AF 32 (011100)	1	AF 42 (100100)	2
AF 13 (001110)	0	AF 23 (010110)	0	AF 33 (011110)	1	AF 43 (100110)	2

Expedited Forwarding (EF) PHB

DSCP	Queue
EF (101110)	2

Other DSCP Values (Local/Experimental Use)

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
1 (000001)	1	17 (010001)	0	39 (100111)	2	53 (110101)	3
2 (000010)	1	19 (010011)	0	41 (101001)	2	54 (110110)	3
3 (000011)	1	21 (010101)	0	42 (101010)	2	55 (110111)	3
4 (000100)	1	23 (010111)	0	43 (101011)	2	57 (111001)	3
5 (000101)	1	25 (011001)	1	44 (101100)	2	58 (111010)	3
6 (000110)	1	27 (011011)	1	45 (101101)	2	59 (111011)	3
7 (000111)	1	29 (011101)	1	47 (101111)	2	60 (111100)	3
9 (001001)	0	31 (011111)	1	49 (110001)	3	61 (111101)	3
11 (001011)	0	33 (100001)	2	50 (110010)	3	62 (111110)	3
13 (001101)	0	35 (100011)	2	51 (110011)	3	63 (111111)	3
15 (001111)	0	37 (100101)	2	52 (110100)	3		

CANCEL APPLY

Copyright © 1996-2011 NETGEAR

To map DSCP values to queues:

- For each DSCP value, select a hardware queue to associate with the value.
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. The valid range is 0–6.
- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
- If you make changes to the page, click **Apply** to apply the changes to the system.

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.

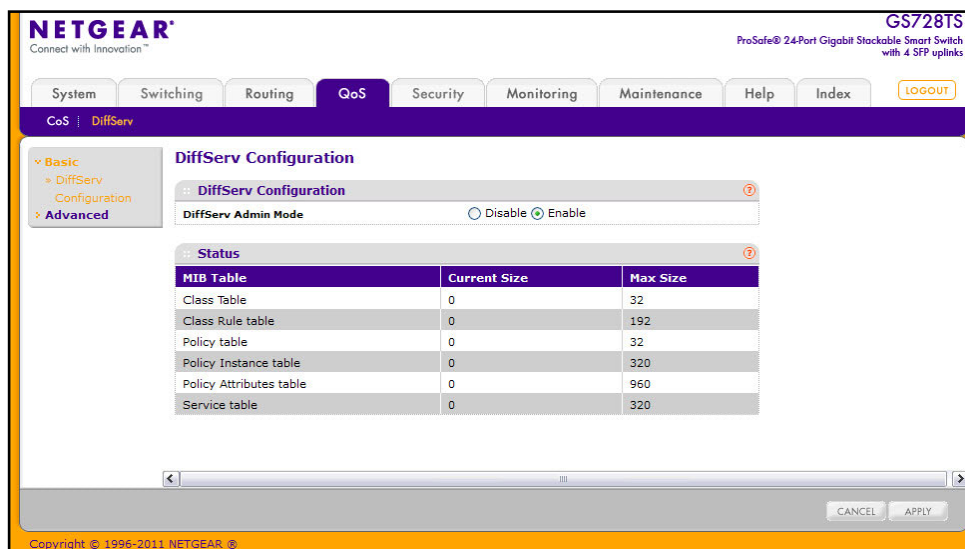
To display the page, click **QoS > DiffServ**. The Differentiated Services menu page contains links to the following features:

- *Diffserv Configuration* on page 185
- *Class Configuration* on page 186
- *IPv6 Class Configuration* on page 189
- *Policy Configuration* on page 191
- *Service Configuration* on page 195
- *Service Statistics* on page 196

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, click **QoS > DiffServ > Advanced > Diffserv Configuration**.



The screenshot shows the Netgear web interface for a GS728TS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, Index, and LOGOUT. The current page is 'DiffServ Configuration' under the 'QoS' menu. The 'DiffServ Admin Mode' is set to 'Enable'. Below this is a 'Status' section with a table of MIB tables.

MIB Table	Current Size	Max Size
Class Table	0	32
Class Rule table	0	192
Policy table	0	32
Policy Instance table	0	320
Policy Attributes table	0	960
Service table	0	320

To configure the global DiffServ mode:

1. Select the administrative mode for DiffServ:
 - **Enable.** Differentiated Services are active.
 - **Disable.** The DiffServ configuration is retained and can be changed, but it is not active.
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.

The following table describes the information displayed in the Status table on the DiffServ Configuration page:

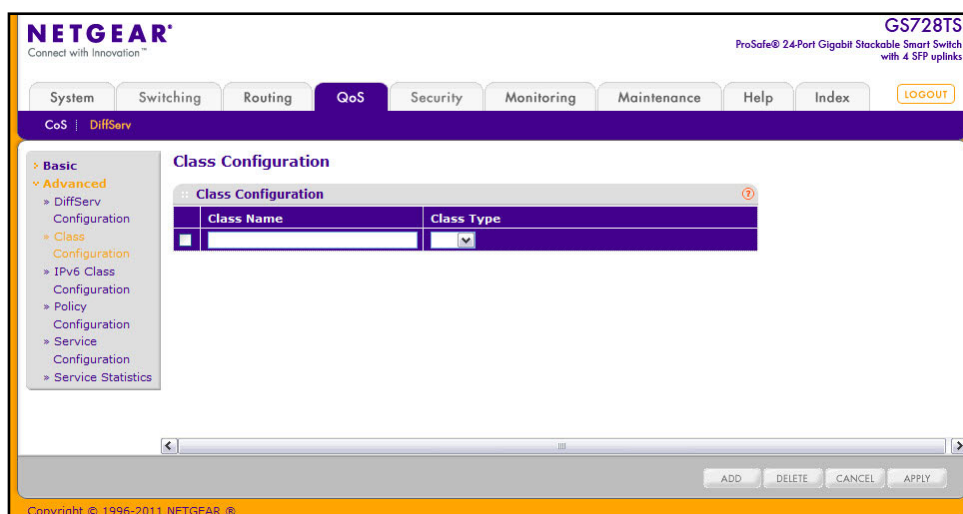
Field	Description
Class Table	Displays the current and maximum number of rows of the class table.
Class Rule Table	Displays the current and maximum number of rows of the class rule table.
Policy Table	Displays the current and maximum number of rows of the policy table.
Policy Instance Table	Displays 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.

Click **Refresh** to update the page with the current settings.

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. After creating a Class, click the class link to the Class page.

To display the page, click **QoS > DiffServ > Advanced > Class Configuration**.

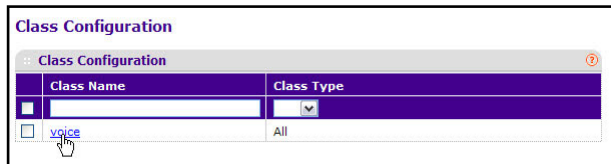


To configure a DiffServ class:

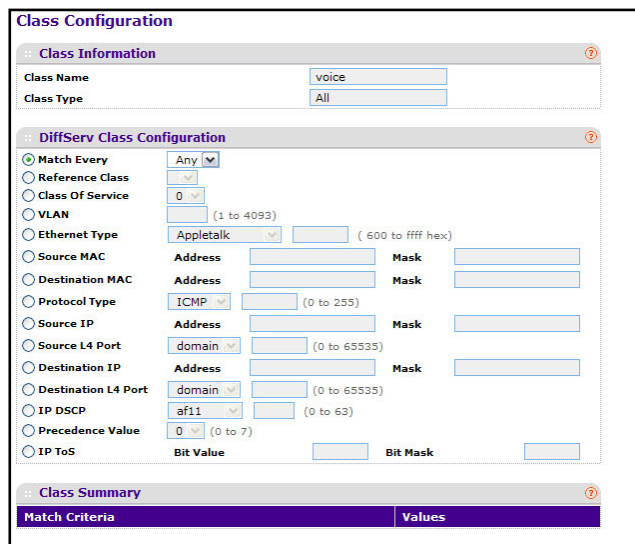
1. To create a new class, enter a class name, select the class type, and click **Add**.
The switch supports only the Class Type value All, which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria.
2. To rename an existing class, select the check box next to the configured class, update the name, and click **Apply**.
3. To remove a class, click the check box beside the Class Name, then click **Delete**.
4. Click **Refresh** to refresh the page with the most current data from the switch.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch. After creating a Class, click the class link to the Class page.

To configure the class match criteria:

1. Click the class name for an existing class.



The class name is a hyperlink. The following figure shows the configuration fields for the class.



2. Define the criteria to associate with a DiffServ class:
 - **Match Every.** This adds to the specified class definition a match condition whereby all packets are considered to belong to the class. If you select this field, no other fields are configurable.
 - **Reference Class.** Selects a class to start referencing for criteria. A specified class can reference at most one other class of the same type.

- **Class of Service.** Select the field and enter a class of service 802.1p user priority value to be matched for the packets. The valid range is 0–7.
- **VLAN.** Select the field and enter a VLAN ID to be matched for packets. The VLAN ID range is 1–4093.
- **Ethernet Type.** Select the EtherType field to compare the match criteria against the value in the header of an Ethernet frame. Select an EtherType keyword or enter an EtherType value to specify the match criteria. If you specify the EtherType value, select User Value from the menu and enter a custom protocol identifier to which packets are matched. The value is a four-digit hexadecimal number in the range of 0600–FFFF.
- **Source MAC.** Select this field and enter the source MAC address to compare against an Ethernet frame.
- **Source MAC Mask.** Enter the source MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame. An f indicates that the address bit is significant, and a 0 indicates that the address bit is to be ignored. A MAC mask of ff:ff:ff:ff:ff:ff matches a single MAC address.
- **Destination MAC.** Select this field and enter the destination MAC address to compare against an Ethernet frame.
- **Destination MAC Mask.** Enter the destination MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame. An f indicates that the address bit is significant, and a 0 indicates that the address bit is to be ignored. A MAC mask of ff:ff:ff:ff:ff:ff matches a single MAC address.
- **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.
- **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. 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.

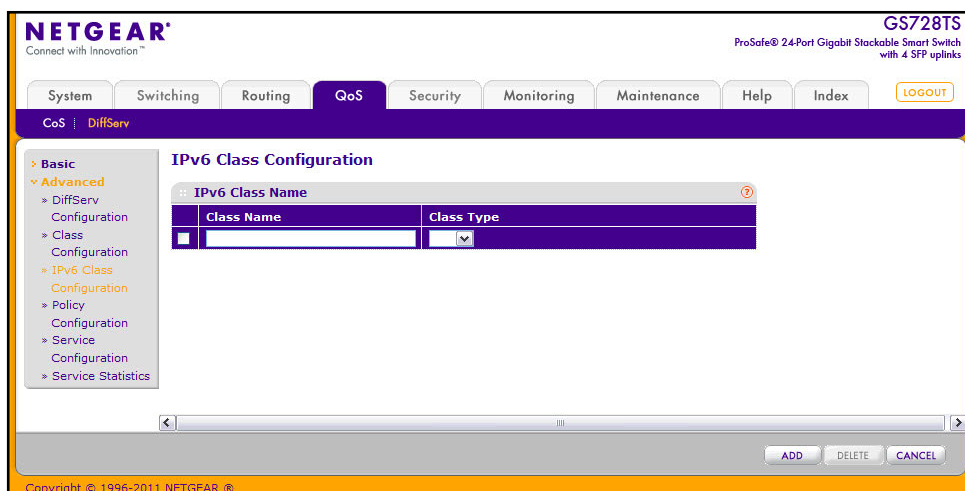
- **IP DSCP.** Matches the packet's DSCP to the class criteria's when selected. Select the DSCP type from the menu or enter a DSCP value to match. If you select Other, enter a custom value in the DSCP Value field that appears.
 - **IP Precedence.** Matches the packet's IP Precedence value to the class 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.
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 occur immediately.
 5. Click **Refresh** to refresh the page with the most current data from the switch.

IPv6 Class Configuration

The IPv6 Class Configuration feature extends the existing DiffServ functionality by providing support for IPv6 packet classification. An Ethernet IPv6 packet is distinguished from an IPv4 packet by its unique EtherType value, so all IPv6 classifiers include the EtherType field.

Packets that match an IPv6 classifier are only allowed to be marked using the 802.1p (COS) field or the IP DSCP field in the Traffic Class octet. IP Precedence is not defined for IPv6: this is not an appropriate type of packet marking.

To display the page, click **QoS > DiffServ > Advanced > IPv6 Class Configuration**.



To configure an IPv6 DiffServ class:

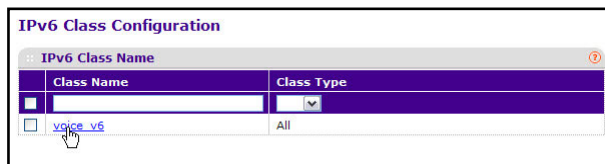
1. To create a new class, enter a class name, select the class type, and click **Add**.

The switch 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.

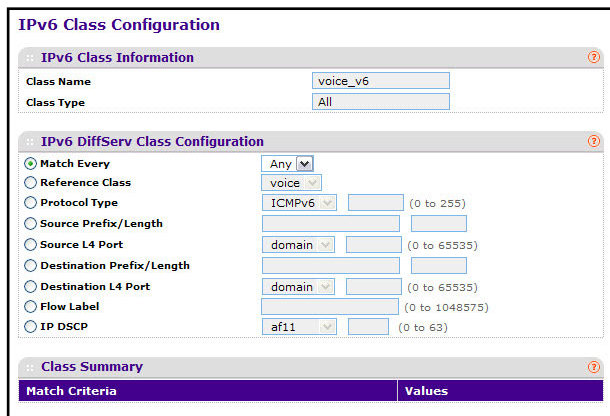
2. To rename an existing class, select the check box next to the configured class, update the name, and click **Apply**.
3. To remove a class, click the check box beside the Class Name, then click **Delete**.
4. Click **Refresh** to refresh the page with the most current data from the switch.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch. After creating a Class, click the class link to the Class page.

To configure the class match criteria:

1. Click the class name for an existing class.



The class name is a hyperlink. The following figure shows the configuration fields for the class.



2. Define the criteria to associate with a DiffServ class:

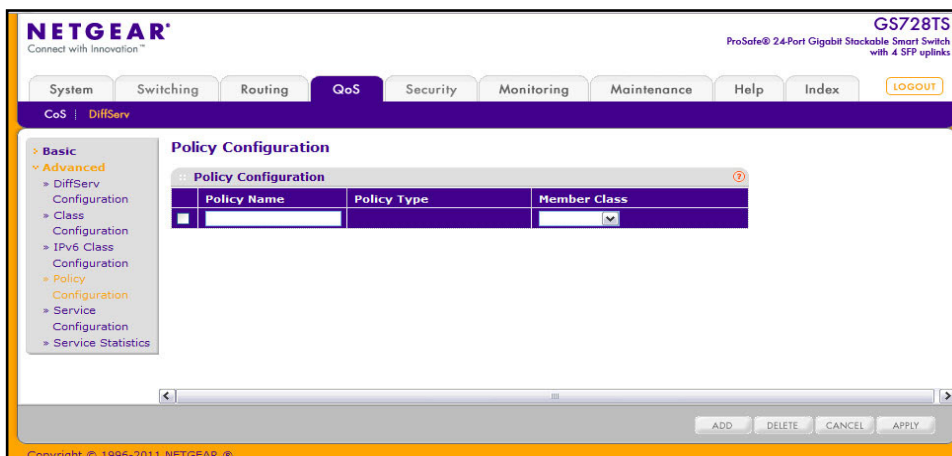
- **Match Every.** This adds to the specified class definition a match condition whereby all packets are considered to belong to the class. If you select this field, no other fields are configurable.
- **Reference Class.** Selects a class to start referencing for criteria. A specified class can reference at most one other class of the same type.
- **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.

- **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 Prefix/Length.** Enter a valid source IPv6 prefix to compare against an IPv6 packet. The prefix is always specified with the prefix length. The prefix can be in the range of ::0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. The prefix length range is 0–128.
 - **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 Prefix/Length.** Requires a packet's destination IPv6 prefix and length matches the address listed here. The prefix can be in the range of ::0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. The prefix length range is 0–128.
 - **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.
 - **Flow Label.** This is a 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify QoS handling in routers. The range is 0 to 1048575.
 - **IP DSCP.** Matches the packet's DSCP to the class criteria's when selected. Select the DSCP type from the menu or enter a DSCP value to match. If you select Other, enter a custom value in the DSCP Value field that appears.
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 occur immediately.
 5. Click **Refresh** to refresh the page with the most current data from the switch.

Policy Configuration

Use the Policy Configuration page to associate a collection of classes with one or more policy statements. After creating a Policy, click the policy link to the Policy page.

To display the page, click **QoS > DiffServ > Advanced > Policy Configuration**.



To configure a DiffServ policy:

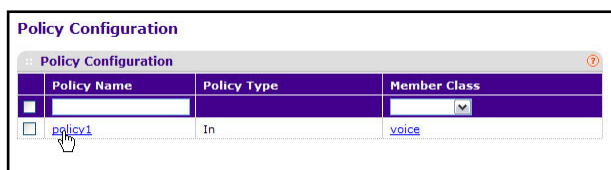
1. To create a new policy, enter a policy name in the Policy Selector field, select the existing DiffServ class to associate with the policy, and click **Add**.

The available policy type is In, which indicates the type is specific to inbound traffic. This field is not configurable.

2. To rename an existing policy or add a new member class to the policy, select the check box next to the configured class, update the fields, and click **Apply**.
3. To remove a policy, click the check box beside the policy, then click **Delete**.
4. Click **Refresh** to refresh the page with the most current data from the switch.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch. After creating a Class, click the class link to the Class page.

To configure the policy attributes:

1. Click the name of the policy.



The policy name is a hyperlink. The following figure shows the configuration fields for the policy.

Policy Class Configuration

Class Information

Policy Name: policy1
 Policy Type: In
 Member Class Name: voice

Policy Attribute

Policy Attribute: Assign Queue (0) | Drop | Mark VLAN CoS (0) | Mark IP Precedence (0) | Mark IP DSCP (af11) | Simple Policy

Color Mode: Color Blind

Committed Rate:
 Committed Burst Size:

Conform Action: Send | Drop | Mark CoS (0) | Mark IP Precedence (0) | Mark IP DSCP (af11) (10)

Violate Action: Send | Drop | Mark CoS (0) | Mark IP Precedence (0) | Mark IP DSCP (af11) (10)

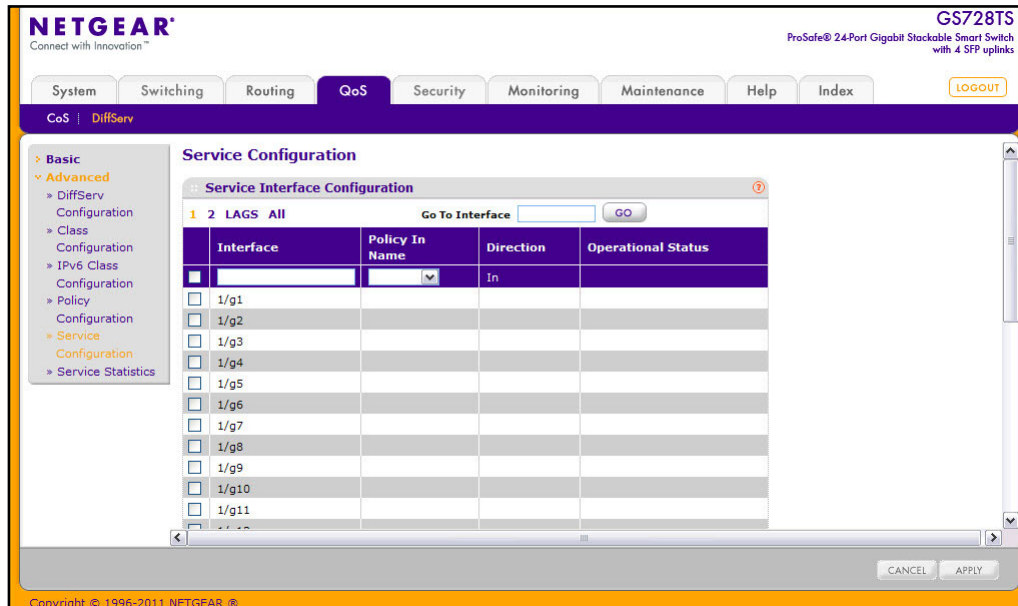
2. Select the queue to which packets of this policy-class will be assigned.
3. Configure the policy attributes:
 - **Drop.** Select this option to drop packets for this policy-class.
 - **Mark CoS.** Enter the specified Class of Service queue number to mark all packets for the associated traffic stream 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 0–7.
 - **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. If you select **Other**, enter a custom value in the **DSCP Value** field that appears.
 - **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: conform and violate.
4. If you select the Simple Policy attribute, you can configure the following 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).
 - **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 1–4294967295.
 - **Committed Burst Size.** The committed burst size is specified in kilobytes (KB) and is an integer from 1–128.

- **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.
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 change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
 7. Click **Refresh** to refresh the page with the most current data from the switch.

Service Configuration

Use the Service Configuration page to activate a policy on an interface.

To display the page, click **QoS > DiffServ > Advanced > Service Configuration**.



To configure DiffServ policy settings on an interface:

1. To configure DiffServ policy settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure DiffServ policy settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure DiffServ policy settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. To activate a policy for the selected interface(s) select the policy from the **Policy In** menu, and then click **Apply**.
6. To remove a policy from the selected interface(s) select None from the **Policy In** menu, and then click **Apply**.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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

The screenshot shows the Netgear web interface for a GS728TS switch. The 'QoS' tab is selected, and the 'DiffServ' sub-tab is active. The 'Service Statistics' page is displayed, showing a table with the following data:

Interface	Direction	Policy Name	Operational Status	Discarded Packets	Member Classes
1/g6	In	policy1	Down	0	voice
1/g7	In	policy1	Down	0	voice
1/g8	In	policy1	Down	0	voice

A 'REFRESH' button is located at the bottom right of the table area.

The following table describes the information available on the Service Statistics page.

Field	Description
Interface	Displays the interface for which service statistics are to display.
Direction	Displays the direction of packets for which service statistics display, which is always <i>In</i> .
Policy Name	Displays the policy associated with the selected interface.
Operational Status	Displays the operational status of this service interface, which is either Up or Down.
Discarded Packets	Displays 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.

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

Managing Device Security

6

Use the features available from the Security tab to configure management security settings for port, user, and server security. The Security tab contains links to the following features:

- [Management Security Settings](#) on page 197
- [Configuring Management Access](#) on page 210
- [Port Authentication](#) on page 218
- [Traffic Control](#) on page 225
- [Configuring Access Control Lists](#) on page 234

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 198
- [RADIUS Configuration](#) on page 199
- [Configuring TACACS+](#) on page 204
- [Authentication List Configuration](#) on page 207

Change Password

Use the page to change the login password. To display the page, click **Security > Management Security > User Configuration > Change Password**.

The screenshot shows the Netgear web interface for a GS752TPS switch. The navigation menu includes System, Switching, Routing, QoS, Security (selected), Monitoring, Maintenance, Help, and Index. The breadcrumb trail is Management Security > Access > Port Authentication > Traffic Control > ACL. The left sidebar shows User Configuration > Change Password selected. The main content area is titled 'Change Password' and contains a form with the following fields:

- Old Password (1 to 20)
- New Password (1 to 20)
- Confirm Password (1 to 20)
- Reset Password (checkbox)

At the bottom of the form are buttons for REFRESH, CANCEL, and APPLY. The footer of the page reads 'Copyright © 1996-2011 NETGEAR'.

To change the login password for the management interface:

1. Specify the current password in the Old Password. The entered password will be displayed in asterisks (*). Passwords are 1–20 alphanumeric characters in length and are case sensitive.
2. Enter the new password. It will not display as it is typed, and only asterisks (*) will show on the screen. Passwords are 1–20 alphanumeric characters in length and are case sensitive.
3. To confirm the password, enter it again to make sure you entered it correctly. This field will not display, but will show asterisks (*).
4. Use the Reset Password field to reset the password to the default value.
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.
7. Click **Refresh** to update the screen with the current information.

Note: In the case of a lost password, press the Factory Default Reset button on the front panel for more than one second to restore the factory default. The reset button will only reboot the device.

RADIUS Configuration

RADIUS servers provide additional security for networks. The RADIUS server maintains a user database, which contains per-user authentication information. The switch passes information to the configured RADIUS server, which can authenticate a user name and password before authorizing use of the network. RADIUS servers provide a centralized authentication method for:

- Web Access
- Access Control Port (802.1X)

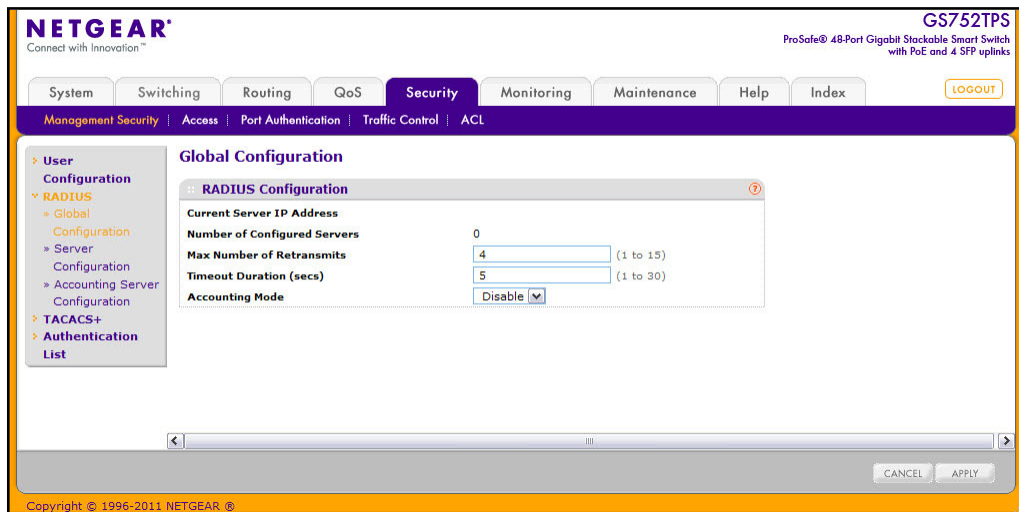
The RADIUS folder contains links to the following features:

- [Global Configuration](#) on page 199
- [RADIUS Server Configuration](#) on page 201
- [Accounting Server Configuration](#) on page 203

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, click **Security > Management Security > RADIUS > Global Configuration**.



The Current Server IP Address field is blank if no servers are configured (see [RADIUS Server Configuration](#) on page 201). The switch supports up to three configured RADIUS servers. 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.

To configure global RADIUS server settings:

1. In the **Max Number of Retransmits** field, specify the value of the maximum number of times a request packet is retransmitted to the RADIUS server.

Consideration to maximum delay time should be given when configuring RADIUS max retransmit 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.

2. In the **Timeout Duration** field, specify the timeout value, in seconds, for request retransmissions.

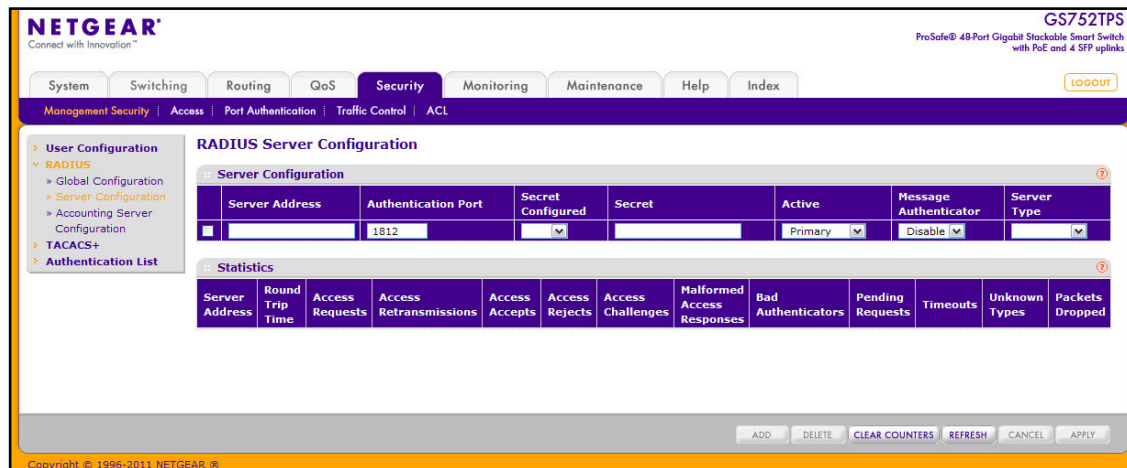
Consideration to maximum delay time should be given when configuring RADIUS max retransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value 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.

3. From the **Accounting Mode** menu, select whether the RADIUS accounting mode is enabled or disabled on the current server.
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.

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



To configure a RADIUS server:

- To add a RADIUS server, specify the settings the following list describes, and click **Add**.
 - In the **Server Address** field, specify the IP address of the RADIUS server to add.
 - In the **Authentication Port** field, specify the UDP port number the server uses to verify the RADIUS server authentication. The valid range is 0–65535.
 - From the **Secret Configured** menu, select Yes to add a RADIUS secret in the next field. You must select Yes before you can configure the RADIUS secret. After you add the RADIUS server, this field indicates whether the shared secret for this server has been configured.
 - In the **Secret** field, type the shared secret text string used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server. This secret must match the RADIUS encryption.
 - From the **Active** menu, specify whether the server is a Primary or Secondary server.
 - From the **Message Authenticator** menu, enable or disable the message authenticator attribute for the selected server.
 - From the **Server Type** menu, specify whether the authentication server is a NETGEAR product or Standard authentication server.
- To modify settings for a RADIUS server that is already configured on the switch, select the check box next to the server address, update the desired fields, and click **Apply**.
- Click **Refresh** to update the page with the most current information.
- To delete a configured RADIUS server, select the check box next to the server address, and then click **Delete**.

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

The following table describes the RADIUS server statistics available on the page.

Field	Description
Server Address	This displays all configured RADIUS servers.
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.
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.

Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear Counters** to clear the authentication server and RADIUS statistics to their default values.
- 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, click **Security** > **Management Security** > **RADIUS** > **Accounting Server Configuration**.

To configure the RADIUS accounting server:

1. In the **Accounting Server Address** field, specify the IP address of the RADIUS accounting server to add.
2. In the **Port** field, specify the UDP port number the server uses to verify the RADIUS accounting server authentication. The valid range is 0–65535.
3. From the **Secret Configured** menu, select Yes to add a RADIUS secret in the next field. You must select Yes before you can configure the RADIUS secret. After you add the RADIUS accounting server, this field indicates whether the shared secret for this server has been configured.
4. In the **Secret** field, type the shared secret to use with the specified accounting server.
5. From the **Accounting Mode** menu, enable or disable the RADIUS accounting mode.
6. Click **Apply** to update the switch with the RADIUS Accounting server settings.
7. To delete a configured RADIUS Accounting server, click **Delete**.
8. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The following table describes RADIUS accounting server statistics available on the page.

Field	Description
Accounting Server Address	Displays the IP address of the supported RADIUS accounting server.
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.

Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear Counters** to reset all statistics to their default value.
- 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. When 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.

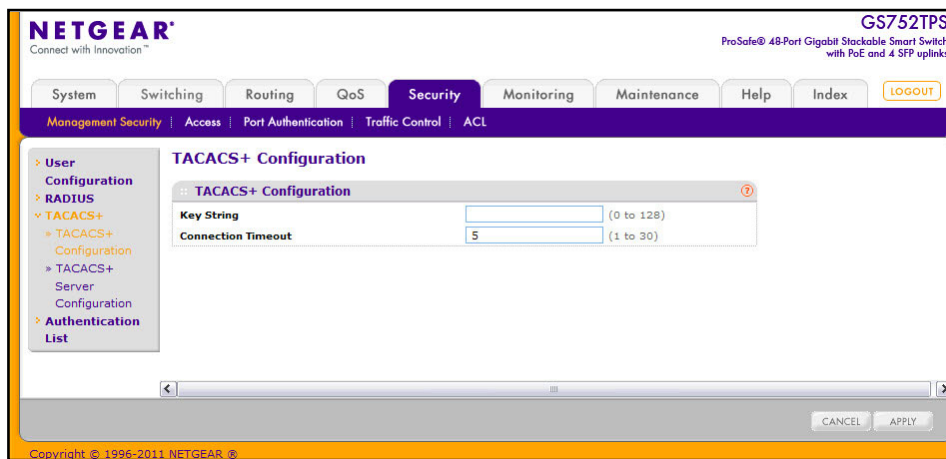
The TACACS+ folder contains links to the following features:

- [Configuring TACACS+](#) on page 204
- [TACACS+ Server Configuration](#) on page 206

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



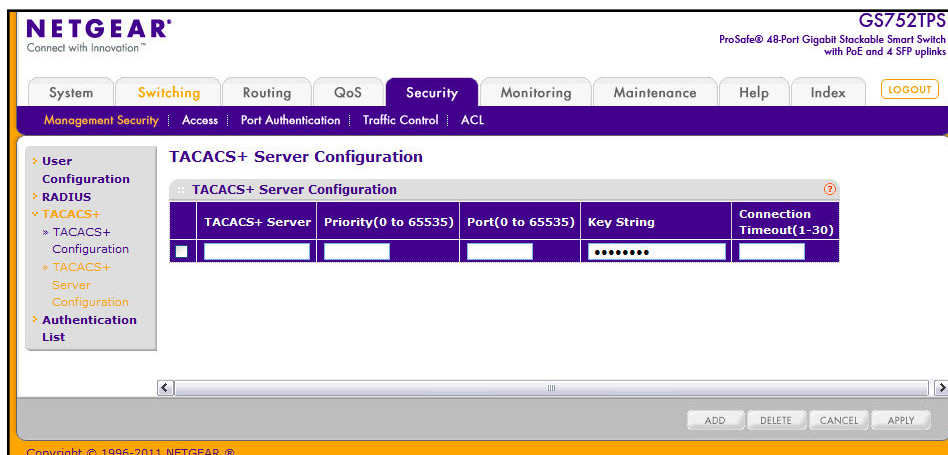
To configure global TACACS+ settings:

1. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the GS728TS, GS728TPS, GS752TS, or GS752TPS and the TACACS+ server. The valid range is 0–128 characters. The key must match the key configured on the TACACS+ server.
2. In the **Connection Timeout** field, specify the maximum number of seconds allowed to establish a TCP connection between the GS728TS, GS728TPS, GS752TS, or GS752TPS and the TACACS+ server. The valid range is 1–30 seconds.
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 the page, click **Apply** to apply the new settings to the system.

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



To configure TACACS+ server settings:

1. To add a new TACACS+ server, enter its IP address or hostname in the **TACACS+ Server** field.
2. In the **Priority** field, specify the order in which the TACACS+ servers are used. A value of 0 is the highest priority.
3. In the **Port** field, specify the authentication port number through which the TACACS+ session occurs. The default is port 49, and the range is 0–65535.
4. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server. This key must match the encryption used on the TACACS+ server. The valid range is 0–128 characters.
5. In the **Connection Timeout** field, specify 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.
6. If you make changes to the page, or add a new entry, click **Apply** to apply the changes to the system.
7. To delete a configured TACACS+ server, select the check box associated with the server you want to remove, and then click **Delete**.
8. Click **Cancel** to abandon the changes.

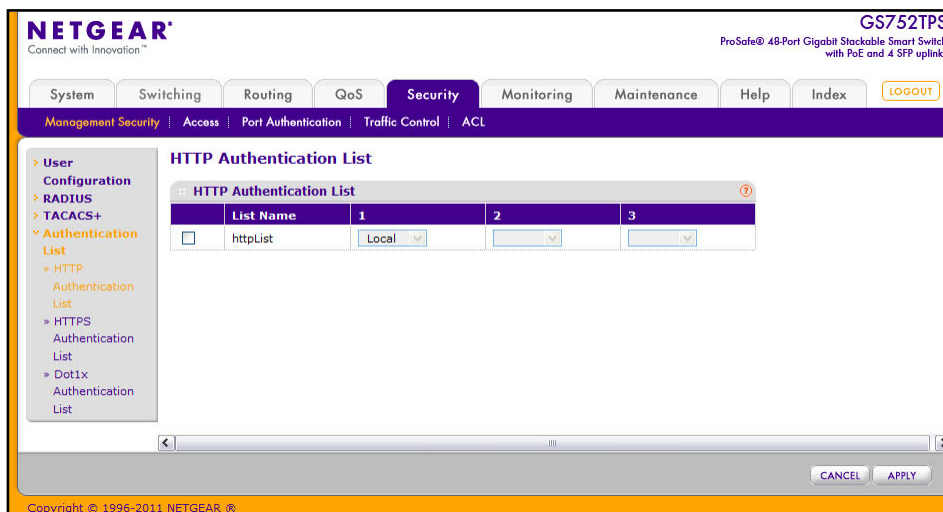
Authentication List Configuration

From the Authentication List pages, you can configure the login lists for HTTP, HTTPS, or IEEE 802.1X authentication. A login list specifies one or more authentication methods to validate switch or port access.

HTTP Authentication List

Use the HTTP Authentication List page to configure the authentication method(s) the **admin** user must use when accessing the management interface through HTTP.

To access the HTTP Authentication List page, click **Security > Management Security > Authentication List**, and then click the **HTTP Authentication List** link.



To change the authentication method for the httpList:

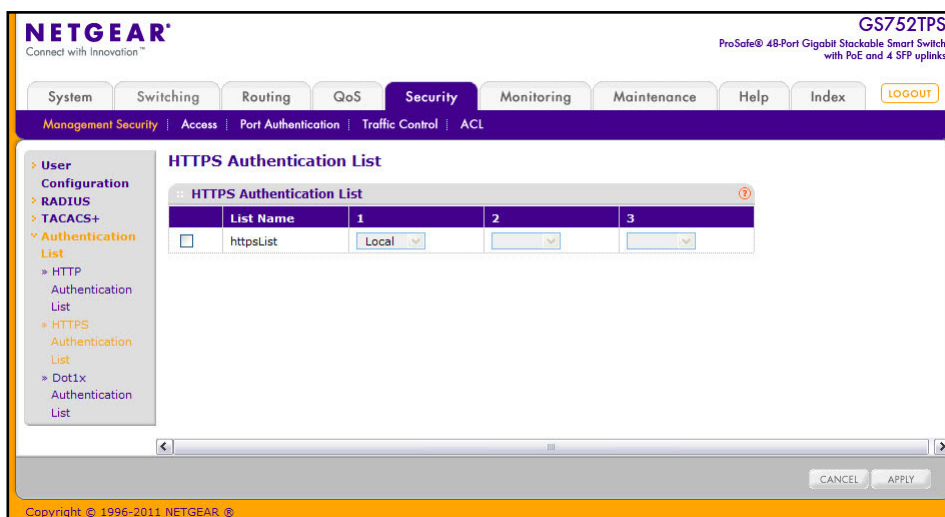
1. Select the check box next to the httpList name
2. Use the drop down menu in the 1 column to select the authentication method that should appear first in the selected authentication login list. If you select a method that does not time out as the first method, such as 'local', no other method will be tried, even if you have specified more than one method. 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.

3. Use the menu in the **2** column 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. This parameter will not appear when you first create a new login list.
4. Use the menu in the **3** column to select the authentication method, if any, that should appear third in the selected authentication login list. This parameter will not appear when you first create a new login list.
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.

HTTPS Authentication List

Use the HTTPS Authentication List page to configure the authentication method(s) the **admin** user must use when accessing the management interface through secure HTTP (HTTPS).

To access the HTTPS Authentication List page, click **Security > Management Security > Authentication List**, and then click the **HTTPS Authentication List** link.



To change the authentication method for the httpsList:

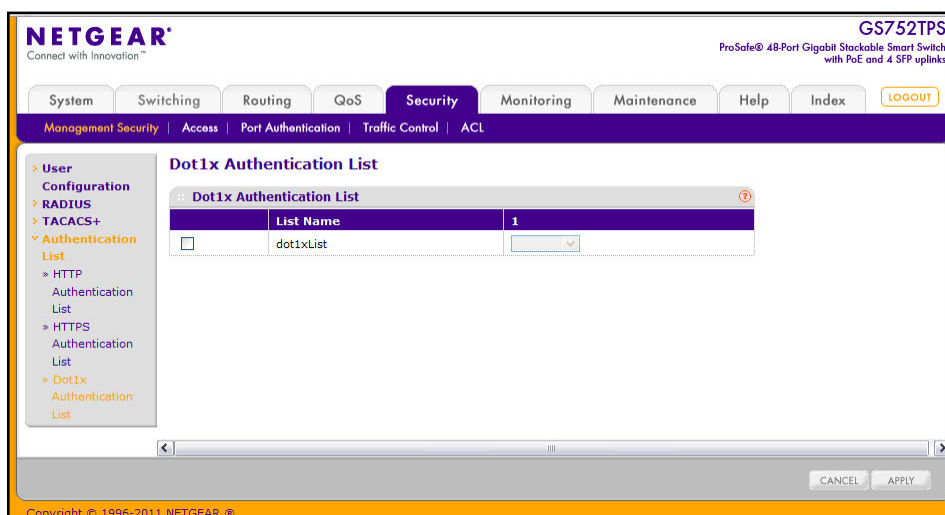
1. Select the check box next to the httpsList name
2. Use the drop down menu in the **1** column to select the authentication method that should appear first in the selected authentication login list. If you select a method that does not time out as the first method, such as 'local', no other method will be tried, even if you have specified more than one method. 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.
3. Use the menu in the **2** column 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. This parameter will not appear when you first create a new login list.
 4. Use the menu in the **3** column to select the authentication method, if any, that should appear third in the selected authentication login list. This parameter will not appear when you first create a new login list.
 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.

Dot1x Authentication List

Use the Dot1x Authentication List page to configure the authentication method(s) a host connected to a switch port must use when attempting to access the network.

To access the Dot1x Authentication List page, click **Security > Management Security > Authentication List**, and then click the **Dot1x Authentication List** link.



To change the authentication method for the dot1xList:

1. Select the check box next to the dot1xList name

2. Use the drop down menu in the **1** column 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. The 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.
 - **None:** The authentication method is unspecified. This option is only available for Method 2 and Method 3.
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.

Configuring Management Access

From the Access page, you can configure HTTP and Secure HTTP access to the GS728TS, GS728TPS, GS752TS, or GS752TPS management interface. You can also configure Access Control Profiles and Access Rules.

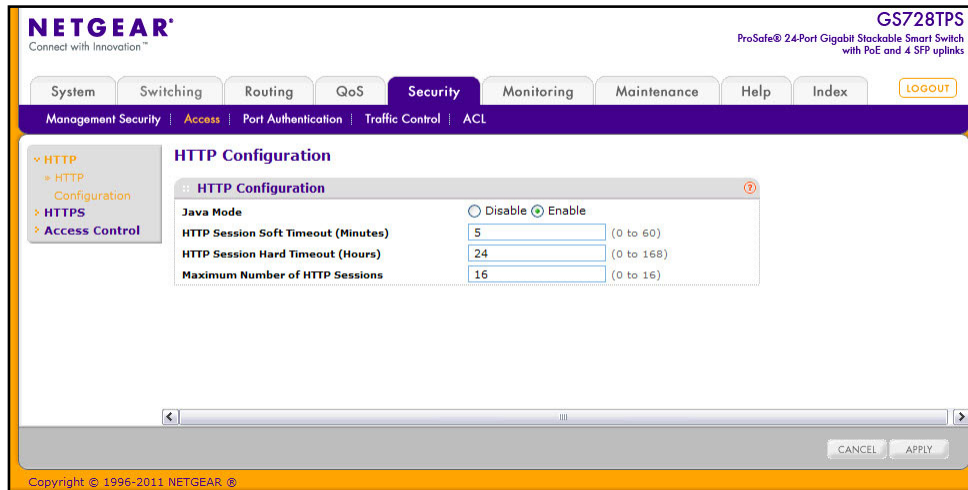
The **Security > Access** tab contains the following folders:

- [HTTP Configuration](#) on page 211
- [Secure HTTP Configuration](#) on page 212
- [Certificate Download](#) on page 214
- [Access Profile Configuration](#) on page 215
- [Access Rule Configuration](#) on page 217

HTTP Configuration

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

To access the HTTP Configuration page, click **Security > Access**, and then click the **HTTP > HTTP Configuration** link.



To configure the HTTP server settings:

1. 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.
2. In the **HTTP Session Soft Timeout** field, specify the number of minutes an HTTP session can be idle before a timeout occurs.

After the session is inactive for the configured amount of time, the administrator is automatically logged out and must re-enter the password to access the management interface. 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.

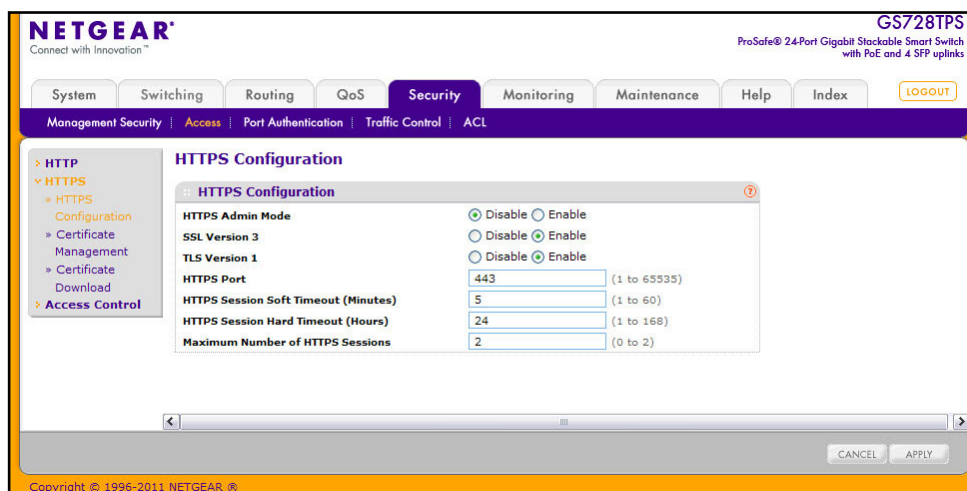
3. In the **HTTP Session Hard Timeout** field, specify the hard timeout for HTTP sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (0–168) hours. A value of zero corresponds to an infinite timeout. The default value is 24 hours. The currently configured value is shown when the Web page is displayed.
4. In the **Maximum Number of HTTP Sessions** field, specify the maximum number of HTTP sessions that can exist at the same time. The value must be in the range of (0–16). The default value is 16. The currently configured value is shown when the Web page is displayed.
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.

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



To configure HTTPS settings:

1. Use the radio buttons in the **HTTPS Admin Mode** field to enable or disable 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.
2. Use the radio buttons in the **SSL Version 3** field to enable or disable Secure Sockets Layer Version 3.0. The currently configured value is shown when the Web page is displayed. The default value is Enable.
3. Use the radio buttons in the **TLS Version 1** field to enable or disable Transport Layer Security Version 1.0. The currently configured value is shown when the Web page is displayed. The default value is Enable.
4. In the **HTTPS Port** field, specify the TCP port to use for HTTPS data. The value must be in the range of 1–65535. Port 443 is the default value. The currently configured value is shown when the Web page is displayed.
5. In the **HTTPS Session Soft Timeout** field, specify the number of minutes an HTTPS session can be idle before a timeout occurs.

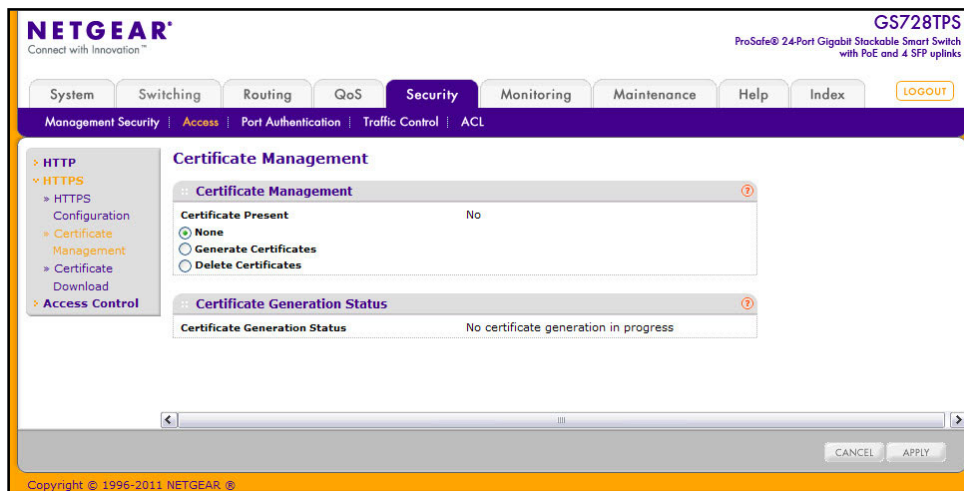
After the session is inactive for the configured amount of time, the administrator is automatically logged out and must re-enter the password to access the management interface. A value of zero corresponds to an infinite timeout. The default value is 5 minutes. The currently configured value is shown when the Web page is displayed.

6. In the **HTTPS Session Hard Timeout** field, specify the number of hours an HTTPS session can remain active, regardless of session activity. The value must be in the range of (1–168) hours. The default value is 24 hours. The currently configured value is shown when the Web page is displayed.
7. In the **Maximum Number of HTTPS Sessions** field, specify the maximum number of HTTPS sessions that can be open at the same time. The value must be in the range of (0–2). The default value is 2. The currently configured value is shown when the Web page is displayed.
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 make changes to the page, click **Apply** to apply the changes to the system.

Certificate Management

Use this menu to generate or delete certificates.

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



1. The **Certificate Present** field indicates whether an SSL certificate exists on the switch. A status of Yes means that a certificate is present, while No means that no certificate exists.
2. To generate a certificate file, select **Generate Certificates** and click **Apply**.
The **Certificate Generation Status** field displays whether SSL certificate generation is in progress.
3. To delete the certificate file from the system, select **Delete Certificates** and click **Apply**.

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

Certificate Download

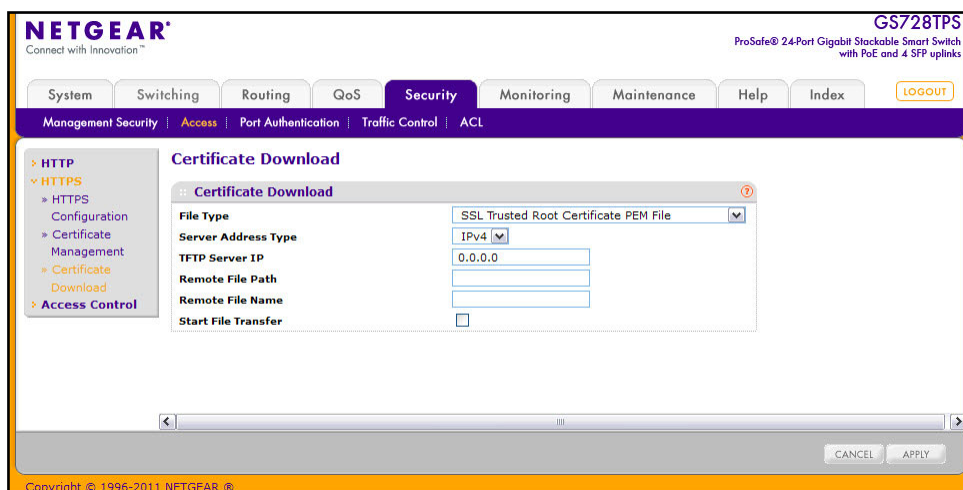
For the Web server on the switch to accept HTTPS connections from a management station, the Web server needs a public key certificate. You can generate a certificate externally (for example, off-line) and download it to the switch.

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.



To configure the certificate download settings for HTTPS sessions:

1. From the **File Type** menu, 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).
2. In the **Server Address Type** field, specify whether the address of the TFTP server is an IPv4 address or a DNS hostname.

3. In the **TFTP Server IP** field, specify the address of the TFTP server. The address can be an IP address in standard x.x.x.x format or a hostname. The hostname must start with a letter of the alphabet. Make sure that the software image or other file to be downloaded is available on the TFTP server.
4. In the **Remote File Path** field, specify the path on the TFTP server where the file is located. You may enter up to 96 characters.
5. In the **Remote File Name** field, specify the name of the file to download. You may enter up to 32 characters.
6. Select the **Start File Transfer** check box.
7. Click **Apply** to start the transfer. A status message displays during the transfer and upon successful completion of the transfer.
8. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Access Profile Configuration

Use the Access Profile Configuration page to configure settings that control management access to the switch. Access profile configuration requires three steps:

1. Use the Access Profile Configuration page to create an access profile. To add rules to the profile, the access profile must be deactivated, which is the default setting.
2. Use the Access Rule Configuration page to add one or more access rules to the profile.
3. Return to the Access Profile Configuration page to activate the profile.

To access the Access Profile Configuration page, click **Security > Access**, and then click the **Access Control > Access Profile Configuration** link.

The screenshot shows the Netgear web interface for a GS728TPS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Security menu is expanded to show Management Security, Access, Port Authentication, Traffic Control, and ACL. The Access menu is further expanded to show HTTP, HTTPS, Access Control, and Configuration. The Access Control menu is expanded to show Access Profile Configuration, Access Rule Configuration, and Configuration. The main configuration area is titled 'Access Profile Configuration' and contains the following fields:

- Access Profile Name: admin_host
- Activate Profile:
- Deactivate Profile:
- Remove Profile:

Below the configuration fields is a 'Profile Summary' table:

Rule Type	Service Type	Source IP Address	Mask	Priority
Permit	HTTP	192.168.2.165	255.255.255.0	1

At the bottom of the page are buttons for REFRESH, CANCEL, and APPLY. The footer of the page reads 'Copyright © 1996-2011 NETGEAR'.

To configure an Access Profile:

1. In the **Access Profile Name** field, specify the name of the access profile to be added. The maximum length is 32 characters.
2. To activate an access profile, select the **Activate Profile** check box. You cannot add rules to an active profile.
3. To deactivate an access profile, select the **Deactivate Profile** check box.
4. To remove an access profile, select the **Remove Profile** check box. The access profile should be deactivated before removing the access profile.
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.

The Profile Summary table shows the rules that are configured for the profile, as the following table describes.

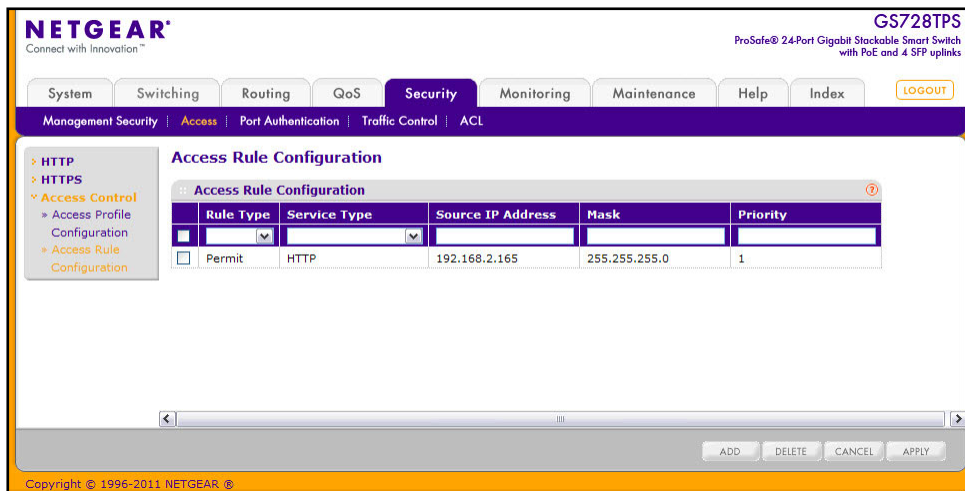
Field	Description
Rule Type	Identifies the action the rule takes, which is either Permit or Deny.
Service Type	Displays the type of service to allow or prohibit from accessing the switch management interface: <ul style="list-style-type: none"> • SNMP • HTTP • HTTPS
Source IP Address	Displays the IP Address of the client that may or may not originate management traffic.
Mask	Displays the subnet mask associated with the IP address.
Priority	Displays 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.

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

Access Rule Configuration

Use the Access Rule Configuration page to configure the rules about what systems can access the GS728TS, GS728TPS, GS752TS, or GS752TPS Web interface and what protocols are allowed.

To access the Access Rule Configuration page, click **Security > Access**, and then click the **Access Control > Access Rule Configuration** link.



Before you create access rules, make sure:

- An access profile exists.
- The access profile is deactivated.

To configure access profile rules:

1. To add an access profile rule, configure the following settings and click **Add**.
 - **Rule Type:** Specify whether the rule permits or denies access to the GS728TS, GS728TPS, GS752TS, or GS752TPS management interface.
 - Select **Permit** to allow access to the management interface 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 management interface 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. Unlike MAC ACLs and IP ACLs, there is no implied *deny all* rule at the end of the rule list.
 - **Service Type.** Select the type of service to allow or prohibit from accessing the switch management interface:
 - SNMP
 - HTTP
 - HTTPS

- **Source IP Address.** Specify the IP Address of the client originating the management traffic.
 - **Mask.** Specify the subnet mask associated with the IP address. The subnet mask is a standard subnet mask, and *not* an inverse (wildcard) mask that you use with IP ACLs.
 - **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 modify an access rule, select the check box next to the Rule Type, update the desired settings, and click **Apply**
 3. To delete an access rule, select the check box next to the Rule Type, 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.

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.

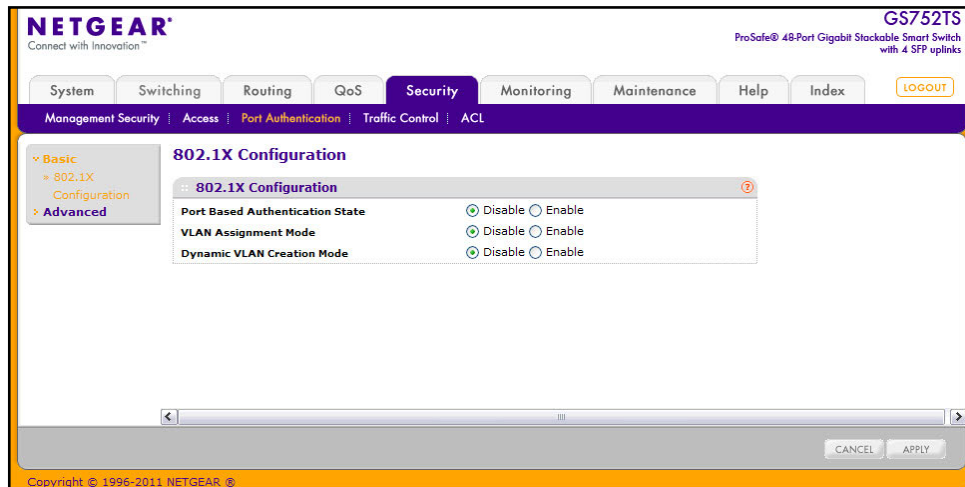
From the Port Authentication link, you can access the following pages:

- Basic:
 - [802.1X Configuration](#) on page 219
- Advanced:
 - [Port Authentication](#) on page 220
 - [Port Summary](#) on page 224

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, click **Security > Port Authentication > Basic > 802.1X Configuration**.



To configure global 802.1X settings:

1. Select the appropriate radio button in the **Port Based Authentication State** field to enable or disable 802.1X administrative mode on the switch.
 - **Enable.** Port-based authentication is permitted on the switch.

Note: If 802.1X is enabled, authentication is performed by a RADIUS server. This means the primary authentication method must be RADIUS. To set the method, go to **Security > Management Security > Dot1x Authentication List** and select RADIUS as method 1 for dot1xList. For more information, see [Authentication List Configuration](#) on page 207.

- **Disable.** The switch does not check for 802.1X authentication before allowing traffic on any ports, even if the ports are configured to allow only authenticated users.
2. Enable or disable the **VLAN Assignment** mode:
 - **Enable.** Allow a RADIUS server to assign the VLAN ID to authenticated supplicants.
 - **Disable.** The RADIUS server can not assign authenticated clients to VLANs.

3. Enable or disable **Dynamic VLAN Creation Mode**:

- **Enable.** If the RADIUS assigned VLAN does not exist on the switch, allow the switch to dynamically create the assigned VLAN.
- **Disable.** The switch will not create a RADIUS-assigned VLAN for a client if it does not already exist.

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 settings, click **Apply** to apply the new settings to the system.

Port Authentication

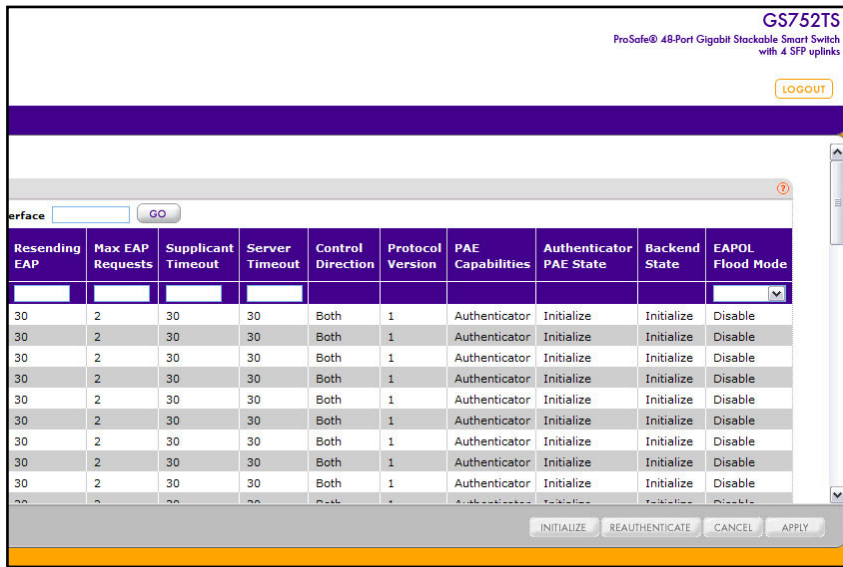
Use the Port Authentication page to enable and configure port access control on one or more ports.

To access the Port Authentication page, 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. The following screen shots show the left and right halves of the Port Authentication page.

The screenshot shows the NETGEAR web interface for Port Authentication configuration. The navigation menu includes System, Switching, Routing, QoS, Security (selected), Monitoring, Maintenance, Help, and Index. The breadcrumb trail is Management Security > Access > Port Authentication > Traffic Control > ACL. The left sidebar shows a tree view with 'Basic' expanded and 'Port Authentication' selected. The main content area is titled 'Port Authentication' and contains a table with the following data:

Port	Port Control	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID	Periodic Reauthentication	Reauthentication Period	Quiet Period
<input type="checkbox"/> 1/g1	Auto	0	90	0	Disable	3600	60
<input type="checkbox"/> 1/g2	Auto	0	90	0	Disable	3600	60
<input type="checkbox"/> 1/g3	Auto	0	90	0	Disable	3600	60
<input type="checkbox"/> 1/g4	Auto	0	90	0	Disable	3600	60
<input type="checkbox"/> 1/g5	Auto	0	90	0	Disable	3600	60
<input type="checkbox"/> 1/g6	Auto	0	90	0	Disable	3600	60
<input type="checkbox"/> 1/g7	Auto	0	90	0	Disable	3600	60
<input type="checkbox"/> 1/g8	Auto	0	90	0	Disable	3600	60
<input type="checkbox"/> 1/g9	Auto	0	90	0	Disable	3600	60



To configure 802.1X settings for the port:

1. Select the check box next to the port to configure. You can also select multiple check boxes to apply the same settings to the select ports, or select the check box in the heading row to apply the same settings to all ports.
2. For the selected port(s), specify the following settings:
 - **Port Control.** Defines the port authorization state. The control mode is set only 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.
 - MAC Based: MAC-based authentication allows multiple supplicants connected to the same port to each authenticate individually.
 - **Guest VLAN ID.** Specify the VLAN ID for the Guest VLAN on the interface. Users who connect to the switch through this interface and do not attempt to authenticate might be placed on the guest VLAN. The valid range is 0–4093. 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 Guest VLAN Authentication. The Guest VLAN timeout must be a value in the range of 1–300. The default value is 90.
 - **Unauthenticated VLAN ID.** Specify the VLAN ID for the Unauthenticated VLAN. Users who fail the 802.1X authentication might be placed on a VLAN for unauthenticated clients that has limited network access.

- **Periodic Reauthentication.** Use this field to enable or disable reauthentication of the supplicant for the specified port. Select 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.** 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.** 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 1–65535. The default value is 30. Changing the value will not change the configuration until you click the Apply button.
- **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/Identify before timing out the supplicant. The maximum requests value must be in the range of 1–10. The default value is 2. Changing the value will not change the configuration until you click the Apply button.
- **Supplicant Timeout.** 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.** 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, which is always Both. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator. The unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames). This field is not configurable.
- **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
 - **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.
3. Click **Apply** to send the updated screen to the switch and cause the changes to occur on the switch and the changes will be saved.
 4. Click **Initialize** to begin the initialization sequence on the selected port(s). This button is only selectable if the control mode is *auto*. If the button is not selectable, it will be grayed out. When this button is clicked, the action is immediate. It is not required to click **Apply** for the action to occur.
 5. 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. When this button is pressed, the action is immediate. It is not required to click **Apply** for the action to occur.
 6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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, click **Security > Port Authentication > Advanced > Port Summary**.

Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Port Status
1/g1	Auto	N/A	FALSE	N/A
1/g2	Auto	N/A	FALSE	N/A
1/g3	Auto	N/A	FALSE	N/A
1/g4	Auto	N/A	FALSE	N/A
1/g5	Auto	N/A	FALSE	N/A
1/g6	Auto	N/A	FALSE	N/A
1/g7	Auto	N/A	FALSE	N/A
1/g8	Auto	N/A	FALSE	N/A
1/g9	Auto	N/A	FALSE	N/A
1/g10	Auto	N/A	FALSE	N/A

The following table describes the fields on the Port Summary page.

Field	Description
Port	The port whose settings are displayed in the current table row.
Control Mode	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>This field indicates the control mode under which the port is actually operating. Possible values are:</p> <ul style="list-style-type: none"> • ForceUnauthorized • ForceAuthorized • Auto • N/A: If the port is in detached state it cannot participate in port access control.

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

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

Traffic Control

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

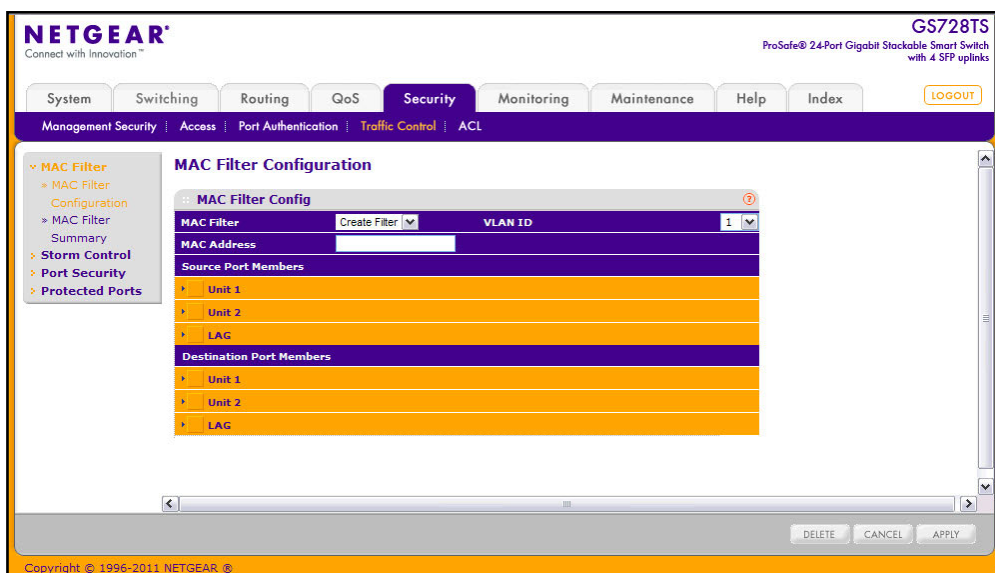
The Traffic Control folder contains links to the following features:

- MAC Filter:
 - [MAC Filter Configuration](#) on page 225
 - [MAC Filter Summary](#) on page 227
- [Storm Control](#) on page 228
- Port Security:
 - [Port Security Configuration](#) on page 230
 - [Port Security Interface Configuration](#) on page 231
 - [Security MAC Address](#) on page 232
- [Protected Ports Membership](#) on page 233

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, click **Security > Traffic Control > MAC Filter > MAC Filter Configuration**.



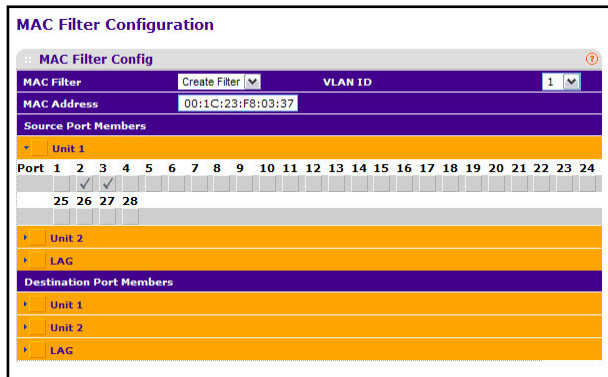
To configure MAC filter settings:

1. To configure a new MAC filter:

- a. Select **Create Filter** from the **MAC Filter** menu. If no filters have been configured, this is the only option available.
- b. From the **VLAN ID** menu, select the VLAN to use with the MAC address to fully identify packets you want filtered. You can change this field only when the **Create Filter** option is selected from the **MAC Filter** menu.
- c. In the **MAC Address** field, specify the MAC address of the filter in the format 00:01:1A:B2:53:4D. You can change this field when you have selected the **Create Filter** option.

You cannot define filters for the following MAC addresses:

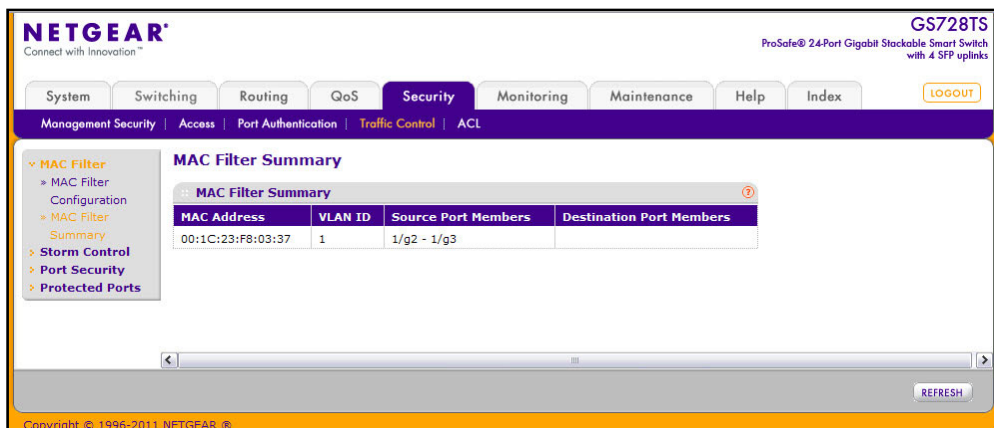
- 00:00:00:00:00:00
 - 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
 - 01:80:C2:00:00:20 to 01:80:C2:00:00:21
 - FF:FF:FF:FF:FF:FF
- d. Click the orange bar to display the available ports and select the port(s) to include in the inbound filter. If a packet with the MAC address and VLAN ID you specify is received on a port that is not in the list, it will be dropped. In the following image shows the configuration of a MAC filter on the MAC address 00:1C:23:F8:03:37 with ports g2 and g3 as source port members.



- e. Click the orange bar to display the available ports and select the port(s) you to include in the outbound filter. Packets with the MAC address and VLAN ID you selected will be transmitted only 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, click **Security > Traffic Control**, and then click the **MAC Filter > MAC Filter Summary** link.



The following table describes the information displayed on the page:

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	Displays the ports included in the inbound filter.
Destination Port Members	Displays the ports included in the outbound filter.

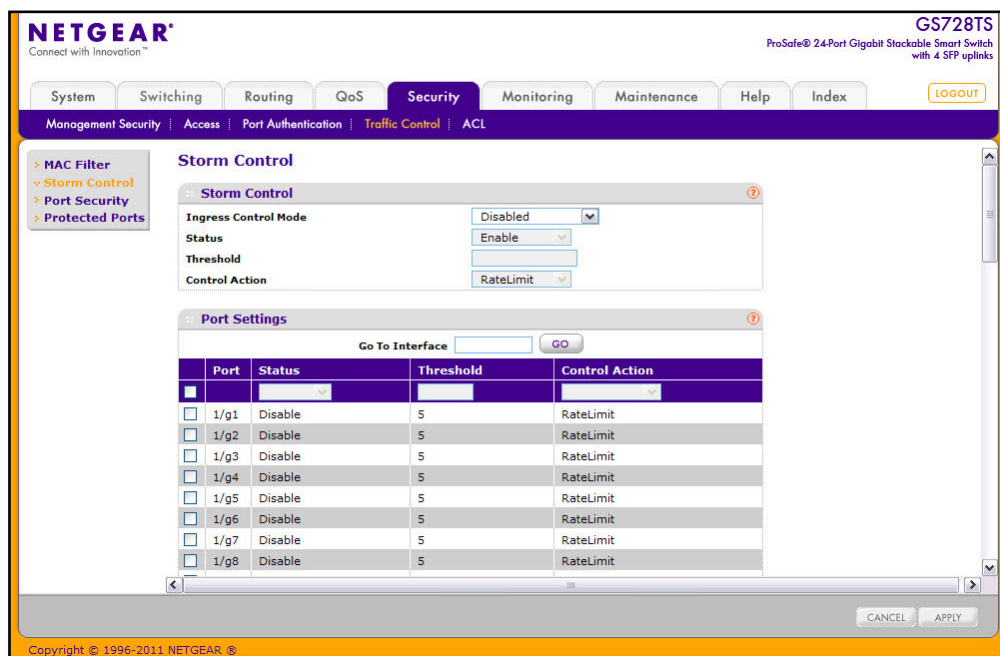
Click **Refresh** to update the page with the most current information.

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



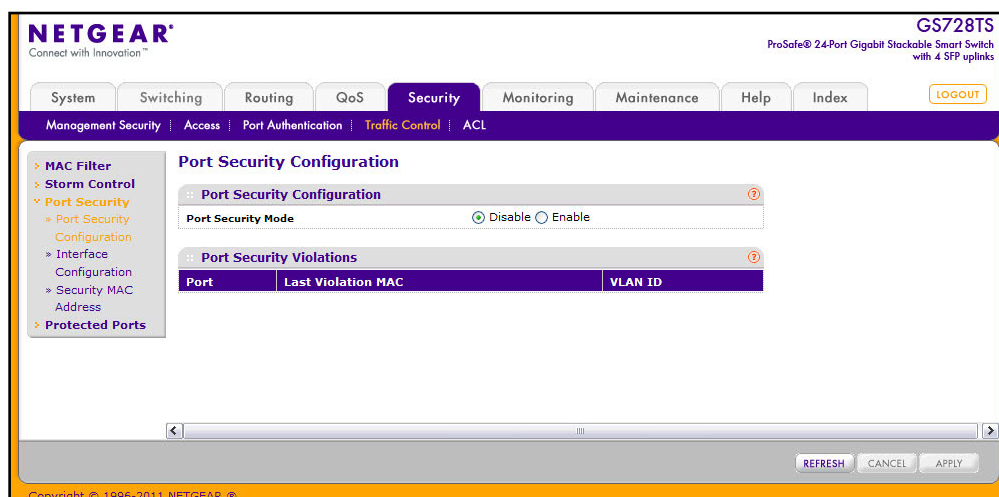
To configure storm control settings:

1. Select the check box next to the port to configure. Select multiple check boxes to apply the same setting to all selected ports. Select the check box in the heading row to apply the same settings to all ports.
2. From the Ingress Control Mode menu, 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.
3. In the **Threshold** field, specify the maximum rate at which unknown packets are forwarded. The range is a percent of the total threshold between 0–100%. The default is 5%.
4. In the **Control Action** field, determine the action to be taken when a broadcast storm is detected:
 - **RateLimit.** Limits the rate at which incoming traffic is forwarded.
 - **Shutdown.** Administratively disables the port when the ingress/incoming broadcast traffic reaches the configured threshold. If the port is shut down because the broadcast traffic exceeds the configured limit, you must manually reenabling it by using the **Switching > Ports > Port Configuration** page (see [Port Configuration](#) on page 102).
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.

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 an allowable source MAC addresses can be forwarded. All other packets are discarded.

To display the Port Security Configuration page, click **Security > Traffic Control**, and then click the **Port Security > Port Security Configuration** link.



To configure the global port security mode:

1. In the **Port Security Mode** field, select the appropriate radio button to enable or disable port security on the switch.
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 the mode, click **Apply** to apply the change to the system.

The Port Security Violation table shows information about violations that occurred on ports that are enabled for port security. The following table describes the fields in the Port Security Violation table.

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.

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

Port Security Interface Configuration

A MAC address can be defined as allowable by one of two methods: dynamically or statically. 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. When 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. 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, click **Security > Traffic Control**, and then click the **Port Security > Interface Configuration** link.

The screenshot shows the NETGEAR web interface for a GS728TS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Security menu is expanded to show Management Security, Access, Port Authentication, Traffic Control, and ACL. The Port Security > Interface Configuration page is displayed, showing a table of port security settings for various ports and LAGs.

Port	Port Security	Max Allowed Dynamically Learned MAC	Max Allowed Statically Locked MAC	Enable Violation Traps	
<input type="checkbox"/>	1/g1	Disable	600	20	No
<input type="checkbox"/>	1/g2	Disable	600	20	No
<input type="checkbox"/>	1/g3	Disable	600	20	No
<input type="checkbox"/>	1/g4	Disable	600	20	No
<input type="checkbox"/>	1/g5	Disable	600	20	No
<input type="checkbox"/>	1/g6	Disable	600	20	No
<input type="checkbox"/>	1/g7	Disable	600	20	No
<input type="checkbox"/>	1/g8	Disable	600	20	No

To configure port security settings:

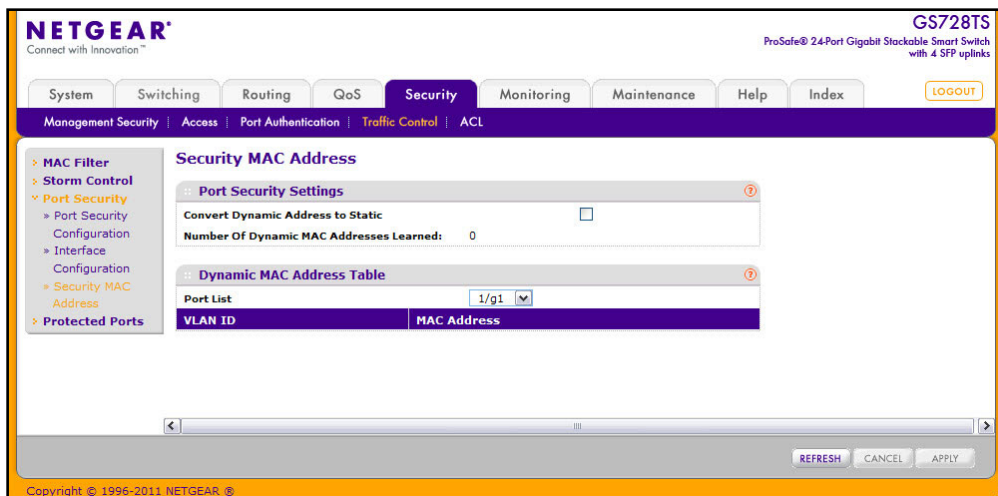
1. To configure port security settings for a physical port, click the unit ID number of the stack member with the ports to configure.
2. To configure port security settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure port security settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. Select multiple check boxes to apply the same setting to all selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

5. Specify the following settings:
 - **Port Security.** Enable or Disable the port security feature for the selected port.
 - **Max Allowed Dynamically Learned MAC.** Sets the maximum number of dynamically learned MAC addresses on the selected interface. Valid range is 0–600.
 - **Max Allowed Statically Locked MAC.** Sets the maximum number of statically locked MAC addresses on the selected interface. Valid range is 0–20.
 - **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.
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, click **Security > Traffic Control**, and then click the **Port Security > Security MAC Address** link.



To convert learned MAC addresses:

1. Select the **Convert Dynamic Address to Static** check box.
2. Click **Apply**. The Dynamic MAC Address entries are converted to Static MAC address entries in a numerically ascending order until the Static limit is reached.

The Dynamic MAC Address Table shows the MAC addresses and their associated VLANs learned on the selected port. Use the **Port List** menu to select the interface for which you want to display data.

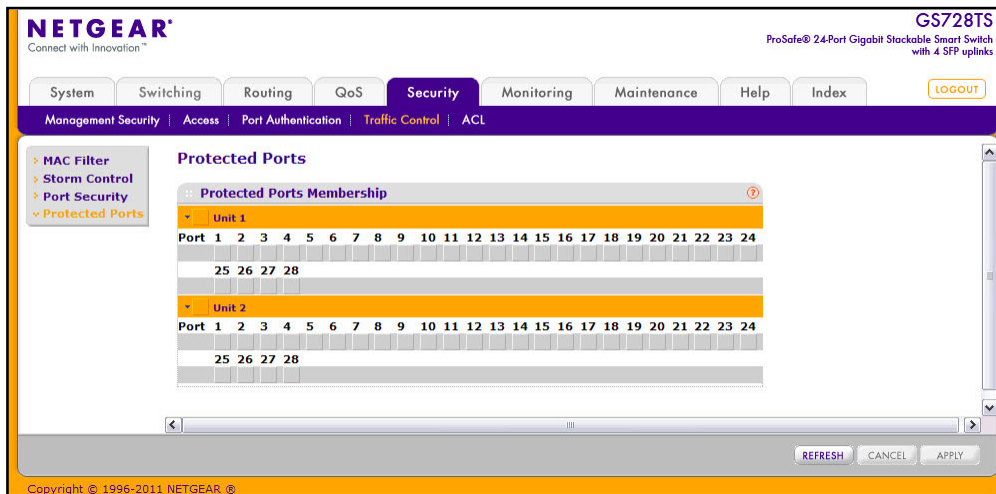
Field	Description
VLAN ID	Displays the VLAN ID corresponding to the Last Violation MAC address.
MAC Address	Displays the MAC addresses learned on a specific port.

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

Protected Ports Membership

If a port is configured as protected, it does not forward traffic to any other protected port on the switch, but it will forward traffic to unprotected ports. Use the Protected Ports Membership page to configure the ports as protected or unprotected.

To display the Protected Ports Membership page, click the **Security > Traffic Control > Protected Ports** link. In the following image, the Unit fields have been expanded to display the ports.



To configure protected ports:

1. Click the orange bar to display the available ports.
2. Click the box below each port to configure as a protected port. Protected ports are marked with a check. No traffic forwarding is possible between two protected ports.
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 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. The GS728TS, GS728TPS, GS752TS, and GS752TPS switches software supports IPv4, IPv6, and MAC ACLs.

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

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

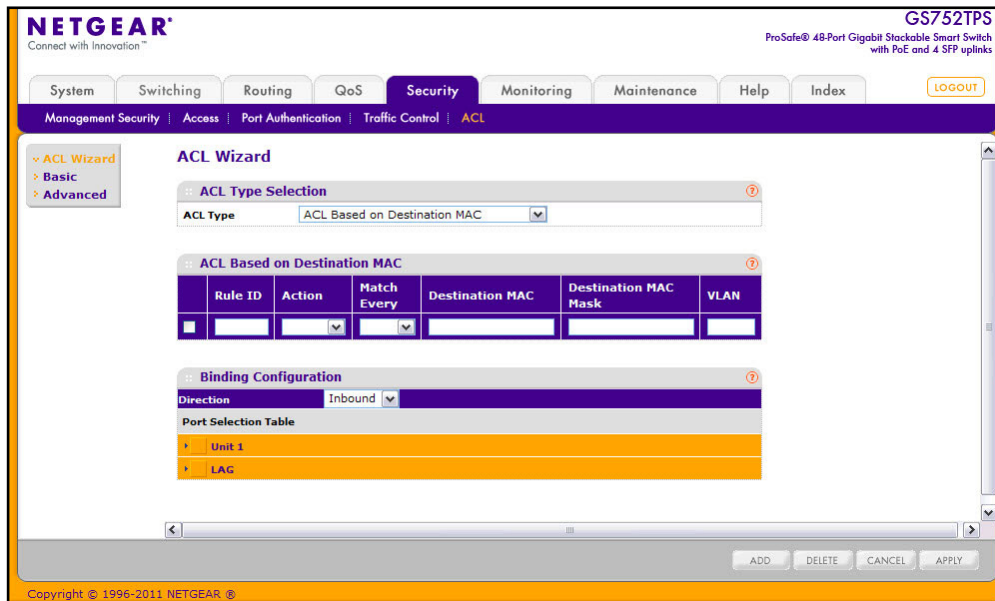
- [ACL Wizard](#)
- Basic:
 - [MAC ACL](#) on page 237
 - [MAC Rules](#) on page 238
 - [MAC Binding Configuration](#) on page 240
 - [MAC Binding Table](#) on page 241
- Advanced:
 - [IP ACL](#) on page 242
 - [IP Rules](#) on page 243
 - [IP Extended Rule](#) on page 245
 - [IPv6 ACL](#) on page 248
 - [IPv6 Rules](#) on page 249
 - [IP Binding Configuration](#) on page 252
 - [IP Binding Table](#) on page 254
 - [VLAN Binding Table](#) on page 255

ACL Wizard

The ACL Wizard helps you to create a simple ACL and apply to the selected ports easily and quickly. You can select an ACL type from a list of common ACLs. The ACL rule fields available on the page change based on the type of ACL you select. You can add an ACL rule to this ACL and then apply the ACL to the selected ports.

Note: The ACL Wizard allows you only to create the ACL, add rules, and bind the ACL to interfaces. The Wizard does not allow you to configure the name, modify the ACL, or delete it. To rename an ACL, modify it, or delete it, go to the MAC ACL, IP ACL, or IPv6 ACL pages.

To display the ACL Wizard page, click **Security > ACL**.



To use the ACL Wizard:

1. Select the type of ACL to configure from the **ACL Type** field. The possible choices include:
 - **ACL Based on Destination MAC** - Use this to create a ACL based on the destination MAC address, destination MAC mask and VLAN.
 - **ACL Based on Source MAC** - Use this to create a ACL based on the source MAC address, source MAC mask and VLAN.
 - **ACL Based on Destination IPv4** - Use this to create a ACL based on the destination IPv4 address and IPv4 address mask.

- **ACL Based on Source IPv4** - Use this to create a ACL based on the source IPv4 address and IPv4 address mask.
 - **ACL Based on Destination IPv6** - Use this to create a ACL based on the destination IPv6 prefix and IPv6 prefix length.
 - **ACL Based on Source IPv6** - Use this to create a ACL based on the source IPv6 prefix and IPv6 prefix length.
 - **ACL Based on Destination IPv4 L4 Port** - Use this to create a ACL based on the destination IPv4 layer4 port number.
 - **ACL Based on Source IPv4 L4 Port** - Use this to create a ACL based on the source IPv4 layer4 port number.
 - **ACL Based on Destination IPv6 L4 Port** - Use this to create a ACL based on the destination IPv6 layer4 port number.
 - **ACL Based on Source IPv6 L4 Port** - Use this to create a ACL based on the source IPv6 layer4 port number.
2. In the **Rule ID** field, enter a whole number in the range of (1 to 10) that will be used to identify the rule.
 3. In the **Action** field, specify what action should be taken if a packet matches the rule's criteria. The choices are permit or deny.
 4. In the **Match Every** field, specify True or False. If you select True, all packets are considered to match the rule criteria, and no other fields are configurable.
 5. Specify the match criteria for the rule. The fields available for match criteria input depend on the selected ACL type.
 6. To add a new rule to the ACL, select the check box next to the Rule ID, then click **Add**. You can add multiple rules to the same ACL type.
 7. In the **Binding Configuration** area, specify the packet filtering direction for an ACL in the **Direction** field. The only valid direction is Inbound.
 8. In the **Port Selection Table** area, select the interfaces for ACL mapping. All non-routing physical ports and LAGs are listed.
 9. To cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch, then click **Cancel**.
 10. To send the updated configuration to the switch, click **Apply**. Configuration changes take effect immediately.

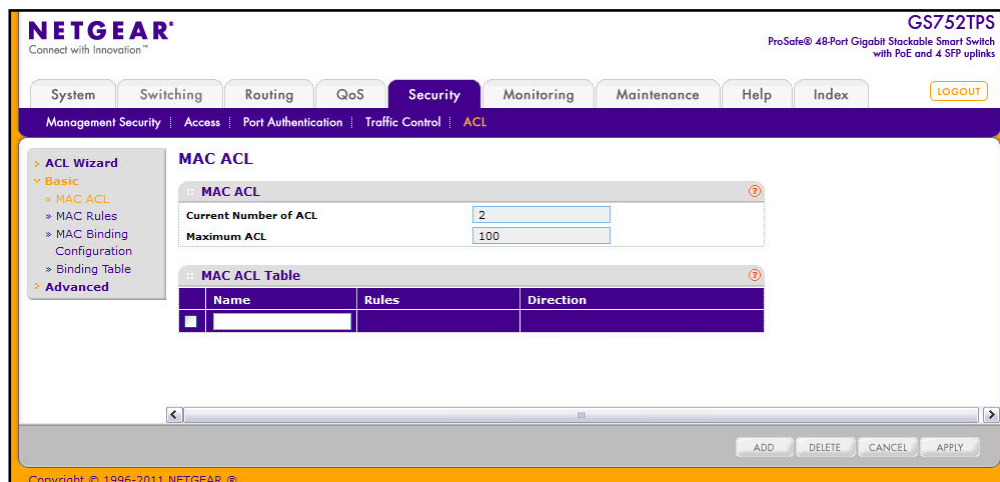
MAC ACL

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 a MAC ACL and applying it to the switch:

1. Use the [MAC ACL](#) page to create the ACL ID.
2. Use the [MAC Rules](#) page to create rules for the ACL.
3. Use the [MAC Binding Configuration](#) page to assign the ACL by its ID number to a port.
4. Optionally, use the [MAC Binding Table](#) page to view the configurations.

To display the MAC ACL page, click **Security > ACL > Basic > MAC ACL**.



The MAC ACL table displays 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.

To configure a MAC ACL:

1. To add a MAC ACL, specify a name for the MAC ACL in the **Name** field, and click **Add**. The name string may include alphabetic, numeric, dash, underscore, or space characters only. The name must start with an alphabetic character.

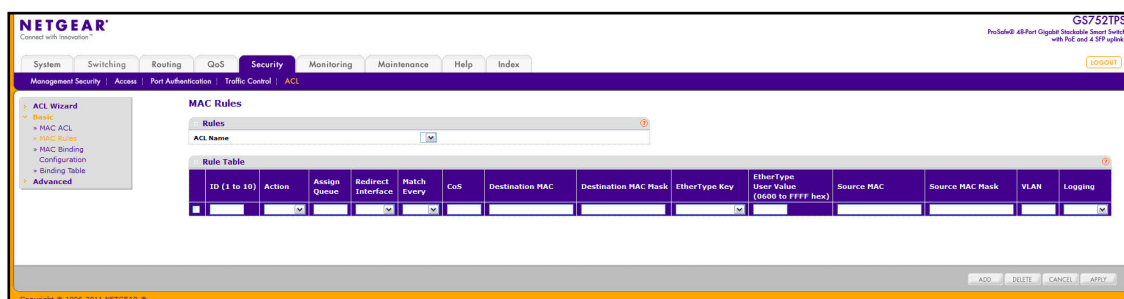
Each configured ACL displays the following information:

- **Rules.** Displays the number of rules currently configured for the MAC ACL.
 - **Direction.** Displays the direction of packet traffic affected by the MAC ACL, which can be Inbound or blank.
2. To delete a MAC ACL, select the check box next to the Name field, then click **Delete**.
 3. To change the name of a MAC ACL, select the check box next to the Name field, update the name, then click **Apply**.
 4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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, click **Security > ACL > Basic > MAC Rules**.



To configure MAC ACL rules:

- From the ACL Name field, specify the existing MAC ACL to which the rule will apply. To set up a new MAC ACL use the [MAC ACL](#) page.
- To add a new rule, enter an ID for the rule, configure the following settings, and click **Add**.
 - 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 0–6 in this field.
 - Redirect Interface.** Specifies the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field cannot be set if a Mirror Interface is already configured for the ACL rule.
 - Match Every.** Requires a packet to match the criteria of this ACL. Select True or False from the drop down 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 0–7 to apply this criteria.
 - Destination MAC.** Requires an Ethernet frame's destination port MAC address to match the address listed here. Enter a MAC address in this 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 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. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is 00:00:ff:ff:ff:ff, all

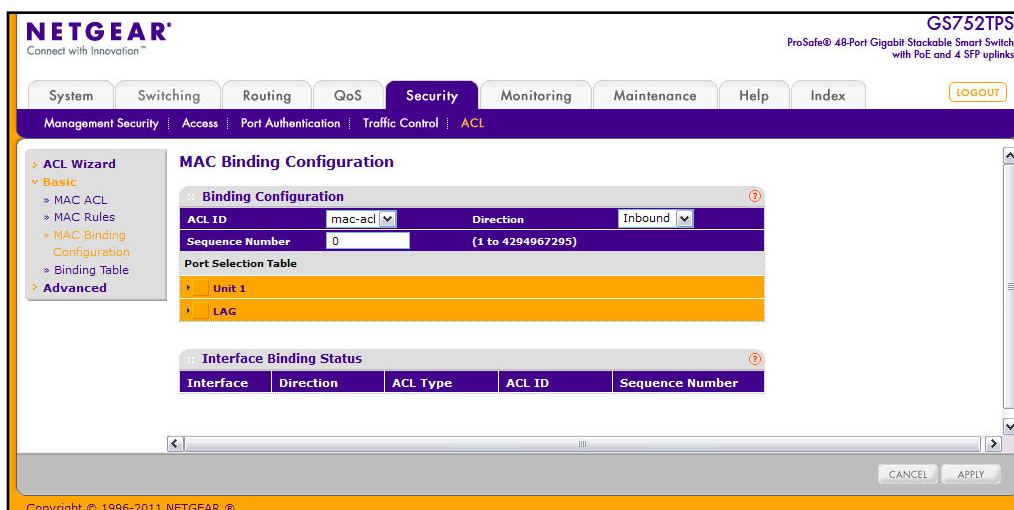
MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). A MAC mask of 00:00:00:00:00:00 matches a single MAC address.

- **EtherType Key.** Requires a packet's EtherType to match the EtherType you select. Select the EtherType value from the drop down menu. If you select User Value, you can enter a custom EtherType value.
 - **EtherType User Value.** This field is configurable if you select User Value from the EtherType drop down menu. The value you enter specifies a customized Ethertype to compare against an Ethernet frame. The valid range of values is 0x0600–0xFFFF.
 - **Source MAC.** Requires a packet's source port MAC address to match the address listed here. Enter a MAC address in the this 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. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.
 - **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 1–4093.
 - **Logging.** When logging is enabled for a rule, the switch periodically sends a message to the log file indicating the number of times a packet matched the rule during that time period. If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was *hit* during the current report interval. A fixed five-minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is only supported for a *Deny* action.
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 delete a rule, select the check box associated with the rule and click **Delete**.
 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, click **Security > ACL > Basic > MAC Binding Configuration**.



To configure MAC ACL interface bindings:

1. Select an existing MAC ACL from the ACL ID menu.
The packet filtering direction for ACL is Inbound, which means the MAC ACL rules are applied to traffic entering the port.
2. Specify an optional sequence number to indicate the order of this access list relative to other access lists already assigned to this interface and direction.

A low number indicates high 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. The valid range is 1–4294967295.

3. Click the appropriate orange bar to expose the available ports or LAGs.
 - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that a check appears in the box.
 - To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. A check in the box indicates that the ACL is applied to the interface.\

In the following figure, the MAC ACL named mac-acl2 is being applied to ports g13 and g20-g22. As the Interface Binding Status table indicates, these ports also have a MAC ACL named mac-acl applied in the inbound direction.

MAC Binding Configuration

Binding Configuration

ACL ID: mac-acl2 Direction: Inbound

Sequence Number: 0 (1 to 4294967295)

Port Selection Table

Unit 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
													✓							✓	✓	✓		
	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	49	50	51	52																				

LAG

Interface Binding Status

Interface	Direction	ACL Type	ACL ID	Sequence Number
1/g13	Inbound	MAC ACL	mac-acl	1
1/g20	Inbound	MAC ACL	mac-acl	2
1/g21	Inbound	MAC ACL	mac-acl	2
1/g22	Inbound	MAC ACL	mac-acl	1

- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
- 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, click **Security > ACL > Basic > Binding Table**.

NETGEAR GS752TPS
ProSafe® 48-Port Gigabit Stackable Smart Switch with PoE and 4 SFP uplinks

System Switching Routing QoS **Security** Monitoring Maintenance Help Index LOGOUT

Management Security Access Port Authentication Traffic Control **ACL**

ACL Wizard
Basic
MAC ACL
MAC Rules
MAC Binding Configuration
Binding Table
Advanced

MAC Binding Table

Interface	Direction	ACL Type	ACL ID	Sequence Number
<input type="checkbox"/> 1/g13	In Bound	MAC ACL	mac-acl	1
<input type="checkbox"/> 1/g13	In Bound	MAC ACL	mac-acl2	2
<input type="checkbox"/> 1/g20	In Bound	MAC ACL	mac-acl	2
<input type="checkbox"/> 1/g20	In Bound	MAC ACL	mac-acl2	3
<input type="checkbox"/> 1/g21	In Bound	MAC ACL	mac-acl	2
<input type="checkbox"/> 1/g21	In Bound	MAC ACL	mac-acl2	3
<input type="checkbox"/> 1/g22	In Bound	MAC ACL	mac-acl	1
<input type="checkbox"/> 1/g22	In Bound	MAC ACL	mac-acl2	2

DELETE CANCEL

Copyright © 1996-2011 NETGEAR

The following table describes the information displayed in the **MAC Binding Table**.

Field	Description
Interface	Displays 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.

To delete a MAC ACL-to-interface binding, select the check box next to the interface and click **Delete**.

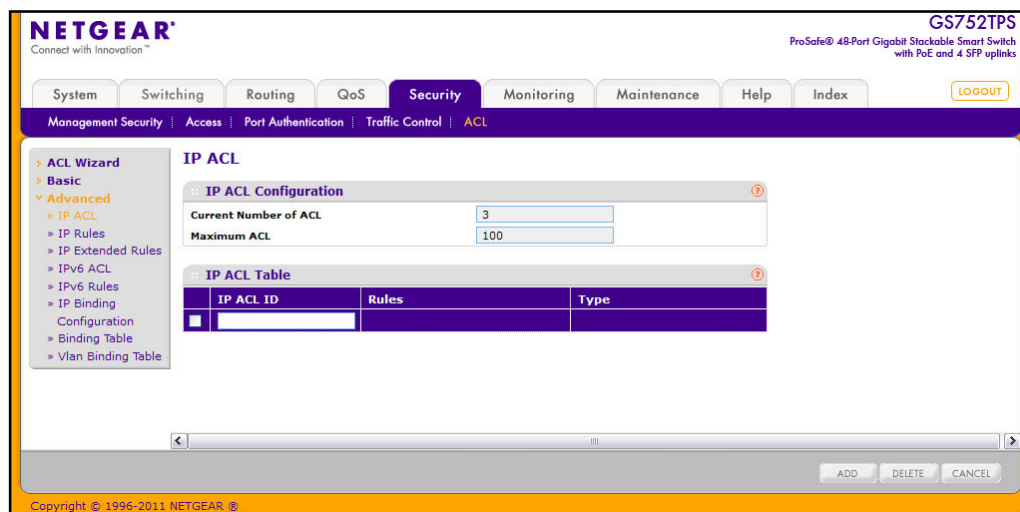
IP ACL

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, click **Security > ACL > Advanced > IP ACL**.



The IP ACL area 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.

To configure an IP ACL:

1. In the **IP ACL ID** field, specify the ACL ID. The ID is 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.
 - Text: Creates a named ACL, which allows the same configuration as an extended ACL.

Each configured ACL displays the following information:

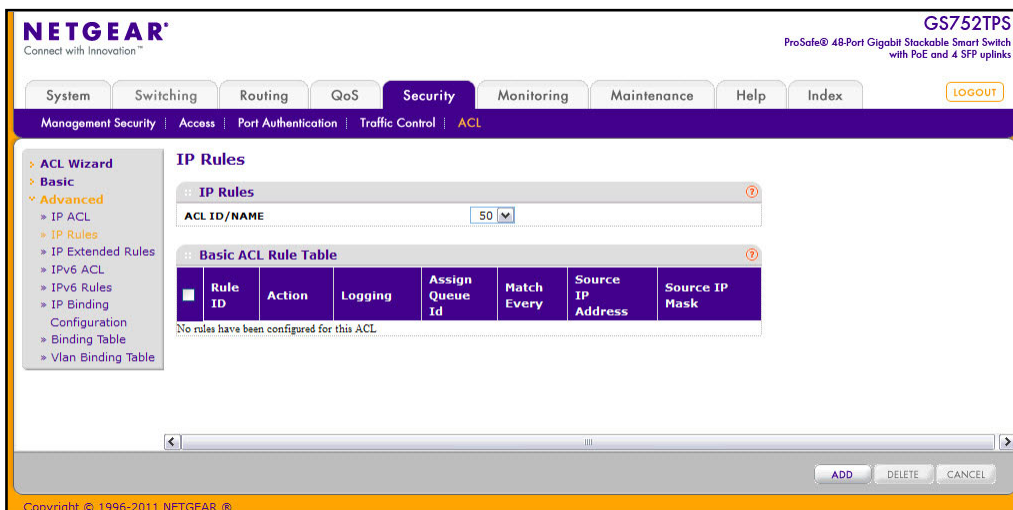
- **Rules.** Displays the number of rules currently configured for the IP ACL.
 - **Type.** Identifies the ACL as either a standard, extended, or named IP ACL.
2. To delete an IP ACL, select the check box next to the IP ACL ID field, then click **Delete**.
 3. To change the name of an IP ACL, select the check box next to the IP ACL ID field, update the name, then click **Apply**.
 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.

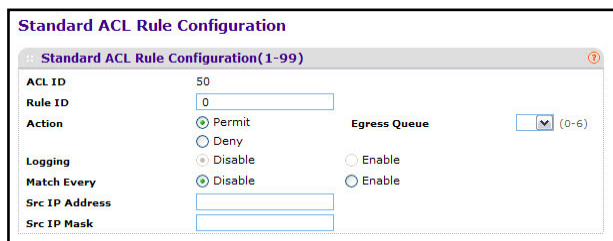
To display the IP Rules page, click **Security > ACL > Advanced > IP Rules**.



To configure rules for an IP ACL:

1. To add an IP ACL rule, select the ACL ID to add the rule to and click **Add**.

The page refreshes and shows the available rules to configure.



2. Complete the fields described in the following list.
 - **Rule ID.** Specify a number from 1–10 to identify the IP ACL rule. 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.
 - **Egress Queue.** Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Enter an identifying number from 0–6 in the appropriate field.
 - **Logging.** When logging is enabled for a rule, the switch periodically sends a message to the log file indicating the number of times a packet matched the rule during that time period. If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was *hit* during the current report interval. A fixed five-minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is only supported for a *Deny* action.

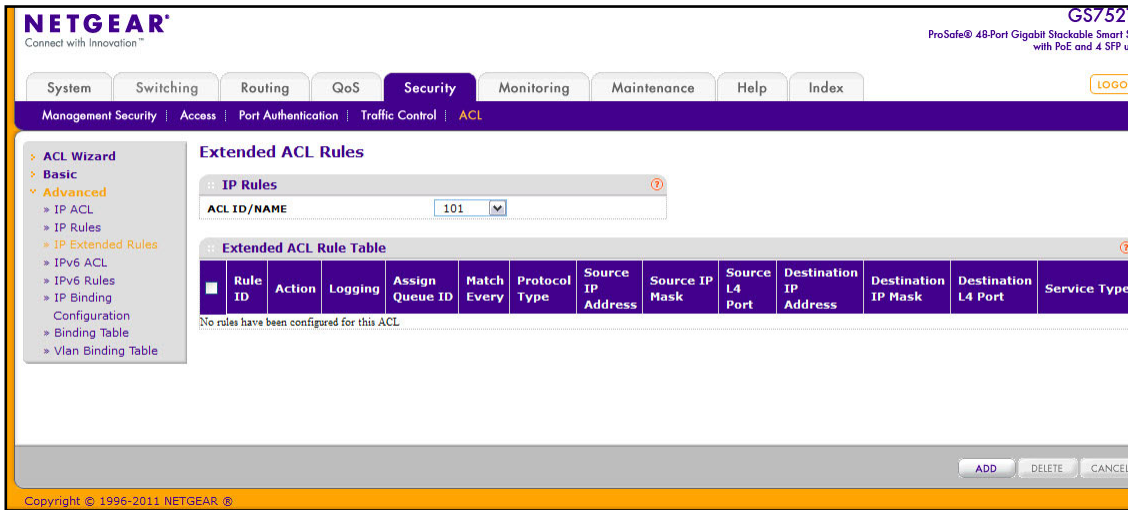
- **Match Every.** Requires a packet to match the criteria of this ACL. Select True or False from the drop down menu. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.
 - **Source IP Address.** Requires a packet's source IP address to match the address listed here. Type 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. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, you type 0.0.0.255 in the Source IP Mask field. This field is required when you configure a source IP address.
3. To delete an IP ACL rule, select the check box associated with the rule, and then click **Delete**.
 4. To update an IP ACL rule, select the check box associated with the rule, update the desired fields, and then click **Apply**. You cannot modify the Rule ID of an existing IP rule.
 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 change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

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.

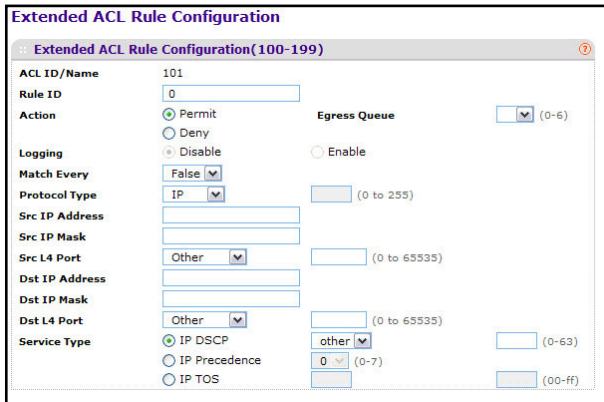
To display the IP extended Rules page, click **Security > ACL > Advanced > IP Extended Rules**.



To configure rules for an IP ACL:

1. To add an IP ACL rule, select the ACL ID to add the rule to and click **Add**.

The page displays the extended ACL Rule Configuration fields, as the following figure shows.



2. Configure the new rule.

- **Rule ID.** Specify a number from 1–10 to identify the IP ACL rule. 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.
- **Egress Queue.** Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Enter an identifying number from 0–6 in the appropriate field.
- **Logging.** When logging is enabled for a rule, the switch periodically sends a message to the log file indicating the number of times a packet matched the rule during that

time period. If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was *hit* during the current report interval. A fixed five-minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is only supported for a *Deny* action.

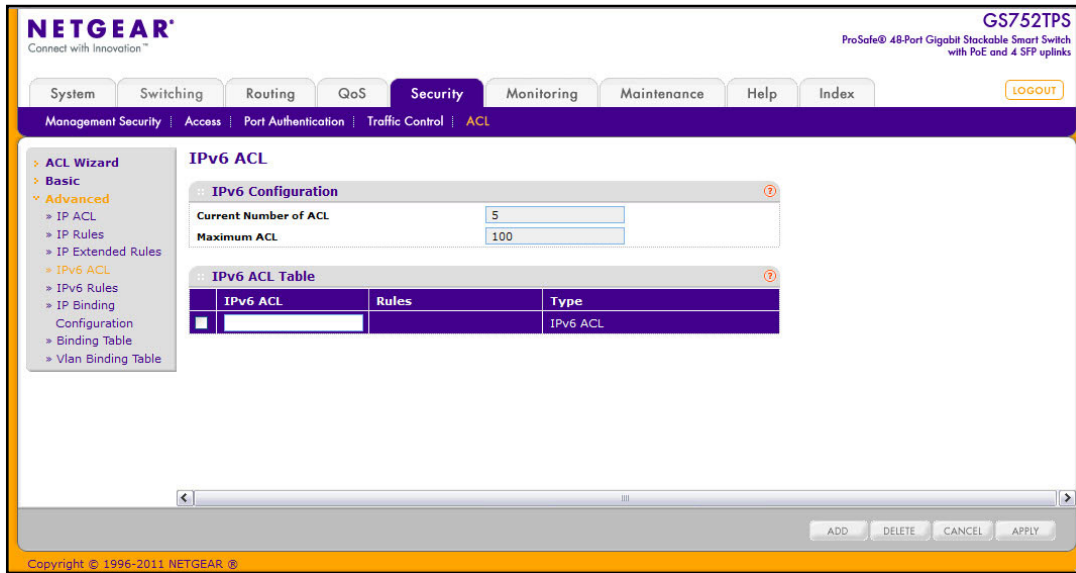
- **Match Every.** Requires a packet to match the criteria of this ACL. Select True or False from the drop down menu. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.
- **Protocol Type.** Requires a packet's protocol to match the protocol listed here. Select a type from the drop down menu or enter the protocol number in the available field.
- **Src IP Address.** Requires a packet's source IP address to match the address listed here. Type 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. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, you type 0.0.0.255 in the Source IP Mask field. 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.** Specifies the destination 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. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, you type 0.0.0.255 in the Source IP Mask field. This field is required when you configure a source IP address.
- **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.** Choose one of the Service Type match conditions for the extended IP ACL rule. The possible values are IP DSCP, IP precedence, and IP TOS, which are alternative ways of specifying a match criterion for the same Service Type field in the IP header, however each uses a different user notation. After you select the service type, specify the value associated with the type.
 - **IP DSCP:** Specify the IP DiffServ Code Point (DSCP) value. The DSCP is defined as the high-order six bits of the Service Type octet in the IP header. Select an IP DSCP value from the menu. To specify a numeric value in the available field, select Other from the menu and type an integer from 0 to 63 in the field.
 - **IP Precedence:** The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 7.
 - **IP TOS Bits:** Matches on the Type of Service bits in the IP header when checked. In the first TOS field, specify the two-digit hexadecimal TOS number. The second field is for the TOS Mask, which specifies the bit positions that are used for comparison against the IP TOS field in a packet. The TOS Mask value is a two-digit hexadecimal number from 00 to ff, representing an inverted (i.e. wildcard) mask. The zero-valued bits in the TOS Mask denote the bit positions in the TOS Bits value that are used for comparison against the IP TOS field of a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of a0 and a TOS Mask of 00.
- 3. To add the new rule to the ACL, click **Apply**.
- 4. To delete a rule from an ACL, select the check box associated with the rule and 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. To modify an existing IP Extended ACL rule, click the Rule ID. The number is a hyperlink to the Extended ACL Rule Configuration page.

IPv6 ACL

An IPv6 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. On this menu, the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the IP ACL are specified/created using the IP ACL Rule Configuration menu.

To display the IPv6 ACL page, click **Security > ACL > Advanced > IPv6 ACL**.



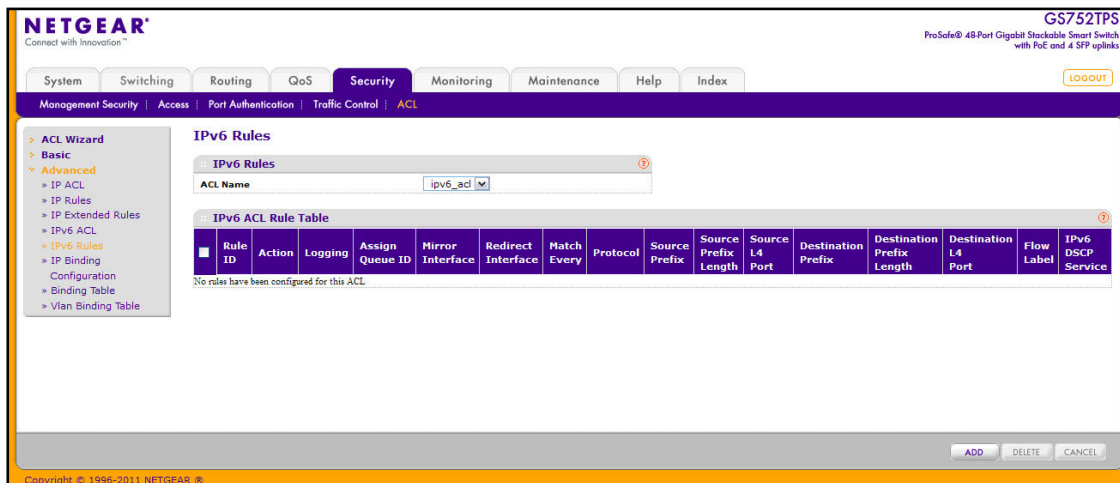
The current number of the IP ACLs configured on the switch is displayed in the **Current Number of ACL** area. The maximum number of IP ACL that can be configured on the switch is displayed in the **Maximum ACL** field, depending on the hardware. The name of IPv6 ACL can be configured in IPv6 ACL field. The number of the rules associated with the IP ACL is displayed in the **Rules** field. The ACL type is IPv6 ACL and displayed in the **Type** field.

1. To add an ACL, type a name in the IPv6 ACL field, and then click **Add**.
2. To delete an ACL, select the check box associated with the ACL, 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 modify the IPv6 ACL name, click **Apply** to submit the changes to the switch.

IPv6 Rules

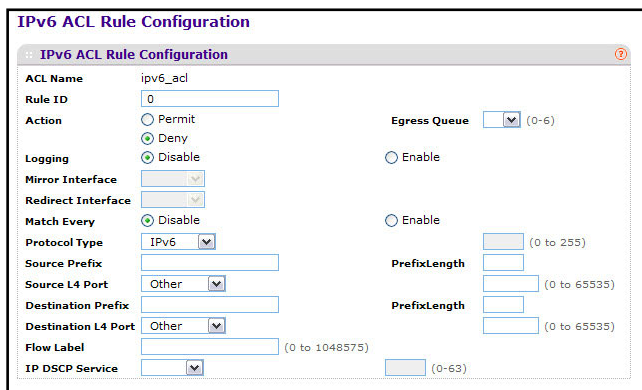
Use the IPv6 Rules page to configure the rules for the IPv6 Access Control Lists. The IPv6 Access Control Lists are created using the IPv6 Access Control List Configuration page. By default, no specific value is in effect for any of the IPv6 ACL rules.

To display the IPv6 Rules page, click **Security > ACL > Advanced > IPv6 Rules**. In the following figure, an IPv6 rule exists, and one rule has been configured.



To configure the IPv6 rules, select the following:

1. To add an IPv6 rule, use the pull-down list in the **ACL Name** field to select the IP ACL for which to create or update a rule. Complete the fields described in the following list, and click **Add**.



2. Configure the new rule.
 - **Rule ID:** Enter a whole number in the range of 1 to 10 that will be used to identify the rule. An IPv6 ACL may have up to 10 rules.
 - **Action:** Specify what action should be taken if a packet matches the rule's criteria. The choices are Permit or Deny.
 - **Egress Queue:** Specifies the hardware egress queue identifier used to handle all packets matching this IPv6 ACL rule. The valid range of Queue IDs is from 0 to 6. This field is visible for a Permit Action.
 - **Logging.** When logging is enabled for a rule, the switch periodically sends a message to the log file indicating the number of times a packet matched the rule during that time period. If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was *hit* during the current report interval. A fixed five-minute report interval is used for the entire system. A trap

is not issued if the ACL rule hit count is zero for the current interval. This field is only supported for a *Deny* action.

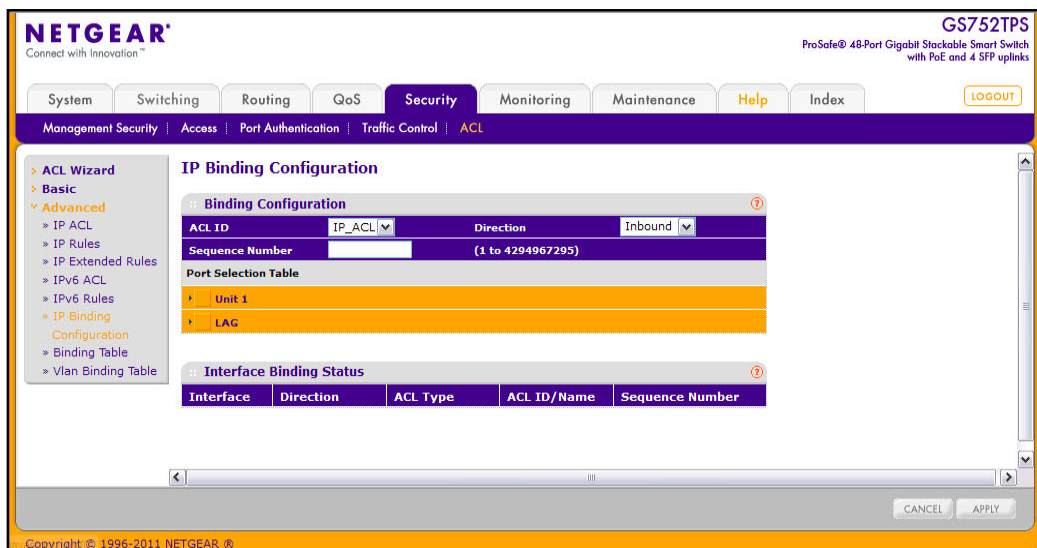
- **Mirror Interface:** Specifies the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. This field cannot be set if a Redirect Interface is already configured for the ACL rule. This field is visible for a Permit action. Mirrored interfaces do not need to be part of the traffic VLAN.
- **Redirect Interface:** Specifies the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field cannot be set if a Mirror Interface is already configured for the ACL rule. This field is visible for a Permit action. Redirected interfaces should be part of the traffic VLAN.
- **Match Every:** Select true or false from the pull down menu. True signifies that all packets will match the selected IPv6 ACL and Rule and will be either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria will not be offered. To configure specific match criteria for the rule, remove the rule and recreate it, or reconfigure Match Every to False for the other match criteria to be visible.
- **Protocol:** There are two ways to configure IPv6 protocol:
 - Specify an integer ranging from 0 to 255 after selecting protocol keyword “other”. This number represents the IPv6 protocol.
 - Select name of a protocol from the existing list of IPv6, ICMPv6, TCP, and UDP.
- **Source Prefix/Prefix Length:** Specify IPv6 Prefix combined with IPv6 Prefix length of the network or host from which the packet is being sent. Prefix length can be in the range (0 to 128).
- **Source L4 Port:** Specify a packet's source layer 4 port as a match condition for the selected IPv6 ACL rule. Source port information is optional. Source port information can be specified in two ways:
 - Select keyword “other” from the drop-down menu and specify the number of the port in the range from 0 to 65535.
 - Select one of the keyword from the list: DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.
- **Destination Prefix/Prefix Length:** Enter up to 128-bit prefix combined with prefix length to be compared to a packet's destination IP Address as a match criteria for the selected IPv6 ACL rule. Prefix length can be in the range (0 to 128).
- **Destination L4 Port:** Specify a packet's destination layer 4 port as a match condition for the selected IPv6 ACL rule. Destination port information is optional. Destination port information can be specified in two ways:
 - Select keyword “other” from the drop-down menu and specify the number of the port in the range from 0 to 65535.
 - Select one of the keyword from the list: DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

- **Flow Label:** Flow label is 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers. Flow label can be specified within the range (0 to 1048575).
 - **IPv6 DSCP Service:** Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IPv6 header. This is an optional configuration. Enter an integer from 0 to 63. The IPv6 DSCP is selected by possibly selection one of the DSCP keyword from a drop-down menu. If a value is to be selected by specifying its numeric value, then select the **Other** option in the drop-down menu and a text box will appear where the numeric value of the DSCP can be entered.
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 the new rule to the ACL, click **Apply**.
 5. To delete a rule from an ACL, select the check box associated with the rule and click **Delete**.

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, click **Security > ACL > Advanced > IP Binding Configuration**.



To configure IP ACL interface bindings:

1. Select an existing IP ACL from the ACL ID menu.

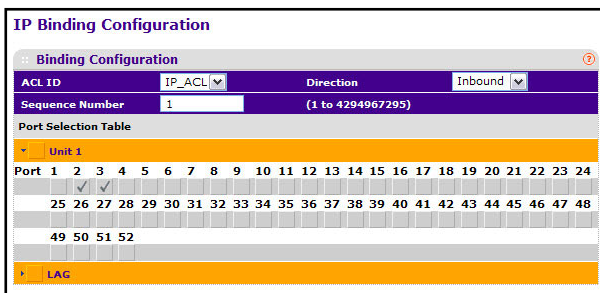
The packet filtering direction for ACL is Inbound, which means the IP ACL rules are applied to traffic entering the port.

2. Specify an optional sequence number to indicate the order of this access list relative to other access lists already assigned to this interface and direction.

A low number indicates high 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. The valid range is 1–4294967295.

3. Click the appropriate orange bar to expose the available ports or LAGs.
 - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that a check appears in the box.
 - To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. A check in the box indicates that the ACL is applied to the interface.

In the following figure, an extended ACL with the ACL ID IP_ACL is being applied to ports g2 and g3.

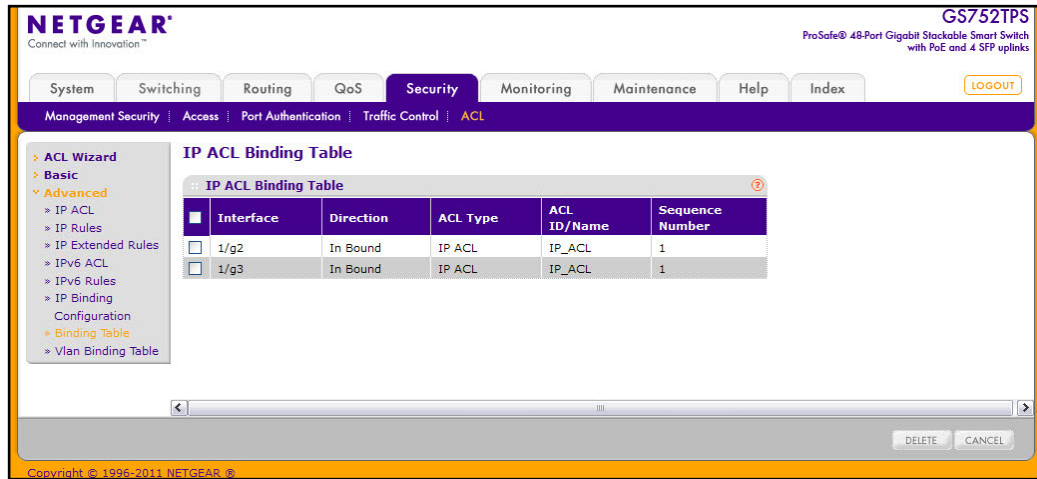


4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Apply** to save any changes to the running configuration.

IP Binding Table

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

To display the IP Binding Table, click **Security > ACL > Advanced > Binding Table**.



The following table describes the information displayed in the **IP ACL Binding Table**.

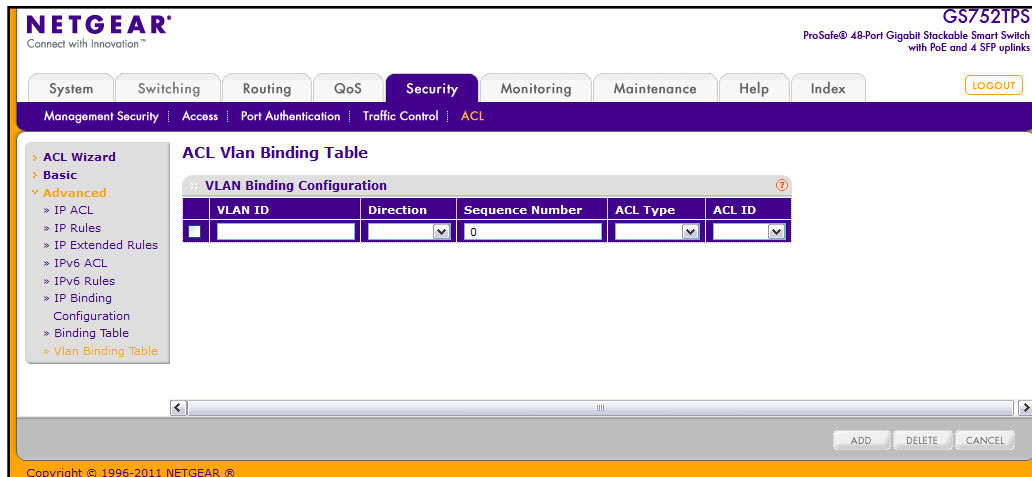
Field	Description
Interface	Displays the interface to which the IP ACL is bound.
Direction	Specifies the packet filtering direction for ACL. The only valid direction is Inbound, which means the IP ACL rules are applied to traffic entering the port.
ACL Type	Displays the type of ACL assigned to selected interface and direction.
ACL ID/Name	Displays the ACL number or name that identifies the ACL assigned to selected interface and direction.
Sequence Number	Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

To delete an IP ACL-to-interface binding, select the check box next to the interface and click **Delete**. Click **Cancel** to abandon any changes.

VLAN Binding Table

Use the VLAN Binding Table page to associate configured ACLs with VLANs.

To display the VLAN Binding Table page, click **Security > ACL > Advanced > Vlan Binding Table**.



In the ACL Binding area, enter the values in the following fields:

1. In the **VLAN ID** field, specify a VLAN ID for ACL mapping.
2. In the **Direction** field, specify the direction of packet traffic affected by the MAC ACL, which can be Inbound or blank.
3. In The **Sequence Number** field, specify the sequence number of the access lists.

This field displays an optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this VLAN and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this VLAN 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 (i.e., the value is 0), a sequence number that is one greater than the highest sequence number currently in use for this VLAN and direction will be used. Valid range is (1 to 4294967295).

4. In the **ACL Type** field, specify the type of ACL. Valid ACL types are:
 - IP ACL
 - MAC ACL
 - IPv6 ACL
5. The **ACL ID** field displays all the ACLs configured, depending on the ACL Type selected.
6. To add a VLAN ID to the selected ACL ID, click **Add**.
7. To remove the VLAN ID to the selected ACL ID, click **Delete**.
8. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Monitoring the System

7

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:

- [Ports](#) on page 256
- [System Logs](#) on page 270
- [Port Mirroring](#) on page 278

Ports

The pages available from the Ports link contain a variety of information about the number and type of traffic transmitted from and received on the switch. From the Ports link, you can access the following pages:

- [Switch Statistics](#) on page 256
- [Port Statistics](#) on page 259
- [Port Detailed Statistics](#) on page 260
- [EAP Statistics](#) on page 266
- [Cable Test](#) on page 268

Switch Statistics

The Switch Statistics page displays detailed statistical information about the traffic the switch handles.

To access the Switch Statistics page, click **Monitoring > Ports > Switch Statistics**.

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

Field	Description
ifIndex	313
Octets Received	3168201
Packets Received Without Errors	25741
Unicast Packets Received	14539
Multicast Packets Received	9563
Broadcast Packets Received	1639
Receive Packets Discarded	6457
Octets Transmitted	19999388
Packets Transmitted Without Errors	24534
Unicast Packets Transmitted	18107
Multicast Packets Transmitted	6410
Broadcast Packets Transmitted	17
Transmit Packets Discarded	0
Most Address Entries Ever Used	10
Address Entries in Use	7
Maximum VLAN Entries	255
Most VLAN Entries Ever Used	4
Static VLAN Entries	4
VLAN Deletes	0
Time Since Counters Last Cleared	2 day 5 hr 51 min 18 sec

The following table describes the Switch Statistics displayed on the screen.

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. 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. This does not include multicast packets.
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.

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

Field	Description
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.
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.

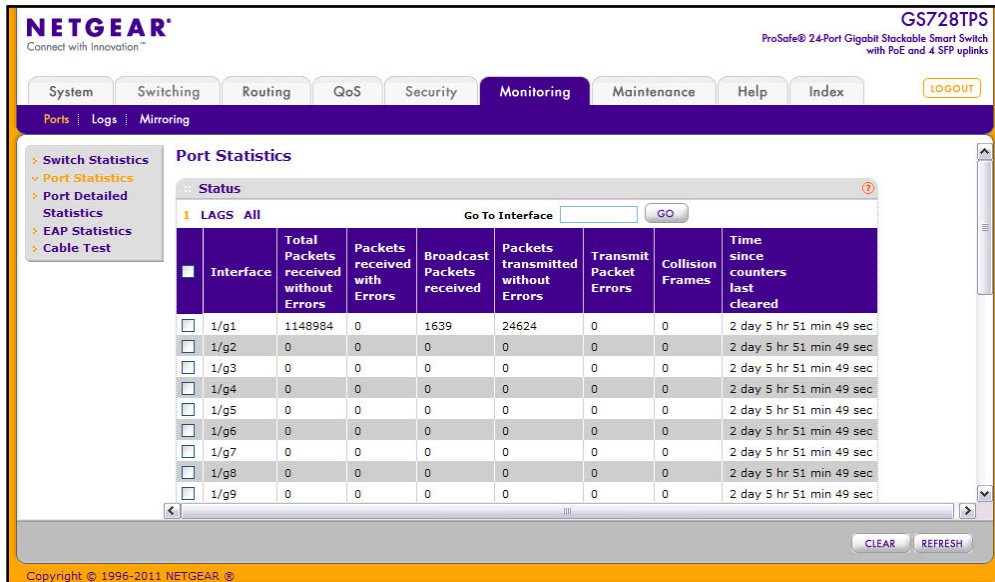
Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear all the statistics counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.
- Click **Refresh** to refresh the page with the most current data from the switch.

Port Statistics

The Port Statistics page displays a summary of per-port traffic statistics on the switch.

To access the Port Summary page, click **Monitoring > Ports**, and then click the **Port Statistics** link.



To view port statistics:

1. To view statistics for a physical port, click the unit ID of the stack member with the ports to view.
2. To view statistics for a Link Aggregation Group (LAG), click **LAGS**.
3. To view statistics for both physical ports and LAGs, click **ALL**.
4. To view statistics for a specific interface, enter the interface ID in the **Go To Interface** and click **Go**.

The following table describes the per-port statistics displayed on the screen.

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. This does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that have been transmitted by this port to its segment.

Field	Description
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.

Use the buttons at the bottom of the page to perform the following actions:

- 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.
- To clear the counters for a specific port, select the check box associated with the port and click **Clear**.
- 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, click the **Monitoring > Ports** tab, and then click **Port Detailed Statistics**. (The following figure shows some, but not all, of the fields on the Port Detailed Statistics page.)

The screenshot shows the Netgear web interface for a GS728TPS switch. The 'Monitoring' tab is selected, and the 'Port Detailed Statistics' page is displayed for interface 1/g1. The page shows a list of configuration parameters and traffic statistics.

Field	Value
Interface	1/g1
MST ID	CST
IfIndex	1
Port Type	Normal
Port Channel ID	not a lag member
Port Role	
STP Mode	Disable
STP State	
Admin Mode	Enable
Flow Control Mode	Disable
LACP Mode	Enable
Physical Mode	Auto
Physical Status	1000 Mbps
Link Status	Link Up
Link Trap	Enable
Packets RX and TX 64 Octets	1131502
Packets RX and TX 65-127 Octets	20231
Packets RX and TX 128-255 Octets	3432
Packets RX and TX 256-511 Octets	4763
Packets RX and TX 512-1023 Octets	1923
Packets RX and TX 1024-1518 Octets	11955

At the bottom of the page, there are 'CLEAR' and 'REFRESH' buttons.

The following table describes the detailed port information displayed on the screen. To view information about a different port, select the port number from the Interface menu.

Field	Description
Interface	Use the drop down 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: <ul style="list-style-type: none"> • Mirrored: Indicates that the port has been configured as a monitoring port and is the source port in a port mirroring session. For additional information about port monitoring and probe ports, see Multiple Port Mirroring on page 278. • Probe: Indicates that the port has been configured as a monitoring port and is the destination port in a port mirroring session. For additional information about port monitoring and probe ports, see Multiple Port Mirroring on page 278. • 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).
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	Displays the Spanning Tree Protocol (STP) Administrative Mode for the port or LAG. The possible values for this field are: <ul style="list-style-type: none"> • Enable: Enables the Spanning Tree Protocol for this port. • Disable: Disables the Spanning Tree Protocol for this port.
STP State	Displays 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: <ul style="list-style-type: none"> • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Admin Mode	Displays the port control administration state: <ul style="list-style-type: none"> • Enable: The port can participate in the network (default). • Disable: The port is administratively down and does not participate in the network.

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

Field	Description
LACP Mode	Selects the Link Aggregation Control Protocol administration state: <ul style="list-style-type: none"> • 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 Enable. <ul style="list-style-type: none"> • 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.
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 > 1522 Octets	The total number of packets (including bad packets) received or transmitted that are in excess of 1522 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).

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

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 in excess of 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. 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. 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). 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.
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).

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

Field	Description
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.
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).

GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches

Field	Description
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 > 1522 Octets	The total number of packets (including bad packets) transmitted that were between over 1522 octets in length inclusive (excluding framing bits but including FCS octets).
Maximum Frame Size	The maximum Ethernet frame size the interface supports or is configured to support. The maximum size includes the Ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.
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.
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.

Field	Description
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.

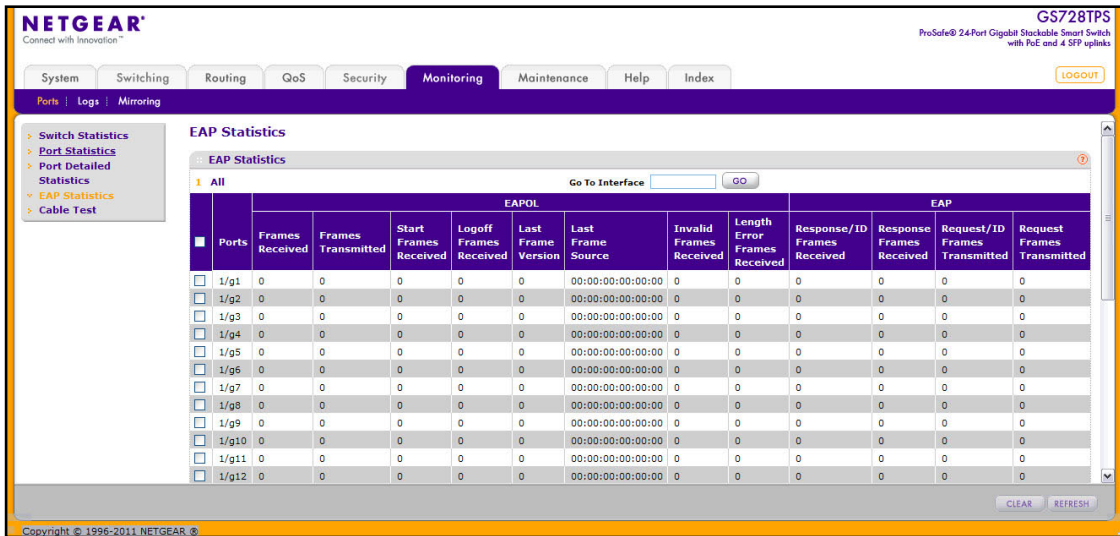
Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear all the counters. This resets all statistics for this port to the default values.
- 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, click the **Monitoring > Ports** tab, and then click the **EAP Statistics** link.



To view EAP statistics:

1. To view statistics for a physical port, click the unit ID of the stack member with the ports to view.
2. To view statistics for a Link Aggregation Group (LAG), click **LAGS**.
3. To view statistics for both physical ports and LAGs, click **ALL**.
4. To view statistics for a specific interface, enter the interface ID in the **Go To Interface** and click **Go**.

The following table describes the EAP statistics displayed on the screen.

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.
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.

Field	Description
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.

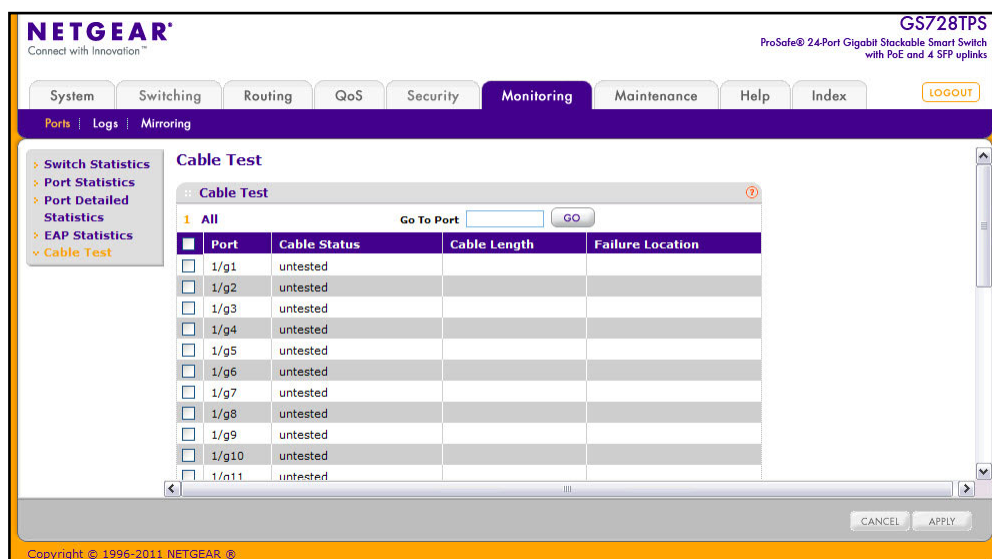
Use the buttons at the bottom of the page to perform the following actions:

- 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.
- To clear the counters for a specific port, select the check box associated with the port and click **Clear**.
- Click **Refresh** to refresh the data on the screen and display the most current statistics.

Cable Test

Use the Cable Test page to display information about the cables connected to switch ports.

To display the Cable Test page, click the **Monitoring** > **Ports** tab, and then click the **Cable Test** link.



To perform the cable test:

1. Select one or more ports to test for cable information.
2. Click **Apply** to run the test.

The following table shows the information the Cable Test page shows:

Field	Description
Cable Status	Displays the cable status. <ul style="list-style-type: none"> • Normal: the cable is working correctly. • Open: the cable is disconnected or there is a faulty connector. • Short: there is an electrical short in the cable. • Cable Test Failed: The cable status could not be determined. The cable may in fact be working. • Unknown: The test has not been performed.
Cable Length	The estimated length of the cable in meters. The length is displayed as a range between the shortest estimated length and the longest estimated length. Unknown is displayed if the cable length could not be determined. The Cable Length is displayed only if the cable status is Normal.
Failure Location	The estimated distance in meters from the end of the cable to the failure location. The failure location is displayed only if the cable status is Open or Short.

Click **Refresh** to refresh the data on the screen and display the most current statistics.

System 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 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 270
- [FLASH Log Configuration](#) on page 272
- [Server Log Configuration](#) on page 274
- [Trap Logs](#) on page 276
- [Event Logs](#) on page 277

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. These log messages are cleared when the switch reboots.

To access the Memory Log page, click the **Monitoring > Logs** tab, and then click the **Memory Log** link.

The screenshot displays the NETGEAR web interface for a GS752TS switch. The 'Monitoring' tab is selected, and the 'Memory Log' sub-tab is active. The interface shows the following configuration and log data:

Memory Log Configuration

- Admin Status: Disable Enable
- Behavior: Wrap

Memory Log

Total number of Messages: 84

Description
<14> Jan 3 08:24:52 10.130.184.57-1 General[47227852]: main_login.c(210) 282 %% HTTP Session 5 initiated for connection from 10.27.65.112
<14> Jan 3 08:24:41 10.130.184.57-1 General[47227852]: main_login.c(210) 281 %% HTTP Session 5 initiated for connection from 10.27.65.112
<14> Jan 3 07:55:01 10.130.184.57-1 CLI_WEB[46244812]: session.c(125) 280 %% HTTP Session 5 ended for user admin connected from 10.27.65.112
<14> Jan 3 06:29:01 10.130.184.57-1 General[47227852]: main_login.c(210) 279 %% HTTP Session 5 initiated for connection from 10.27.65.112
<14> Jan 3 06:28:50 10.130.184.57-1 General[47227852]: main_login.c(210) 278 %% HTTP Session 5 initiated for connection from 10.27.65.112
<14> Jan 3 05:10:31 10.130.184.57-1 CLI_WEB[46244812]: session.c(125) 277 %% HTTP Session 5 ended for user admin connected from 10.27.65.112
<14> Jan 3 04:53:40 10.130.184.57-1 DRIVER[47020004]: dapi.c(879) 276 %% Error on command 47: usp 2/0/22: Card Not Attached.
<14> Jan 3 04:09:51 10.130.184.57-1 UNITMGR[47137884]: unitmgr.c(6244) 275 %% Copy of running configuration to backup unit complete
<14> Jan 3 04:09:50 10.130.184.57-1 UNITMGR[47227852]: unitmgr.c(6113) 273 %% Configuration propagation successful for config type 0

At the bottom of the log list, there are buttons for CLEAR, REFRESH, CANCEL, and APPLY.

To configure the Memory Log settings:

1. Use the radio buttons in the **Admin Status** field to determine whether to log messages.
 - **Enable:** Enables system logging.
 - **Disable:** Prevents the system from logging messages.
2. From the **Behavior** menu, specify 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.
3. If you change the buffered log settings, click **Apply** to apply the changes to the system and the changes will be saved.

The Memory Log table also appears on the Memory Log page.

Field	Description
Total Number of Messages	Displays the number of messages the system has logged in memory. Only the 65 most recent entries are displayed on the page.
Description	The log message text, which includes the time the log was recorded.

The rest of the page displays the Memory Log messages. The format of the log message is the same for messages that are displayed for the message log, persistent log, or console log. Messages logged to a collector or relay via syslog have the same format as well.

The following example shows the standard format for a log message:

```
<14> Mar 24 05:34:05 10.131.12.183-1 UNKN[2176789276]:
main_login.c(179) 3855 %% HTTP Session 19 initiated for user admin
connected from 10.27.64.122
```

The number contained in the angle brackets represents the message priority, which is derived from the following values:

Priority = (facility value × 8) + severity level.

The facility value is usually one, which means it is a user-level message. Therefore, to determine the severity level of the message, subtract eight from the number in the angle brackets. The example log message has a severity level of 6 (informational). For more information about the severity of a log message, see the **Severity Filter** description on 275.

The message was generated on March 24 at 5:34:05 a.m by the switch with an IP address of 10.131.12.183. The component that generated the message is unknown, but it came from line 179 of the main_login.c file. This is the 3,855th message logged since the switch was last booted. The message indicates that the administrator logged onto the HTTP management interface from a host with an IP address of 10.27.64.122.

Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear the messages out of the buffered log in the memory.
- Click **Refresh** to update the page with the latest messages in the log.

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

FLASH Log Configuration

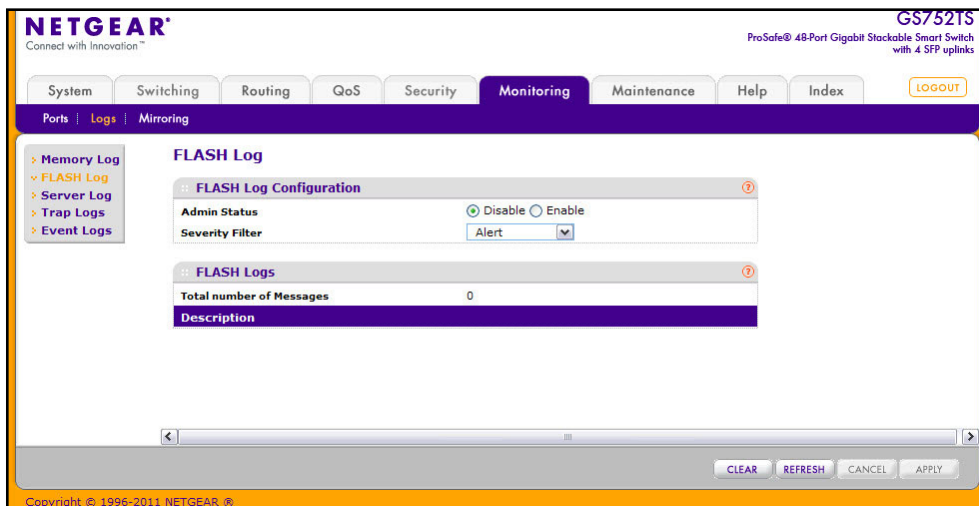
The FLASH log is a log that is stored in persistent storage, which means that the log messages are retained across a switch reboot.

- 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. 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, click the **Monitoring > Logs tab**, and then click the **FLASH Log** link.



To configure the FLASH Log settings:

1. Use the radio buttons in the **Admin Status** field to determine whether to log messages to persistent storage.
 - **Enable**: Enables persistent logging.
 - **Disable**: Prevents the system from logging messages in persistent storage.

2. From the **Severity Filter** field, specify the type of log messages to record. A log records messages equal to or above a configured severity threshold. 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.
 - **Information** (6): Provides device information.
 - **Debug** (7): Provides detailed information about the log. Debugging should only be entered by qualified support personnel.
3. If you make any changes to the page, click **Apply** to apply the change to the system.

The rest of the page displays the number of persistent messages the system has logged and the persistent log messages.

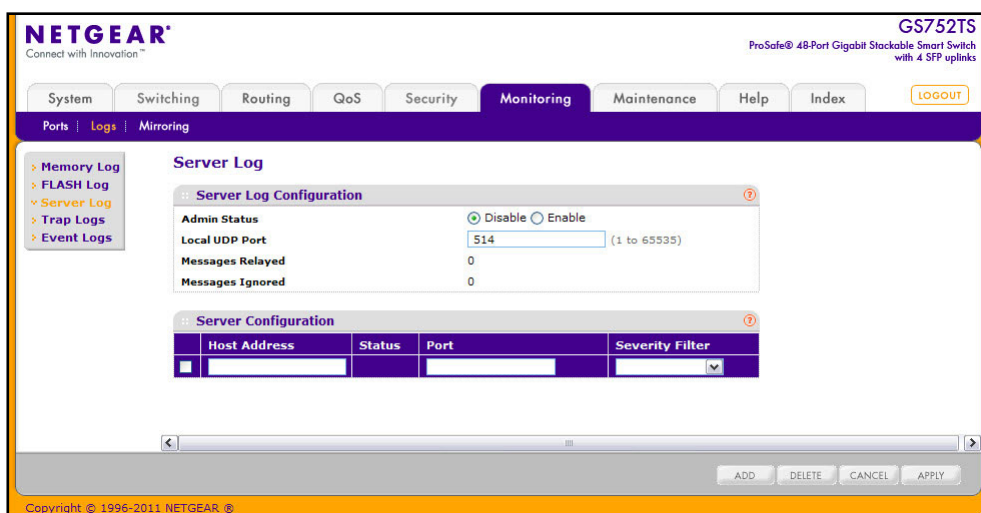
Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear the messages out of the buffered log.
- Click **Refresh** to refresh the page with the most current data from the switch.
- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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, click the **Monitoring > Logs tab**, and then click the **Server Log** link.



To configure local log server settings:

1. Use the radio buttons in the **Admin Status** field to determine 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.
2. In the Local UDP Port field, specify the port on the switch from which syslog messages are sent.
3. Click **Apply** to save the settings.

The Server Log Configuration area also displays the following information:

- The **Messages Relayed** field shows the number of messages forwarded by the syslog function to a syslog host. **Messages forwarded to multiple hosts are counted once for each host.**
- The **Messages Ignored** field shows the number of messages that were ignored.

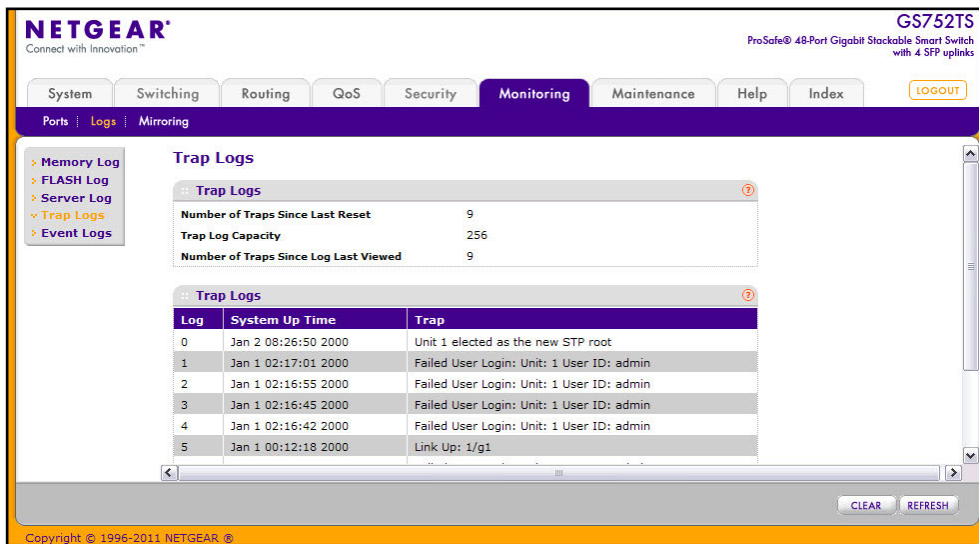
To configure a remote log server

1. To add a remote syslog host (log server), specify the settings in the following list and click **Add**.
 - **Host Address**. Specify the IP address or hostname of the host configured for syslog.
 - **Port**. Specify the port on the host to which syslog messages are sent. The default port is 514.
 - **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 delete an existing host, select the check box next to the host and click **Delete**.
3. To modify the settings for an existing host, select the check box next to the host, change the desired information, and click **Apply**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The **Status** field in the Server Configuration table shows whether the remote logging host is currently active.

Trap Logs

Use the Trap Logs page to view information about the SNMP traps generated on the switch. To access the Trap Logs page, click the **Monitoring > Logs tab**, and then click the **Trap Logs** link.



The following table describes the Trap Log information displayed on the screen.

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 (such as terminal interface display, Web display, or upload file from switch) will cause this counter to be cleared to 0.

The page also displays information about the traps that were sent.

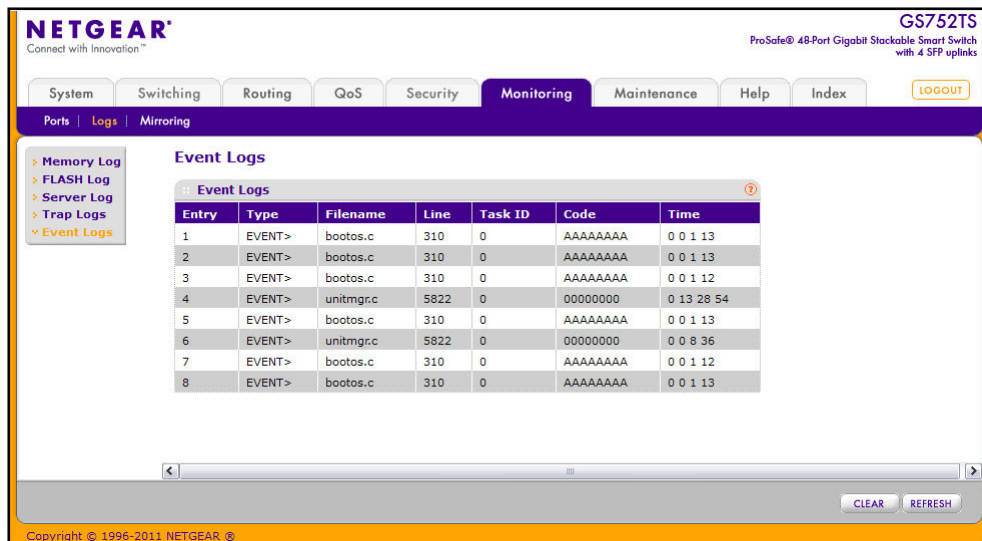
Field	Description
Log	The sequence number of this trap.
System Up Time	The time at which this trap occurred, expressed in days, hours, minutes, and seconds since the last reboot of the switch.
Trap	Information identifying the trap.

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, click the **Monitoring > Logs tab**, and then click the **Event Logs** link.



The following table describes the Event Log information displayed on the screen.

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 GS728TS, GS728TPS, GS752TS, or GS752TPS 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.

Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear the messages out of the Event Log.
- Click **Refresh** to refresh the data on the screen and display the most current information.

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, click **Monitoring > Port Mirroring**.

Source Port	Destination Port	Session Mode	Direction	Mirroring Port
<input type="checkbox"/> 1/g1		Disable		
<input type="checkbox"/> 1/g2		Disable		
<input type="checkbox"/> 1/g3		Disable		
<input type="checkbox"/> 1/g4		Disable		
<input type="checkbox"/> 1/g5		Disable		
<input type="checkbox"/> 1/g6		Disable		
<input type="checkbox"/> 1/g7		Disable		
<input type="checkbox"/> 1/g8		Disable		
<input type="checkbox"/> 1/g9		Disable		

To configure Port Mirroring:

1. To configure port mirroring settings for a physical port, click the unit ID of the stack member with the ports to configure.
2. To configure port mirroring settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure port mirroring settings for both physical ports and LAGs, click **ALL**. Select the check box next to a port to configure it as a source port.

4. Alternatively, to configure settings for a specific interface, enter the interface ID in the **Go To Interface** and click **Go**.
5. Select the check box next to a port or LAG to configure it as a source port.
6. In the **Destination Port** field, specify the port to which port traffic is be copied. Use the <unit>/g<port> format to specify the port, for example 1/g1. You can configure only one destination port on the system.
7. From the **Session Mode** menu, select the mode for port mirroring on the selected port:
 - **Enable**. Multiple Port Mirroring is active on the selected port.
 - **Disable**. Port mirroring is not active on the selected port, but the mirroring information is retained. This is the default value.
8. Specify the traffic on the source port to monitor:
 - **Tx and Rx**: Both ingress and egress traffic.
 - **Tx only**: Egress traffic (traffic leaving the port) only.
 - **Rx only**: Ingress traffic (traffic entering the port) only.
9. Click **Apply** to apply the settings to the system.

***Note:** If the port is configured as a source port, the **Mirroring Port** field value is Mirrored.*

10. To delete a mirrored port, select the check box next to the mirrored port, and then click **Delete**.
11. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Maintaining the System

8

Use the features available from the Maintenance tab to help you manage the switch. The Maintenance tab contains links to the following features:

- [Reset](#) on page 280
- [Upload File From Switch](#) on page 282
- [Download File To Switch](#) on page 284
- [File Management](#) on page 288
- [Troubleshooting](#) on page 292

Reset

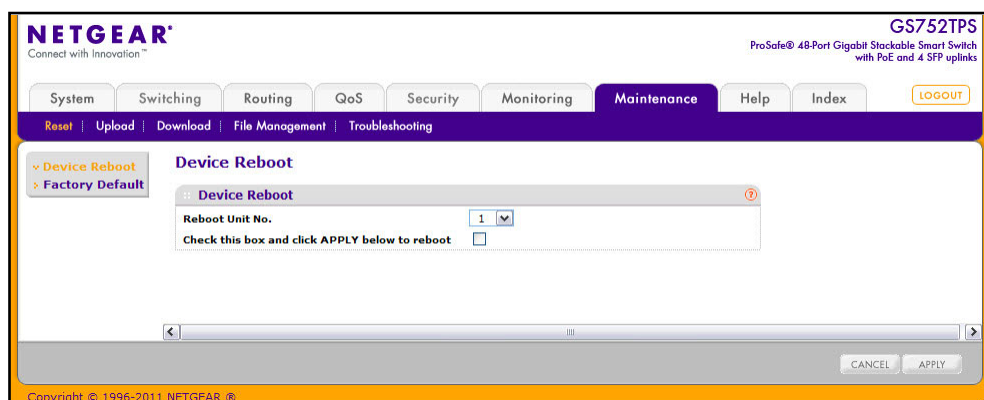
The **Reset** menu contains links to the following options:

- [Device Reboot](#) on page 280
- [Factory Default](#) on page 281

Device Reboot

Use the Device Reboot page to reboot a switch. If you are managing a stack of switches, you can use this page to reboot any stack member.

To access the Device Reboot page, click **Maintenance > Reset > Device Reboot**.



To reboot the switch:

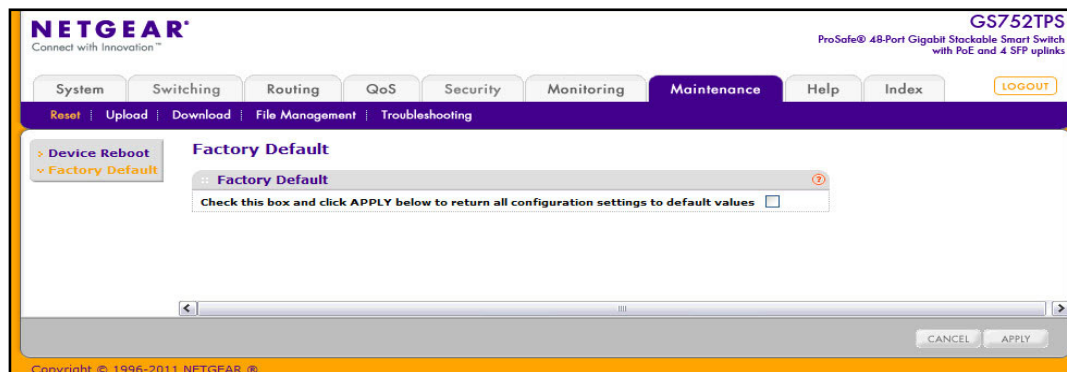
1. Select the Unit ID of the stack member to reboot, or select All to reboot all units in the stack.
2. Select the check box on the page.
3. Click **Apply** to reset the switch immediately, or click **Cancel** to abandon the reset request. After the switch reset begins, the management interface is not available until the switch completes the boot cycle. After the switch resets, the login screen appears.

Factory Default

Use the Factory Default page to reset the system configuration to the factory default values.

Note: If you reset the switch to the default configuration, the IP address is reset to 192.168.0.239, and the DHCP client is enabled. If you lose network connectivity after you reset the switch to the factory defaults, see [Connecting the Switch to the Network](#) on page 11.

To access the Factory Defaults page, click **Maintenance > Reset > Factory Default**.



To reset the switch to the factory default settings:

1. Select the check box on the page.
2. Click **Apply** to reset the switch immediately, or click **Cancel** to abandon the changes.

Upload File From Switch

The switch supports system file uploads from the switch to a remote system by using either TFTP or HTTP.

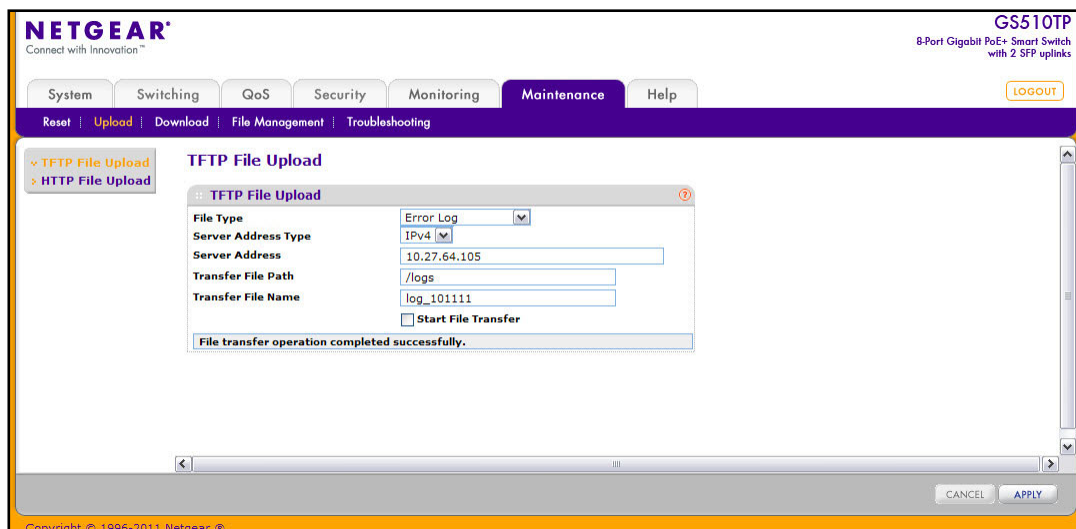
The **Upload** menu contains links to the following options:

- [TFTP File Upload](#) on page 282
- [HTTP File Upload](#) on page 283

TFTP File Upload

Use the TFTP File Upload page to upload configuration (ASCII), log (ASCII), and image (binary) files from the switch to the TFTP server.

To display the File Upload page, click **Maintenance > Upload > TFTP File Upload**.



To upload a file from the switch to the TFTP server:

1. Use the **File Type** menu to specify the type of file you want to upload:
 - **Archive:** Uploads a stored code image.
 - **Text Configuration:** Uploads the text configuration file.
 - **Error Log:** Uploads the system error (persistent) log, sometimes referred to as the event log.
 - **Buffered Log:** Uploads the system buffered (in-memory) log.
 - **Trap Log:** Uploads the system trap records.
2. If the file type is Archive, use the **Image Name** menu to specify whether to upload image1 or image2. This field is visible only when Archive is selected as the File Type.

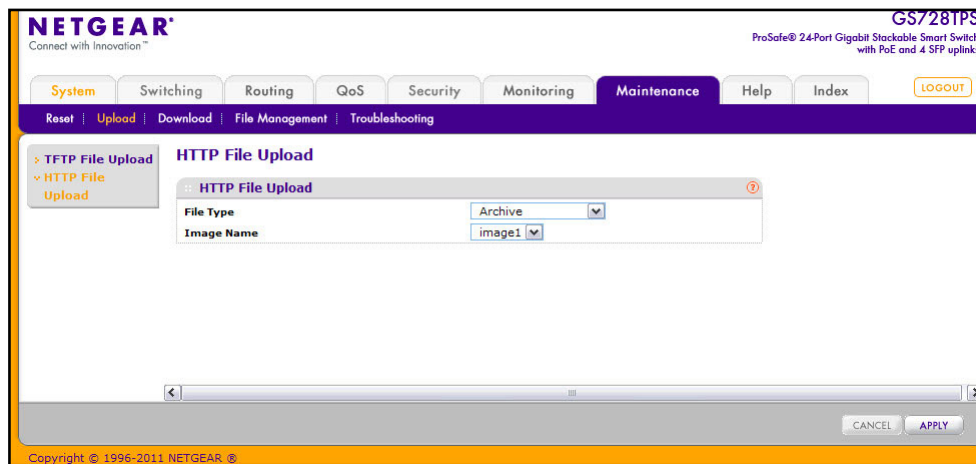
3. From the **Server Address Type** field, specify the format to use for the address you type in the TFTP Server Address field:
 - **IPv4**. Indicates the TFTP server address is an IP address in dotted-decimal format.
 - **DNS**. Indicates the TFTP server address is a hostname.
4. In the **Server Address** field, specify the IP address or hostname of the TFTP server. The address you type must be in the format indicated by the TFTP Server Address Type.
5. In the **Transfer File Path** field, specify the path on the TFTP server where you want to put the file. You may enter up to 96 characters. Include the backslash at the end of the path closest to the root. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.
6. In the **Transfer File Name** field, specify a destination file name for the file to upload. You may enter up to 32 characters. The transfer fails if you do not specify a file name. For a code transfer, use an *.stk* file extension.
7. Select the **Start File Transfer** check box to initiate the file upload.
8. Click **Apply** to begin the file transfer, or click **Cancel** to abandon the changes.

After the file transfer begins, the last row of the table displays information about the progress of the file transfer. The page refreshes automatically until the file transfer completes or fails.

HTTP File Upload

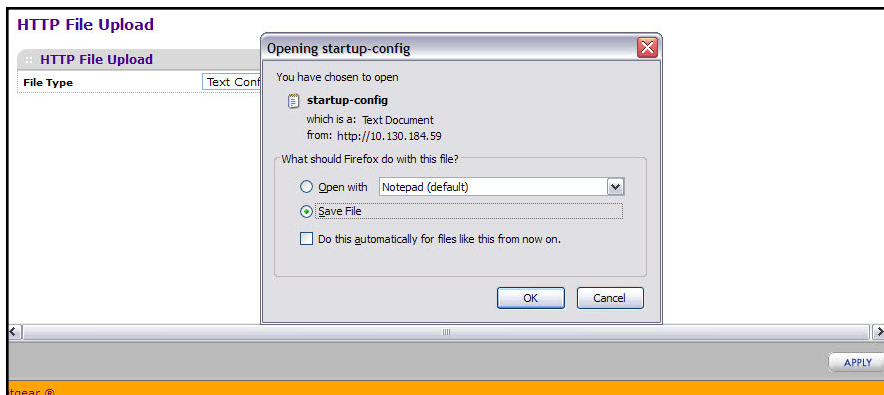
Use the HTTP File Upload page to upload files of various types from the switch to an administrative system using an HTTP session (for example, via your Web browser).

To display this page, click **Maintenance > Upload > HTTP File Upload**.



To upload a file from the switch to an administrative system by using HTTP:

1. From the **File Type** menu, Specify what type of file you want to download to the switch:
 - **Archive:** 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 the 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 (for example, change the device name, serial number, IP address), and download it to that device.
2. If you are uploading an image (Archive), use the **Image Name** field to select the image to upload (image1 or image2). This field is only visible when Archive is selected as the File Type.
3. Click **Apply** to open a window that allows you to either open the file or browse to a location on an administrative system and save the file.



4. Click **OK** to open or save the file to the selected location.

Download File To Switch

The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.

The **Download** menu contains links to the following options:

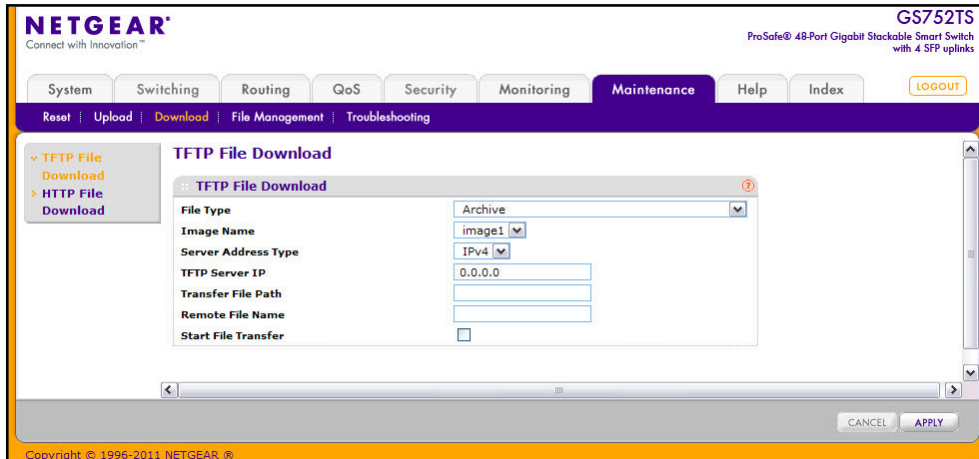
- [TFTP File Download](#) on page 285
- [HTTP File Download](#) on page 287

TFTP File Download

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 287 for additional information.

To access the TFTP File Download page, click **Maintenance > Download > TFTP File Download**.



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.

To download a file to the switch from a TFTP server:

1. From the **File Type** menu, Specify what type of file you want to download to the switch:
 - **Archive:** 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 the 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 (for example, change the device name, serial number, IP address), 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).
2. If you are downloading an image (Archive) file, select the image on the switch to overwrite from the Image Name field. This field is only visible when Archive is selected as the File Type.

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. From the **Server Address Type** field, specify the format for the address you type in the TFTP Server Address field
 - **IPv4.** Indicates the TFTP server address is an IP address in dotted-decimal format.
 - **DNS.** Indicates the TFTP server address is a hostname.
4. In the **Server Address** field, specify the IP address or hostname of the TFTP server. The address you type must be in the format indicated by the TFTP Server Address Type.
5. In the **Transfer File Path** field, specify the path on the TFTP server where the file is located. You may enter up to 96 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.
6. In the **Remote File Name** field, specify the name of the file to download from the TFTP server. You may enter up to 32 characters. A file name with a space is not accepted.
7. Select the **Start File Transfer** check box to initiate the file upload.
8. Click **Apply** to begin the file transfer, or click **Cancel** to abandon the transfer.

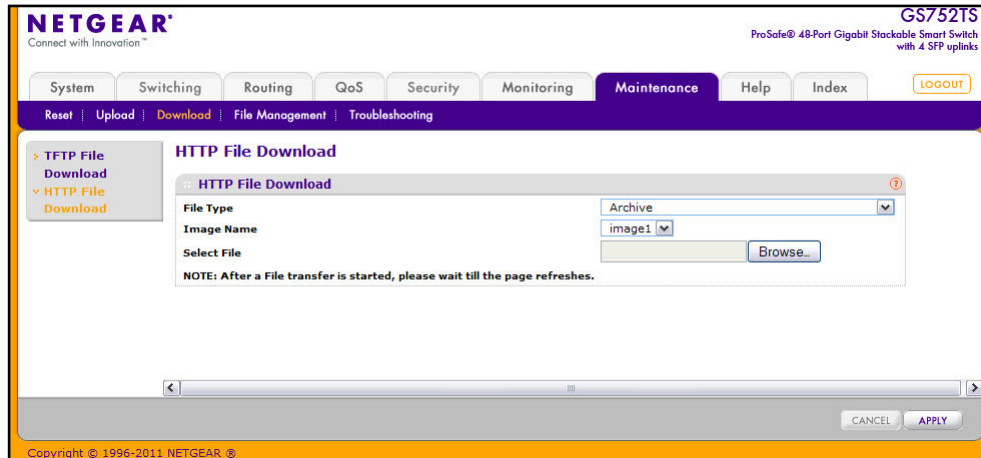
After the transfer starts, the last row of the table displays information about the progress of the file transfer. The page refreshes automatically until the file transfer completes or fails.

To activate a software image that you download to the switch, see [File Management](#) on page 288.

HTTP File Download

Use the HTTP File Download page to download files of various types to the switch using an HTTP session (for example, via your Web browser).

To display this page, click **Maintenance > Download > HTTP File Download**.



To download a file to the switch from by using HTTP:

- From the **File Type** menu, Specify what type of file you want to download to the switch:
 - Archive:** 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 the 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 (for example, change the device name, serial number, IP address), 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).
- If you are downloading an image (Archive), use the **Image Name** field to select the image to download (image1 or image2). This field is only visible when Archive is selected as the File Type.

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. Click **Browse** to open a window that allows you to locate the file you want to download.
4. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
5. 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.

File Management

The system maintains two versions of the GS728TS, GS728TPS, GS752TS, or GS752TPS 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 or downgrading the GS728TS, GS728TPS, GS752TS, or GS752TPS software.

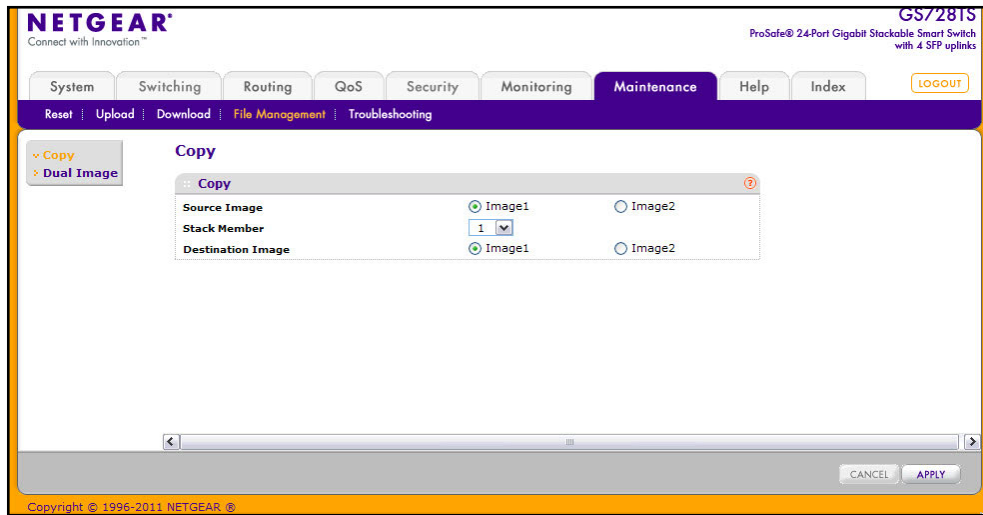
The **File Management** menu contains links to the following options:

- [Copy](#) on page 288
- [Dual Image Configuration](#) on page 289
- [Dual Image Status](#) on page 291

Copy

Use the Copy page to copy an image from the stack master to another stack member or all stack members. You can also copy one image to the other on the stack master (e.g. copy image1 to image2).

To display the Copy page, click **Maintenance > File Management > Copy**.



To copy an image:

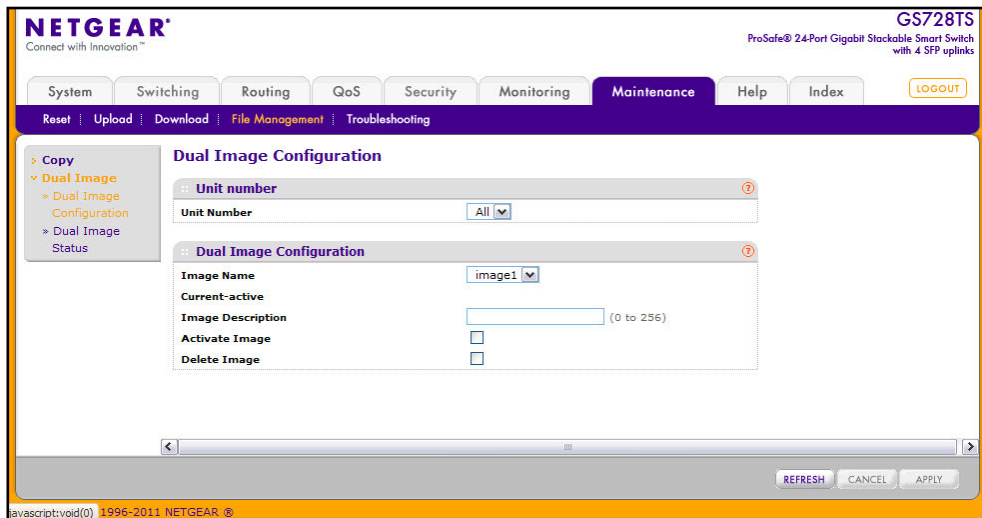
1. Use the **Source Image** field to select the image on the stack master to use as the source. The source image overwrites the destination image, if it exists.
2. Use the **Stack Member** menu to select the destination unit to which you are going to copy the image. To copy the selected image from the stack master to all stack members, select **All**.
3. Use the **Destination Image** field to determine which image on the stack member(s) to overwrite (if an image currently exists in the selected destination). The image on the stack master is copied to the destination you select.
4. Click **Cancel** to cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch.
5. Click **Apply** to initiate the file transfer from the stack master to the selected stack member.

Dual Image Configuration

The system running a legacy 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, configure an image description, or delete an image.

To display the Dual Image Configuration page, click **Maintenance > File Management > Dual Image > Dual Image Configuration**.



To configure Dual Image settings:

1. Select the ID of the stack member to configure, or select **All** to configure all units in the stack with the same dual image settings.
2. Select the image to configure.
The **Current-active** field displays the name of the active image.
3. To configure a descriptive name for the selected software image, type the name in the **Image Description** field.
4. To set the selected image as the active image, select the **Active Image** check box.

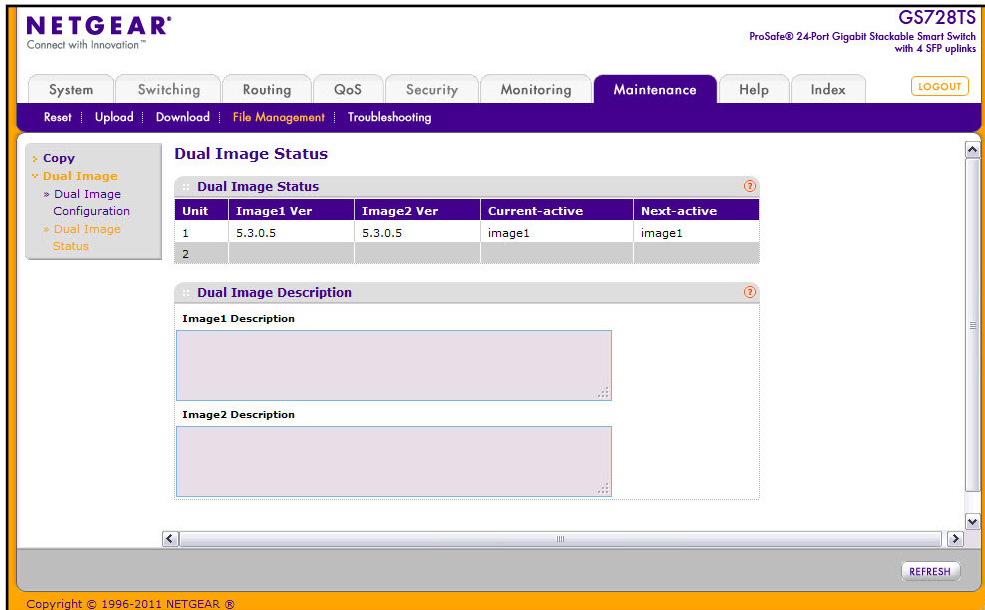
Note: After activating an image, you must perform a system reset of the stack in order to run the new code.

5. To remove the selected image from permanent storage on the switch, select the **Delete Image** check box. 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 apply the settings to the switch.

Dual Image Status

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, click **Maintenance > File Management > Dual Image > Dual Image Status**.



The following table describes the information on the Dual Image Status page.

Field	Description
Unit	The unit ID of the switch is always 1.
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 switch.
Next-active	Displays the image to be used on the next restart of this switch.
Image1 Description	Displays the description associated with the image1 code file.
Image2 Description	Displays the description associated with the image2 code file.

Click **Refresh** to display the latest information from the switch.

For information about how to update or change the system images, see [File Management](#) on page 288.

Troubleshooting

The **Troubleshooting** menu contains links to the following options:

- [Ping](#) on page 292
- [Ping IPv6](#) on page 293
- [Traceroute](#) on page 294

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, click **Maintenance > Troubleshooting > Ping**.

The screenshot shows the Netgear web interface for a GS752TPS switch. The top navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Maintenance menu is expanded to show Troubleshooting, which includes Ping, Ping IPv6, and Traceroute. The Ping Details form has the following fields:

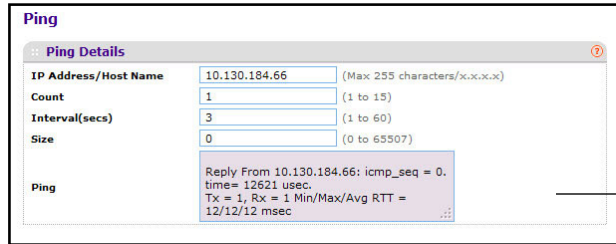
IP Address/Host Name	<input type="text"/>	(Max: 255 characters/x.x.x.x)
Count	<input type="text" value="1"/>	(1 to 15)
Interval(secs)	<input type="text" value="3"/>	(1 to 60)
Size	<input type="text" value="0"/>	(0 to 65507)

Below the form is a Ping status area and CANCEL/APPLY buttons at the bottom right.

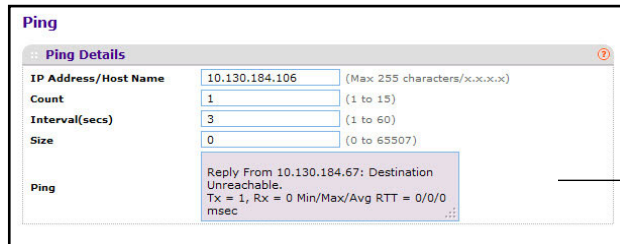
To configure the settings and ping a host on the network:

1. In the **Hostname/IP Address** field, specify the IP address or the hostname of the station you want the switch to ping. The initial value is blank. This information is not retained across a power cycle.
2. Optionally, configure the following settings:
 - **Count.** Specify the number of pings to send. The valid range is 1–15.
 - **Interval.** Specify the number of seconds between pings sent. The valid range is 1–60.
 - **Size.** Specify the size of the ping (ICMP) packet to send. The valid range is 0–65507.
3. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.

4. Click **Apply** to send the ping. The switch sends the number of pings specified in the **Count** field, and the results are displayed below the configurable data in the **Ping** area.
 - 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”.



Ping Success Message

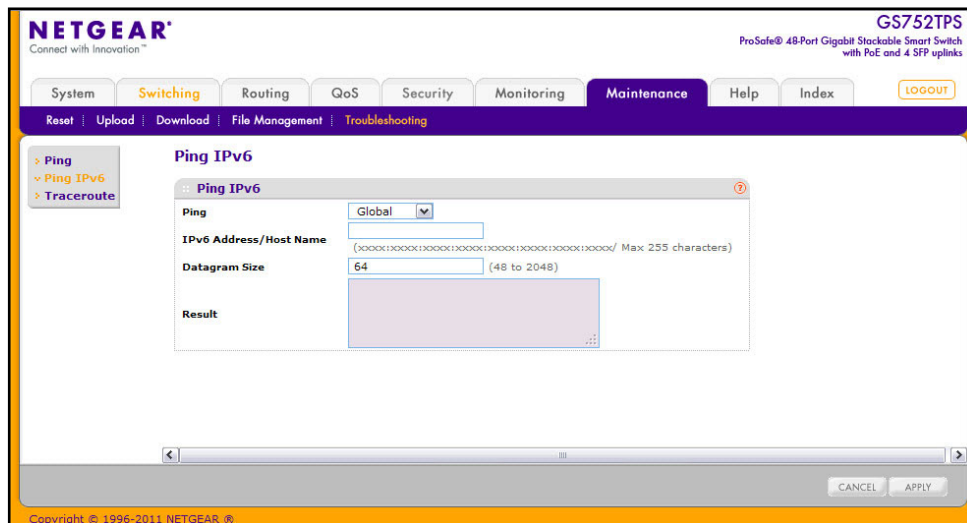


Ping Unsuccessful Message

Ping IPv6

Use the Ping IPv6 page to send a Ping request to a specified Hostname or IPv6 address. You can use this to check whether the switch can communicate with a particular IPv6 station. When you click the **Apply** button, the switch will send three pings and the results will be displayed below the configurable data.

To access the Ping IPv6 page, click **Maintenance > Troubleshooting > Ping IPv6**.



To configure the settings and ping a host on the network:

1. In the **Ping** field, select either Global or Link Global to select either the global IPv6 Address/Hostname or Link Local Address to ping.
2. Optionally, configure the following settings:
 - In the **IPv6 Address/Host Name** field, enter the IPv6 address or Hostname of the station you want the switch to ping. The initial value is blank. The IPv6 Address or Hostname you enter is not retained across a power cycle.
 - In the **Datagram Size** field, specify the size of the datagram to send. The valid range is 48–2048.
 - The **Result** field displays the result after the switch send a Ping IPv6 request to the specified IPv6 address.
3. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
4. Click **Apply** to send the ping. The switch sends the number of pings specified in the **Count** field, and the results are displayed below the configurable data in the **Result** area.
 - If successful, the output will be Send count=3, Receive count = *n* from (IPv6 Address).Average round trip time = *n* ms.
 - If a reply to the ping is not received, the following displays: “Reply From IP/Host: Destination Unreachable. Tx = *x*, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec”.

Traceroute

Use the Traceroute utility to discover the paths that a packet takes to a remote destination.

To display this page, click **Maintenance > Troubleshooting > Traceroute**.

The screenshot shows the Netgear web interface for a GS752TPS switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Maintenance section is active, and the Traceroute utility is selected. The configuration fields are as follows:

Field	Value	Range
IP Address/Hostname		(Max: 255 Characters/x.x.x.x)
Probes Per Hop	3	(1 to 10)
Max TTL	30	(1 to 255)
Init TTL	1	(1 to 255)
Maxfail	5	(0 to 255)
Interval	3	(1 to 60)
Port	33434	(1 to 65535)
Size	0	(0 to 65507)

The Results section shows the following output:

```

1 10.27.34.1 3 ms 2 ms 3 ms
2 66.194.17.9 69 ms 4 ms 4 ms
3 66.192.246.82 43 ms 15 ms 15 ms
4 0.0.0.0 0 ms 0 ms 0 ms
5 0.0.0.0 0 ms 0 ms 0 ms
Hop Count = 4 Last TTL = 5 Test attempt = 14 Test Success = 9
  
```

At the bottom of the interface, there are CANCEL and APPLY buttons.

To configure the Traceroute settings and send probe packets to discover the route to a host on the network:

1. In the **Hostname/IP Address** field, specify the IP address or the hostname of the station you want the switch to ping. The initial value is blank. This information is not retained across a power cycle.
2. Optionally, configure the following settings:
 - **Probes Per Hop**. Specify the number of times each hop should be probed. The valid range is 1–10.
 - **MaxTTL**. Specify the maximum time-to-live for a packet in number of hops. The valid range is 1–255.
 - **InitTTL**. Specify the initial time-to-live for a packet in number of hops. The valid range is 1–255.
 - **MaxFail**. Specify the maximum number of failures allowed in the session. The valid range is 0–255.
 - **Interval**. Specify the time between probes in seconds. The valid range is 1–60.
 - **Port**. Specify the UDP destination port in probe packets. The valid range is 1–65535.
 - **Size**. Specify the size of probe packets. The valid range is 0–9192.
3. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
4. Click **Apply** to initiate the traceroute. The results display in the TraceRoute area.

Accessing Help

9

Use the features available from the Help tab to connect to online resources for assistance. The **Help** tab contains links to the following features:

- *Online Help* on page 296
- *Registration* on page 298.

Online Help

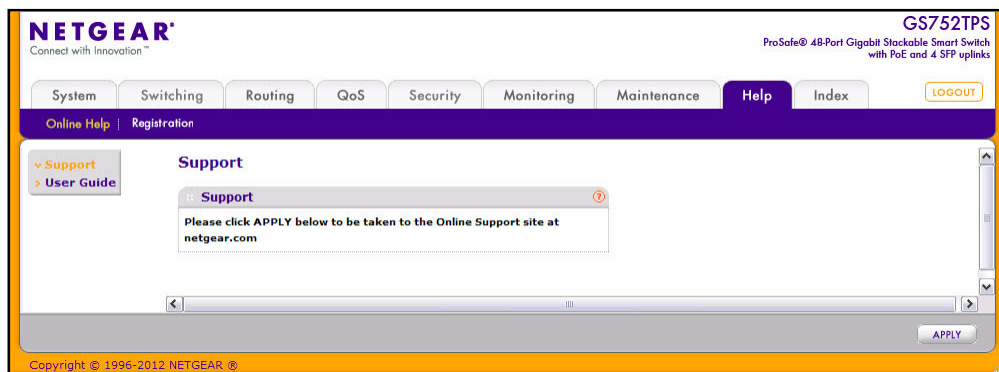
The Online Help includes the following pages:

- *Support* on page 296
- *User Guide* on page 297

Support

Use the Support page to connect to the Online Support site at netgear.com.

To access the Support page, click **Help > Online Help > Support**.

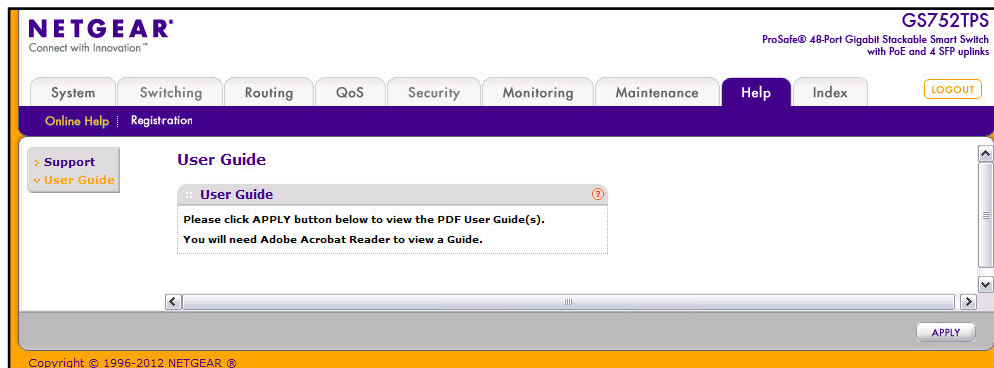


To connect to the NETGEAR support site for the GS728TS, GS728TPS, GS752TS, or GS752TPS, click **Apply**.

User Guide

Use the User Guide page to access the *GS728TS, GS728TPS, GS752TS, and GS752TPS Smart Switch Software Administration Manual* (the guide you are now reading) that is available on the NETGEAR Website.

To access the User Guide page, click **Help > Online Help > User Guide**.



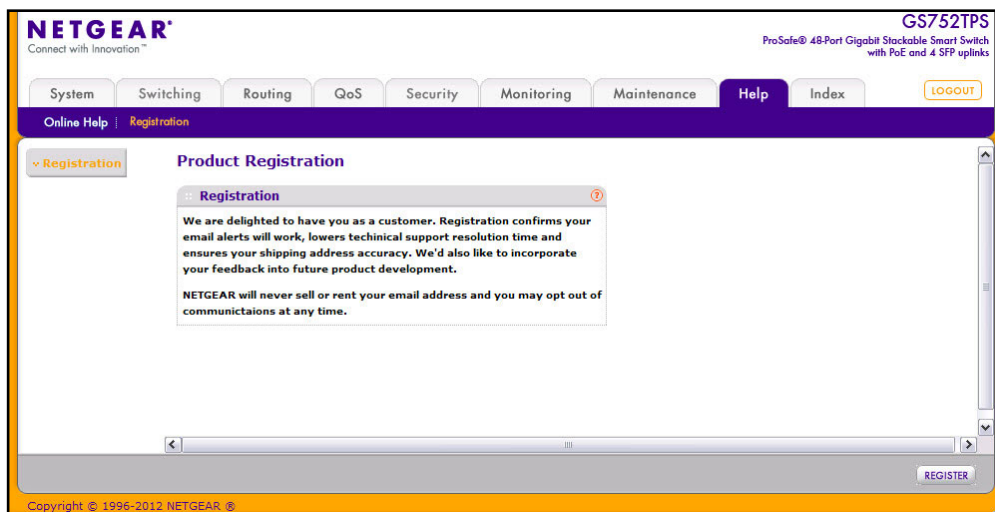
To access to the User Guide that is available online, click **Apply**.

Registration

Use the Registration page to register your GS728TS, GS728TPS, GS752TS, or GS752TPS switch. Completing the registration confirms your email address, lowers technical support resolution time, and ensures your shipping address accuracy. NETGEAR, Inc. would also like to incorporate your feedback into future product development.

Note: NETGEAR will never sell or rent your email address, and you may opt out of communications at any time.

To access the Registration page, click **Help > Registration**.



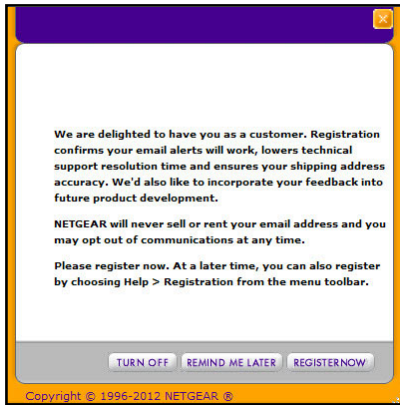
To register the switch, click **Register**. The switch attempts to contact the NETGEAR Registration Server.

For the product registration process to proceed, the administrative system running the browser must meet the following requirements:

- The administrative system must have Internet access.
- The browser must allow pop up windows.
- If the browser is Microsoft® Internet Explorer, ActiveX must be enabled.

If the switch successfully contacts the Registration Server, the NETGEAR Product Registration page opens in a new browser window. The product serial number and model number fields are pre populated. After you provide some basic information and click **Register**, the registration process is complete.

If you have not registered the product or have not disabled the registration reminders, the following pop-up window appears each time a user successfully logs on to the switch:



The registration pop-up window includes the following buttons:

- **TURN OFF.** Use this button to turn off the Product Registration feature and to prevent the registration reminder pop-up window from appearing on subsequent successful login sessions.
- **REMIND ME LATER.** The pop-up window is closed without taking any action, and the registration reminder pop-up appears on next successful login.
- **REGISTER NOW.** The NETGEAR Registration Server is contacted to initiate the registration process.

Hardware Specifications and Default Values



Switch Specifications

The GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches conform to the TCP/IP, UDP, HTTP, ICMP, TFTP, DHCP, IEEE 802.1D, IEEE 802.1p, and IEEE 802.1Q standards.

GS728TS Specifications

Feature	Value
Interfaces	24 copper 10/100/1000M Ethernet ports 2 combo ports: 10/100/1000M copper or 1G/100M optical 2 SFP 1G optical ports (port 25 and 26) 2 SFP ports (port 27 and 28) for 1G optical uplink or 2.5G optical stacking
Flash memory size	32 MB
SRAM size and type	128MB DDR2 SDRAM

GS728TPS Specifications

Feature	Value
Interfaces	24 copper 10/100/1000M PoE Ethernet ports (8 PoE+) 2 combo ports: 10/100/1000M copper or 1G/100M optical 2 SFP 1G optical ports (port 25 and 26) 2 SFP ports (port 27 and 28) for 1G optical uplink or 2.5G optical stacking
Flash memory size	32 MB
SRAM size and type	128MB DDR2 SDRAM

GS752TS Specifications

Feature	Value
Interfaces	48 copper 10/100/1000M Ethernet ports 2 combo ports: 10/100/1000M copper or 1G/100M optical 2 SFP 1G optical ports (port 49 and 50) 2 SFP ports (port 51 and 52) for 1G optical uplink or 2.5G optical stacking
Flash memory size	32 MB
SRAM size and type	128MB DDR2 SDRAM

GS752TPS Specifications

Feature	Value
Interfaces	48 copper 10/100/1000M PoE Ethernet ports (8 PoE+) 2 combo ports: 10/100/1000M copper or 1G/100M optical 2 SFP 1G optical ports (port 49 and 50) 2 SFP ports (port 51 and 52) for 1G optical uplink or 2.5G optical stacking
Flash memory size	32 MB
SRAM size and type	128MB DDR2 SDRAM

Switch Performance

Feature	Value
Switching capacity	Non-Blocking Full WireSpeed on all packet sizes
Forwarding method	Store and Forward
Packet forwarding rate	10M:14,880 pps/ 100M:148,800 pps/ 1G:1,488,000 pps
MAC addresses	16K
Green Ethernet	Automatic power down on port when link is down, short cable mode and EEE mode

Switch Features and Defaults

Port Characteristics

Feature	Sets Supported	Default
Auto negotiation/static speed/duplex	All ports	Auto negotiation
Auto MDI/MDIX	N/A	Enabled
802.3x flow control/back pressure	1 (per system)	Disabled
Port mirroring	1	Disabled
Port trunking (aggregation)	8	Pre-configured
802.1D spanning tree	1	Disabled
802.1w RSTP	1	Disabled
802.1s spanning tree	5 instances	Disabled
Static 802.1Q tagging	256	VID = 1 Max member ports are: 28/52 for standalone switch 300 for 6-unit stacking switch
Learning process	Supports static and dynamic MAC entries	Dynamic learning is enabled by default

Traffic Control

Feature	Sets Supported	Default
Storm control	All ports	Disabled
Jumbo frame	All ports	Disabled Max = 9216 bytes

Quality of Service

Feature	Sets Supported	Default
Number of queues	7	N/A
Port based	N/A	N/A
802.1p	1	Enabled
DSCP	1	Disabled
Rate limiting	All ports	Disabled
Auto-QoS	All ports	Disabled

Security

Feature	Sets Supported	Default
802.1X	All ports	Disabled
MAC ACL	100 (shared with IP and IPv6 ACLs)	All MAC addresses allowed
IP ACL	100 (shared with MAC and IPv6 ACLs)	All IP addresses allowed
IPv6 ACL	100 (shared with IP ACL and MAC ACL)	All IP addresses allowed
Password control access	1	Idle timeout = 5 mins. Password = "password"
Management security	1 profile with 20 rules for HTTP/HTTPS/SNMP access to allow/deny an IP address/subnet	All IP addresses allowed
Port MAC lock down	All ports	Disabled

System Setup and Maintenance

Feature	Sets Supported	Default
Boot code update	1	N/A
DHCP/manual IP	1	DHCP enabled/192.168.0.239
Default gateway	1	192.168.0.254
System name configuration	1	NULL
Configuration save/restore	1	N/A
Firmware upgrade	1	N/A
Restore defaults	1 (Web and front-panel button)	N/A
Dual image support	1	Enabled
Factory reset	1	N/A

System Management

Feature	Sets Supported	Default
Multi-session Web connections	16	Enabled
SNMPv1/V2c SNMP v3	Max 5 community entries	Enabled (read, read-write communities)
Time control	1 (Local or SNTP)	Local Time enabled
LLDP/LLDP-MED	All ports	Disabled
Logging	3 (Memory/Flash/Server)	Memory Log enabled
MIB support	1	Disabled
Smart Control Center	N/A	Enabled
Statistics	N/A	N/A

Other Features

Feature	Sets Supported	Default
IGMP snooping v1/v2/v3	All ports	Disabled
Configurations upload/download	1	N/A
EAPoL flooding	All ports	Disabled
BPDU flooding	All ports	Disabled
Static multicast groups	8	Disabled
Filter multicast control	1	Disabled
Number of static routes	32	N/A
Number of routed VLANs	15	N/A
Number of ARP Cache entries	1024	N/A
Number of DHCP snooping bindings	8K	N/A
Number of DHCP static entries	1024	N/A
MLD Snooping	N/A	Disabled
Protocol and MAC-based VLAN	N/A	N/A
Timer Schedule entries	100 (max of 10 periodic and 1 absolute entry per timer schedule entry)	N/A

Configuration Examples

B

This chapter contains information about how to configure the following features:

- *Virtual Local Area Networks (VLANs)* on page 306
- *Access Control Lists (ACLs)* on page 308
- *Differentiated Services (DiffServ)* on page 311
- *802.1X* on page 315
- *MSTP* on page 318
- *Configuring VLAN Routing* on page 322

Virtual Local Area Networks (VLANs)

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

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

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

VLANs have a number of advantages:

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

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

- When an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID tag number. Each port has a default VLAN ID setting that is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed in the Port PVID Configuration screen. See [Port VLAN ID Configuration](#) on page 113.
- When a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID setting. The packet proceeds to the VLAN specified by its VLAN ID tag number.
- If the port through which the packet entered does not have membership with the VLAN specified by the VLAN ID tag, the packet is dropped.
- If the port is a member of the VLAN specified by the packet's VLAN ID, the packet can be sent to other ports with the same VLAN ID.
- Packets leaving the switch are either tagged or untagged, depending on the setting for that port's VLAN membership properties. A U for a given port means that packets leaving the switch from that port are untagged. Inversely, a T for a given port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

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

VLAN Example Configuration

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

In this example, you create two new VLANs, change the port membership for default VLAN 1, and assign port members to the two new VLANs:

1. In the Basic VLAN Configuration screen (see [VLAN Configuration](#) on page 110), create the following VLANs:
 - A VLAN with VLAN ID 10.
 - A VLAN with VLAN ID 20.

2. In the VLAN Membership screen (see [VLAN Membership Configuration](#) on page 112) specify the VLAN membership as follows:
 - For the default VLAN with VLAN ID 1, specify the following members: port 7 (U) and port 8 (U).
 - For the VLAN with VLAN ID 10, specify the following members: port 1 (U), port 2 (U), and port 3 (T).
 - For the VLAN with VLAN ID 20, specify the following members: port 4 (U), port 5 (T), and port 6 (U).
3. In the Port PVID Configuration screen (see [Port VLAN ID Configuration](#) on page 113), specify the PVID for ports 1 and 4 so that packets entering these ports are tagged with the port VLAN ID:
 - Port 1: PVID 10
 - Port 4: PVID 20
4. With the VLAN configuration that you set up, the following situations produce results as described:
 - If an untagged packet enters port 1, the switch tags it with VLAN ID 10. The packet has access to port 2 and port 3. The outgoing packet is stripped of its tag to leave port 2 as an untagged packet. For port 3, the outgoing packet leaves as a tagged packet with VLAN ID 10.
 - If a tagged packet with VLAN ID 10 enters port 3, the packet has access to port 1 and port 2. If the packet leaves port 1 or port 2, it is stripped of its tag to leave the switch as an untagged packet.
 - If an untagged packet enters port 4, the switch tags it with VLAN ID 20. The packet has access to port 5 and port 6. The outgoing packet is stripped of its tag to become an untagged packet as it leaves port 6. For port 5, the outgoing packet leaves as a tagged packet with VLAN ID 20.

Access Control Lists (ACLs)

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 provide security for the network. ACLs are normally used in firewall routers that are positioned between the internal network and an external network, such as the Internet. They can also be used on a router positioned between two parts of the network to control the traffic entering or exiting a specific part of the internal network. The added packet processing required by the ACL feature does not affect switch performance. That is, ACL processing occurs at wire speed.

Access lists are a sequential collection of permit and deny conditions. This collection of conditions, known as the filtering criteria, is applied to each packet that is processed by the switch or the router. The forwarding or dropping of a packet is based on whether or not the packet matches the specified criteria.

Traffic filtering requires the following two basic steps:

1. Create an access list definition.

The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can assign traffic that matches the criteria to a particular queue or redirect the traffic to a particular port. A default *deny all* rule is the last rule of every list.

2. Apply the access list to an interface in the inbound direction.

GS728TS, GS728TPS, GS752TS, and GS752TPS Smart Switches allow ACLs to be bound to physical ports and LAGs. The switch software supports MAC ACLs and IP ACLs.

MAC ACL Example Configuration

The following example shows how to create a MAC-based ACL that permits Ethernet traffic from the Sales department on specified ports and denies all other traffic on those ports.

1. From the MAC ACL screen, create an ACL with the name Sales_ACL for the Sales department of your network (See [MAC ACL](#) on page 237).

By default, this ACL will be bound on the inbound direction, which means the switch will examine traffic as it enters the port.

2. From the MAC Rules screen, create a rule for the Sales_ACL with the following settings:

- ID: 1
- Action: Permit
- Assign Queue: 0
- Match Every: False
- CoS: 0
- Destination MAC: 01:02:1A:BC:DE:EF
- Destination MAC Mask: 00:00:00:00:FF:FF
- Source MAC: 02:02:1A:BC:DE:EF
- Source MAC Mask: 00:00:00:00:FF:FF
- VLAN ID: 2

For more information about MAC ACL rules, see [MAC Rules](#) on page 238.

3. From the MAC Binding Configuration screen, assign the Sales_ACL to the interface gigabit ports 6, 7, and 8, and then click **Apply** (See [MAC Binding Configuration](#) on page 240).

You can assign an optional sequence number to indicate the order of this access list relative to other access lists if any are already assigned to this interface and direction.

4. The MAC Binding Table displays the interface and MAC ACL binding information (See [MAC Binding Table](#) on page 241).

The ACL named Sales_ACL looks for Ethernet frames with destination and source MAC addresses and MAC masks defined in the rule. Also, the frame must be tagged with VLAN ID

2, which is the Sales department VLAN. The CoS value of the frame must be 0, which is the default value for Ethernet frames. Frames that match this criteria are permitted on interfaces 6, 7, and 8 and are assigned to the hardware egress queue 0, which is the default queue. All other traffic is explicitly denied on these interfaces. To allow additional traffic to enter these ports, you must add a new *permit* rule with the desired match criteria and bind the rule to interfaces 6, 7, and 8.

Standard IP ACL Example Configuration

The following example shows how to create an IP-based ACL that prevents any IP traffic from the Finance department from being allowed on the ports that are associated with other departments. Traffic from the Finance department is identified by each packet's network IP address.

1. From the IP ACL screen, create a new IP ACL with an IP ACL ID of 1 (See [IP ACL](#) on page 242).
2. From the IP Rules screen, create a rule for IP ACL 1 with the following settings:
 - Rule ID: 1
 - Action: Deny
 - Assign Queue ID: 0 (optional: 0 is the default value)
 - Match Every: False
 - Source IP Address: 192.168.187.0
 - Source IP Mask: 255.255.255.0

For additional information about IP ACL rules, see [IP Rules](#) on page 243.

3. Click **Add**.
4. From the IP Rules screen, create a second rule for IP ACL 1 with the following settings:
 - Rule ID: 2
 - Action: Permit
 - Match Every: True
5. Click **Add**.
6. From the IP Binding Configuration page, assign ACL ID 1 to the interface gigabit ports 2, 3, and 4, and assign a sequence number of 1 (See [IP Binding Configuration](#) on page 252).

By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch.
7. Click **Apply**.
8. Use the IP Binding Table screen to view the interfaces and IP ACL binding information (See [IP Binding Table](#) on page 254).

The IP ACL in this example matches all packets with the source IP address and subnet mask of the Finance department's network and deny it on the Ethernet interfaces 2, 3, and 4 of the switch. The second rule permits all non-Finance traffic on the ports. The second rule is required because there is an explicit *deny all* rule as the lowest priority rule.

Differentiated Services (DiffServ)

Standard IP-based networks are designed to provide *best effort* data delivery service. *Best effort* service implies that the network deliver 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. However, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide 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. If one node is unable to meet the necessary timing requirements, this creates a deficiency in the network path and the performance of the entire packet flow is compromised.

There are two basic types of QoS:

- **Integrated Services:** network resources are apportioned based on request and are reserved (resource reservation) according to network management policy (RSVP, for example).
- **Differentiated Services:** network resources are apportioned based on traffic classification and priority, giving preferential treatment to data with strict timing requirements.

The GS728TS, GS728TPS, GS752TS, and GS752TPS switches support DiffServ.

The DiffServ feature contains a number of conceptual QoS building blocks you can use to construct a differentiated service network. Use these same blocks in different ways to build other types of QoS architectures.

There are 3 key QoS building blocks needed to configure DiffServ:

- Class
- Policy
- Service (i.e., the assignment of a policy to a directional interface)

Class

You can classify incoming packets at layers 2, 3 and 4 by inspecting the following information for a packet:

- Source/destination MAC address
- EtherType
- Class of Service (802.1p priority) value (first/only VLAN tag)
- VLAN ID range (first/only VLAN tag)
- Secondary 802.1p priority value (second/inner VLAN tag)
- Secondary VLAN ID range (second/inner VLAN tag)
- IP Service Type octet (also known as: ToS bits, Precedence value, DSCP value)
- Layer 4 protocol (TCP, UDP etc.)
- Layer 4 source/destination ports
- Source/destination IP address

From a DiffServ point of view, there are two types of classes:

- DiffServ traffic classes
- DiffServ service levels/forwarding classes

DiffServ Traffic Classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multi-field (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

You can combine these classifiers with logical AND or OR operations to build complex MF-classifiers (by specifying a class type of *all* or *any*, respectively). That is, within a single class, multiple match criteria are grouped together as an AND expression or a sequential OR expression, depending on the defined class type. Only classes of the same type can be nested; class nesting does not allow for the negation (i.e., *exclude* option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a given DSCP value, on the egress interface. These service levels are defined by configuring BA classes for each.

Creating Policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, there are two types of policies:

- **Traffic Conditioning Policy:** a policy applied to a DiffServ traffic class
- **Service Provisioning Policy:** a policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

Traffic Conditioning Policy

Traffic conditioning pertains to actions performed on incoming traffic. There are several distinct QoS actions associated with traffic conditioning:

- **Dropping:** drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
- **Marking IP DSCP or IP Precedence:** marking/re-marking the DiffServ code point in a packet with the DSCP value representing the service level associated with a particular DiffServ traffic class. Alternatively, the IP Precedence value of the packet can be marked/re-marked.
- **Marking CoS (802.1p):** sets the three-bit priority field in the first/only 802.1p header to a specified value when packets are transmitted for the traffic class. An 802.1p header is inserted if it does not already exist. This is useful for assigning a layer 2 priority level based on a DiffServ forwarding class (i.e., DSCP or IP Precedence value) definition to convey some QoS characteristics to downstream switches which do not routinely look at the DSCP value in the IP header.
- **Policing:** a method of constraining incoming traffic associated with a particular class so that it conforms to the terms of the TCS. Special treatment can be applied to out-of-profile packets that are either in excess of the conformance specification or are non-conformant. The DiffServ feature supports the following types of traffic policing treatments (actions):
 - drop: the packet is dropped
 - mark cos: the 802.1p user priority bits are (re)marked and forwarded
 - mark dscp: the packet DSCP is (re)marked and forwarded
 - mark prec: the packet IP Precedence is (re)marked and forwarded
 - send: the packet is forwarded without DiffServ modification

Color Mode Awareness: Policing in the DiffServ feature uses either *color blind* or *color aware* mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome. An auxiliary traffic class is used in conjunction with the policing definition to specify a value for one of the 802.1p, Secondary 802.1p, IP DSCP, or IP

Precedence fields designating the incoming color value to be used as the conforming color. The color of exceeding traffic may be optionally specified as well.

- **Counting:** updating octet and packet statistics to keep track of data handling along traffic paths within DiffServ. In this DiffServ feature, counters are not explicitly configured by the user, but are designed into the system based on the DiffServ policy being created. See the Statistics section of this document for more details.
- **Assigning QoS Queue:** directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
- **Redirecting:** forces classified traffic stream to a specified egress port (physical or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

DiffServ Example Configuration

To create a DiffServ Class/Policy and attach it to a switch interface, follow these steps:

1. From the QoS Class Configuration screen, create a new class with the following settings:
 - Class Name: Class1
 - Class Type: All

For more information about this screen, see [Class Configuration](#) on page 186.

2. Click the Class1 hyperlink to view the DiffServ Class Configuration screen for this class.
3. Configure the following settings for Class1:
 - Protocol Type: UDP
 - Source IP Address: 192.12.1.0
 - Source Mask: 255.255.255.0
 - Source L4 Port: Other, and enter 4567 as the source port value
 - Destination IP Address: 192.12.2.0
 - Destination Mask: 255.255.255.0
 - Destination L4 Port: Other, and enter 4568 as the destination port value

For more information about this screen, see [Class Configuration](#) on page 186.

4. Click **Apply**.
5. From the Policy Configuration screen, create a new policy with the following settings:
 - Policy Selector: Policy1
 - Member Class: Class1

For more information about this screen, see [Policy Configuration](#) on page 191.

6. Click **Add** to add the new policy.
7. Click the Policy1 hyperlink to view the Policy Class Configuration screen for this policy.

8. Configure the Policy attributes as follows:

- Assign Queue: 3
- Policy Attribute: Simple Policy
- Color Mode: Color Blind
- Committed Rate: 1000000 Kbps
- Committed Burst Size: 128 KB
- Confirm Action: Send
- Violate Action: Drop

For more information about this screen, see [Policy Configuration](#) on page 191.

9. From the Service Configuration screen, select the check box next to interfaces g7 and g8 to attach the policy to these interfaces, and then click **Apply** (See [Service Configuration](#) on page 195).

All UDP packet flows destined to the 192.12.2.0 network with an IP source address from the 192.12.1.0 network that have a Layer 4 Source port of 4567 and Destination port of 4568 from this switch on ports 7 and 8 are assigned to hardware queue 3.

On this network, traffic from streaming applications uses UDP port 4567 as the source and 4568 as the destination. This real-time traffic is time sensitive, so it is assigned to a high-priority hardware queue. By default, data traffic uses hardware queue 0, which is designated as a best-effort queue.

Also the *confirmed action* on this flow is to send the packets with a committed rate of 1000000 Kbps and burst size of 128 KB. Packets that violate the committed rate and burst size are dropped.

802.1X

Local Area Networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments, it may be desirable to restrict access to the services offered by the LAN to those users and devices that are permitted to use those services.

Port-based network access control makes use of the physical characteristics of LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics and of preventing access to that port in cases in which the authentication and authorization process fails. In this context, a port is a single point of attachment to the LAN, such as ports of MAC bridges and associations between stations or access points in IEEE 802.11 Wireless LANs.

The IEEE 802.11 standard describes an architectural framework within which authentication and consequent actions take place. It also establishes the requirements for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

The GS728TS, GS728TPS, GS752TS, and GS752TPS switches support a guest VLAN, which allows unauthenticated users to have limited access to the network resources.

Note: You can use QoS features to provide rate limiting on the guest VLAN to limit the network resources the guest VLAN provides.

Another 802.1X feature is the ability to configure a port to Enable/Disable EAPoL packet forwarding support. You can disable or enable the forwarding of EAPoL when 802.1X is disabled on the device.

The ports of an 802.1X authenticator switch provide the means in which it can offer services to other systems reachable via the LAN. Port-based network access control allows the operation of a switch's ports to be controlled in order to ensure that access to its services is only permitted by systems that are authorized to do so.

Port access control provides a means of preventing unauthorized access by supplicants to the services offered by a system. Control over the access to a switch and the LAN to which it is connected can be desirable in order to restrict access to publicly accessible bridge ports or to restrict access to departmental LANs.

Access control is achieved by enforcing authentication of supplicants that are attached to an authenticator's controlled ports. The result of the authentication process determines whether the supplicant is authorized to access services on that controlled port.

A Port Access Entity (PAE) is able to adopt one of two distinct roles within an access control interaction:

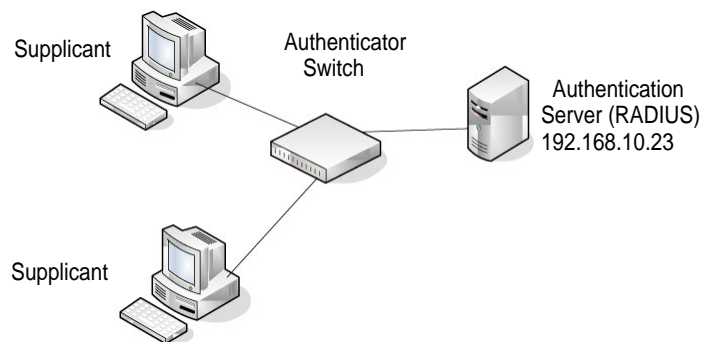
1. **Authenticator:** A Port that enforces authentication before allowing access to services available via that Port.
2. **Supplicant:** A Port that attempts to access services offered by the Authenticator.

Additionally, there exists a third role:

3. **Authentication server:** Performs the authentication function necessary to check the credentials of the Supplicant on behalf of the Authenticator.

All three roles are required in order to complete an authentication exchange.

The GS728TS, GS728TPS, GS752TS, and GS752TPS switches support the Authenticator role only, in which the PAE is responsible for communicating with the Supplicant. The Authenticator PAE is also responsible for submitting the information received from the Supplicant to the Authentication Server in order for the credentials to be checked, which will determine the authorization state of the Port. The Authenticator PAE controls the authorized/unauthorized state of the controlled Port depending on the outcome of the RADIUS-based authentication process.



802.1X Example Configuration

This example shows how to configure the switch so that 802.1X-based authentication is required on the ports in a corporate conference room (5–8). These ports are available to visitors and need to be authenticated before granting access to the network. The authentication is handled by an external RADIUS server. When the visitor is successfully authenticated, traffic is automatically assigned to the guest VLAN. This example assumes that a VLAN has been configured with a VLAN ID of 150 and VLAN Name of Guest.

1. From the Port Authentication screen, select ports 5, 6, 7, and 8.
2. From the Port Control menu, select Unauthorized.

The Port Control setting for all other ports where authentication is not needed should be Authorized. When the Port Control setting is Authorized, the port is unconditionally put in a force-Authorized state and does not require any authentication. When the Port Control setting is Auto, the authenticator PAE sets the controlled port mode.

3. In the Guest VLAN field for ports 5–8, enter 150 to assign these ports to the guest VLAN.
You can configure additional settings to control access to the network through the ports. See [Port Security Interface Configuration](#) on page 231 for information about the settings.
4. Click **Apply**.
5. From the 802.1X Configuration screen, set the Port Based Authentication State and Guest VLAN Mode to Enable, and then click **Apply** (See [Port Security Configuration](#) on page 230).

This example uses the default values for the port authentication settings, but there are several additional settings that you can configure. For example, the EAPOL Flood Mode field allows you to enable the forwarding of EAPoL frames when 802.1X is disabled on the device.

6. From the RADIUS Server Configuration screen, configure a RADIUS server with the following settings:
 - Server Address: 192.168.10.23
 - Secret Configured: Yes
 - Secret: secret123
 - Active: Primary

For more information, see [RADIUS Configuration](#) on page 199.

7. Click **Add**.
8. From the Authentication List screen, configure the default List to use RADIUS as the first authentication method (See [Authentication List Configuration](#) on page 207).

This example enables 802.1X-based port security on the GS728TS, GS728TPS, GS752TS, or GS752TPS switch and prompts the hosts connected on ports 5–8 for an 802.1X-based authentication. The switch passes the authentication information to the configured RADIUS server.

MSTP

Spanning Tree Protocol (STP) runs on bridged networks to help eliminate loops. If a bridge loop occurs, the network can become flooded with traffic. IEEE 802.1s 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, with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the Forwarding state).

The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the 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. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provides simple and full connectivity for frames assigned to any given VLAN throughout a Bridged LAN comprising arbitrarily interconnected networking devices, each operating MSTP, STP or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MSTP Bridges. These Regions and the other Bridges and LANs are connected into a single Common Spanning Tree (CST). [IEEE DRAFT P802.1s/D13]

MSTP connects all Bridges and LANs with a single Common and Internal Spanning Tree (CIST). The CIST supports the automatic determination of each MST region, choosing its maximum possible extent. The connectivity calculated for the CIST provides the CST for interconnecting these Regions, and an Internal Spanning Tree (IST) within each Region. MSTP ensures that frames with a given VLAN ID are assigned to one and only one of the MSTIs or the IST within the Region, that the assignment is consistent among all the networking devices in the Region and that the stable connectivity of each MSTI and IST at the boundary of the Region matches that of the CST. The stable active topology of the Bridged LAN with respect to frames consistently classified as belonging to any given VLAN thus simply and fully connects all LANs and networking devices throughout the network,

though frames belonging to different VLANs can take different paths within any Region, per IEEE DRAFT P802.1s/D13.

All bridges, whether they use STP, RSTP or MSTP, send information in configuration messages via Bridge Protocol Data Units (BPDUs) to assign port roles that determine each port's participation in a fully and simply connected active topology based on one or more spanning trees. The information communicated is known as the spanning tree priority vector. The BPDU structure for each of these different protocols is different. A MSTP bridge will transmit the appropriate BPDU depending on the received type of BPDU from a particular port.

An MST Region comprises of one or more MSTP Bridges with the same MST Configuration Identifier, using the same MSTIs, and which have no Bridges attached that cannot receive and transmit MSTP BPDUs. The MST Configuration Identifier has the following components:

1. Configuration Identifier Format Selector
2. Configuration Name
3. Configuration Revision Level
4. Configuration Digest: 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID to MSTID mapping)

As there are Multiple Instances of Spanning Tree, there is a MSTP state maintained on a per-port, per-instance basis (or on a per port per VLAN basis: as any VLAN can be in one and only one MSTI or CIST). For example, port A can be forwarding for instance 1 while discarding for instance 2. The port states have changed since IEEE 802.1D specification.

To support multiple spanning trees, a MSTP bridge has to be configured with an unambiguous assignment of VLAN IDs (VIDs) to spanning trees. This is achieved by:

1. Ensuring that the allocation of VIDs to FIDs is unambiguous.
2. Ensuring that each FID supported by the Bridge is allocated to exactly one Spanning Tree Instance.

The combination of VID to FID and then FID to MSTI allocation defines a mapping of VIDs to spanning tree instances, represented by the MST Configuration Table.

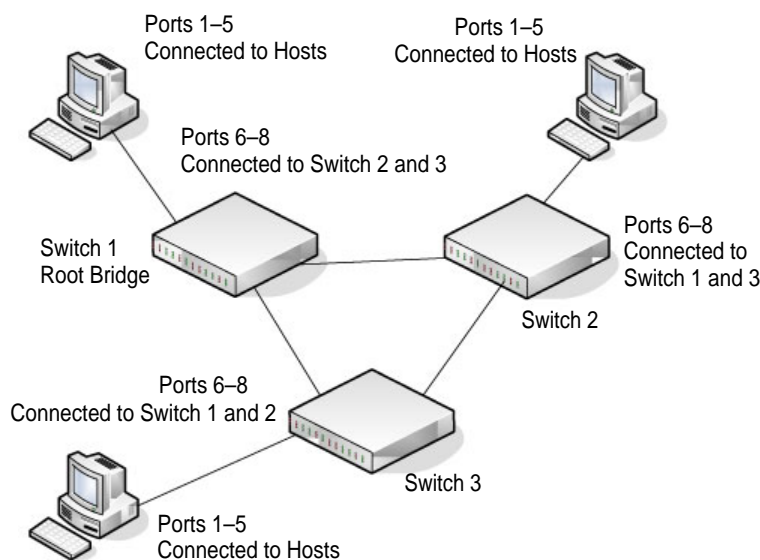
With this allocation we ensure that every VLAN is assigned to one and only one MSTI. The CIST is also an instance of spanning tree with a MSTID of 0.

An instance may occur that has no VIDs allocated to it, but every VLAN must be allocated to one of the other instances of spanning tree.

The portion of the active topology of the network that connects any two bridges in the same MST Region traverses only MST bridges and LANs in that region, and never Bridges of any kind outside the Region, in other words connectivity within the region is independent of external connectivity.

MSTP Example Configuration

This example shows how to create an MSTP instance from the GS728TS, GS728TPS, GS752TS, or GS752TPS switch. The example network has three different GS728TS, GS728TPS, GS752TS, or GS752TPS switches that serve different locations in the network. In this example, ports 1–5 are connected to host stations, so those links are not subject to network loops. Ports 6–8 are connected across switches 1, 2 and 3.



Perform the following procedures on each switch to configure MSTP:

1. Use the VLAN Configuration screen to create VLANs 300 and 500 (see [VLAN Configuration](#) on page 110).
2. Use the VLAN Membership screen to include ports 1–8 as tagged (T) or untagged (U) members of VLAN 300 and VLAN 500 (see [VLAN Membership Configuration](#) on page 112).
3. From the STP Configuration page, enable the Spanning Tree State option (see [STP Switch Configuration](#) on page 123).
4. In the **Configuration Name** field on the STP Configuration page, configure the name so that it is the same on each switch, for example netgear-stp. By default, the Configuration Name is the switch MAC address which means that it is unique for each switch.

Use the default values for the rest of the STP configuration settings. By default, the STP Operation Mode is MSTP.

5. From the CST Configuration screen, set the Bridge Priority value for each of the three switches to force Switch 1 to be the root bridge:
 - Switch 1: 4096
 - Switch 2: 12288
 - Switch 3: 20480

Note: Bridge priority values are multiples of 4096.

If you do not specify a root bridge and all switches have the same Bridge Priority value, the switch with the lowest MAC address is elected as the root bridge (see [CST Configuration](#) on page 125).

6. From the CST Port Configuration screen, select ports 1–8 and select Enable from the STP Status menu (see [CST Port Configuration](#) on page 126).

7. Click **Apply**.

8. Select ports 1–5 (edge ports), and select Enable from the Fast Link menu.

Since the edge ports are not at risk for network loops, ports with Fast Link enabled transition directly to the Forwarding state.

9. Click **Apply**.

You can use the CST Port Status screen to view spanning tree information about each port.

10. From the MST Configuration screen, create a MST instances with the following settings:
 - MST ID: 1
 - Priority: Use the default (32768)
 - VLAN ID: 300

For more information, see [MST Configuration](#) on page 130.

11. Click **Add**.

12. Create a second MST instance with the following settings

- MST ID: 2
- Priority: 49152
- VLAN ID: 500

13. Click **Add**.

In this example, assume that Switch 1 has become the Root bridge for the MST instance 1, and Switch 2 has become the Root bridge for MST instance 2. Switch 3 has hosts in the Sales department (ports 1, 2, and 3) and in the HR department (ports 4 and 5). Switches 1 and 2 also have hosts in the Sales and Human Resources departments. The hosts connected from Switch 2 use VLAN 500, MST instance 2 to communicate with the hosts on Switch 3 directly. Likewise, hosts of Switch 1 use VLAN 300, MST instance 1 to communicate with the hosts on Switch 3 directly.

The hosts use different instances of MSTP to effectively use the links across the switch. The same concept can be extended to other switches and more instances of MSTP.

Configuring VLAN Routing

VLANs divide broadcast domains in a LAN environment. Whenever hosts in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed between them. This is known as inter-VLAN routing. On NETGEAR GS728TS, GS728TPS, GS752TS, and GS752TPS switches, it is accomplished by creating Layer 3 interfaces (Switch virtual interfaces (SVI)).

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. 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.

Creating VLAN Routing Interfaces

1. Use the IP Configuration screen to enable routing on the switch (see [IP Configuration](#) on page 161).
2. Determine the IP addresses you want to assign to the VLAN interface on the switch. For the switch to be able to route between the VLANs, the VLAN interfaces must be configured with an IP address. When the switch receives a packet destined for another subnet/VLAN, the switch looks at the routing table to determine where to forward the packet. The packet is then passed to the VLAN interface of the destination. It is then sent to the port where the end device is attached.
3. If the VLAN has not been created, use the VLAN Routing Wizard screen to create and configure the VLAN interfaces (see [VLAN Routing Wizard](#) on page 165)
 - a. Specify the VLAN ID to configure for routing.
 - b. Enter the IP address and associated subnet mask in the available fields.
 - c. Select the ports or LAGs to include as VLAN members.
 - d. Apply the configuration changes to the switch.
4. If the VLAN has already been configured by using the VLAN pages under the **Switching** tab, you can use the VLAN Routing Configuration page to enable routing on the VLAN and assign an IP address and subnet mask (see [VLAN Routing Configuration](#) on page 167).
5. Repeat this process for all VLANs identified to be configured as the routing interfaces.

Notification of Compliance



NETGEAR Wired Products

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

FCC Requirements for Operation in the United States

FCC Information to User

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

The digital apparatus, GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches, do not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

European Union

The GS728TS, GS728TPS, GS752TS, and GS752TPS Gigabit Smart Switches complies with essential requirements of EU EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC as supported by applying the following test methods and standards:

- EN55022: 2006 / A1: 2007
- EN55024: 1998 / A1: 2001 / A2 : 2003
- EN60950-1: 2005 2nd Edition
- EN 61000-3-2:2006
- EN 61000-3-3:1995 w/A1: 2001+A2: 2005

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to <ftp://downloads.netgear.com/files/GPLnotice.pdf>

For GNU General Public License (GPL) related information, please visit http://support.netgear.com/app/answers/detail/a_id/2649

Index

Numerics

802.1X **199, 219**
example configuration **315**

A

access control
ACL example configuration **308**
ACLs **234**
management interface **210**

ARP

Cache **172**
configuring **171**
Entry configuration **173**
Entry Management **175**
Global ARP configuration **174**

authentication

802.1X **218, 315**
enable **29**
list **207**
port-based **218**
RADIUS **199, 201**
SNMP **29, 78, 80**
TACACS+ **204**

Auto-Video **110, 137**

B

Binding Configuration **95**

C

certificate **214**
changing the password **17, 198**
compliance **323**
Configuration
802.1X **219**
Access Control Lists **234**
Access Profile **215**
Access Rule **217**
Authentication List **207**
Class **186, 189**
Community **75**
CoS **178**
DHCP Filtering **93**
DHCP Snooping **95, 97**

Differentiated Services **184**
DiffServ **185**
DNS **49**
Dual Image **289**
Dynamic Address **158**
Dynamic Host **51**
Global **138**
Green Ethernet **51, 53, 54, 59**
HTTP **211**
IGMP Snooping **138**
LACP **108**
LACP Port **109**
LAG **105**
LLDP **81**
MAC Filter **225**
Management Access **210**
MST Port **131**
Network Settings on the Administrative System **15**
password **198**
Policy **191**
Port Security **230**
Port VLAN ID **113**
RADIUS **199**
Global **199**
Secure HTTP **212**
SNMP v3 User **79**
SNTP Server **43**
Standard IP ACL Example **310**
STP **122**
TACACS+ **204**
Time **41**
Trap **77**
VLAN **110**
VLAN example **307**
VLAN Port Membership **112**
CoS **178**

D

defaults **300**
CoS **310**
factory **198**
DES **29**
Device View **26**
DHCP
client **11**
Filtering **92**

Filtering Interface Configuration **94**
 refreshing the client **17**

DiffServ **184**

DNS **49**

DoS **45**

download

 a file **285**

 files via HTTP **285**

 from a remote system **282, 284**

 software **285**

Dual Image Status **288, 291**

E

EAP **266, 268**

EAPOL **267**

F

file management **288**

firmware **20**

firmware download **282, 284**

G

Green Ethernet **51, 53, 54**

guest VLAN configuration **317**

H

help, HTML-based **25**

HTTP **211**

 management interface access **16**

 secure **210**

 using to download files **283, 287**

HTTPS **212**

I

IEEE 802.11x **315**

IEEE 802.1AB **80**

IEEE 802.1D **122**

IEEE 802.1Q **110, 122**

IEEE 802.1s **122**

IEEE 802.1w **122**

IEEE 802.1X **199**

IEEE 802.3 flow control **104**

IGMP **138**

 snoothing **138**

 snoothing querier **144**

interface

 LAG **105**

 logical **30**

 naming convention **30**

 physical **30**

 queue configuration **181**

IP address

 administrative system **15**

 switch **11, 35**

IP DSCP **178**

 Mapping **183**

IPv6

 network interface **37**

IPv6 network

 configuration **38**

IPv6 Network Configuration **37**

IPv6 Network Interface IPv6 Neighbor Table **38**

IPv6 Network Neighbor **38**

L

LACP port configuration **109**

LAG VLAN **105**

LAGP PDUs **105**

LAGs **105**

 Membership **107**

 Static **105**

LLDP **80**

 Local Information **86**

 neighbors information **88**

 packets **82**

 port settings **82**

LLDP-MED **81**

M

MAC **33, 87, 128, 138**

 ACL **237**

 bridge identifier **131**

 CPU Management Interface **30**

 dynamic address **158**

 filter summary **227**

 MFDB Table **135**

 multicast destination **135**

 rules **238**

 searching address table **156**

 Static Address **159**

MD5 **40**

MIBs **29**

MLD **147**

multicast, layer 2 **138**

N

navigation **24**

O

OUI [120](#)

P

password

change [17](#), [198](#)

login [198](#)

Persistent Configuration [97](#)

Ping [292](#)

PoE [70](#), [99](#)

port

authentication [218](#)

summary [224](#)

product registration [298](#)

Q

QoS [177](#)

802.1p to Queue Mapping [182](#)

R

RADIUS [197](#)

server [199](#)

statistics [202](#)

reboot [17](#), [280](#)

registration

disabling [298](#)

product [298](#)

serial number [298](#)

reset

button [198](#)

configuration to defaults [281](#)

switch [280](#)

Route Status [170](#)

Router Discovery [168](#)

routing

navigation tree [160](#)

statistics [162](#)

VLAN [165](#)

Routing Table [169](#)

RSTP [122](#)

S

Security MAC Address [232](#)

server, HTTP [211](#)

severity, log message [273](#)

Simple Network Time Protocol [40](#)

SNMP

traps [77](#)

using [29](#)

v1, v2 [75](#)

v3 [79](#)

SNTP [40](#)

Global Status [42](#)

global status [42](#)

server configuration [43](#)

server status [44](#)

specifications [300](#)

SSL [212](#)

Statistics [98](#)

storm control [228](#)

STP [122](#)

example configuration [318](#)

Status [123](#)

Stratum

0 [40](#)

1 [40](#)

2 [40](#)

T

T1 [40](#)

T2 [40](#)

T3 [40](#)

T4 [40](#)

TACACS+

folder [205](#)

settings [205](#)

technical support [2](#)

Time

configure through SNTP [42](#)

UTC [42](#)

time [40](#)

clock source [42](#)

levels [40](#)

local [41](#)

zone [41](#)

TraceRoute [294](#)

trademarks [2](#)

traffic control [225](#)

trap

flags [78](#)

manager [78](#)

U

Unicast [40](#)

upload configuration [282](#)

V

video [110](#)

VLAN **110**

example configuration **306**

guest **221, 316**

ID **110**

management **36**

managing **110**

Port VLAN ID **113**

PVID **113**

voice **118**

Voice VLAN OUI **120**

VoIP **120, 121**

W

Web interface panel **23**