



# ProSafe® Managed Switch

## Web Management User Manual

350 East Plumeria Drive  
San Jose, CA 95134  
USA

October 27, 2010  
202-10757-01  
v1.0

©2010 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, or get support online, visit us at <http://support.netgear.com>.

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

Phone (Other Countries): See Support information card.

## Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Wizard, Auto Uplink, X-RAID2, and NeoTV are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

## 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
202-10757-01	v1.0	October 27, 2010	

# Table of Contents

## Chapter 1 Getting Started

Switch Management Interface .....	9
Web Access .....	9
Understanding the User Interfaces .....	10
Using the Web Interface .....	10
Using SNMP .....	17
Interface Naming Convention .....	18

## Chapter 2 Configuring System Information

Management .....	19
System Information .....	20
Switch Statistics .....	26
System Resource .....	29
Slot Information .....	30
Loopback Interface .....	32
Network Interface .....	33
Time .....	38
DNS .....	46
License .....	49
Show License .....	49
License Features .....	50
Services .....	50
DHCP Server .....	51
DHCP Relay .....	62
DHCP L2 Relay .....	64
UDP Relay .....	67
DHCPv6 Server .....	71
DHCPv6 Relay .....	79
Stacking .....	79
Basic .....	80
Advanced .....	83
PoE .....	86
Basic .....	86
Advanced .....	89
SNMP .....	93
SNMPV1/V2 .....	93
SNMP V3 .....	101
LLDP .....	102
LLDP .....	103

LLDP-MED .....	113
ISDP .....	121
Basic .....	121
Advanced .....	124

## Chapter 3 Configuring Switching Information

VLANs .....	130
Basic .....	131
Advanced .....	134
Spanning Tree Protocol .....	151
Basic .....	152
Advanced .....	155
Multicast .....	168
MFDB .....	168
IGMP Snooping .....	172
MLD Snooping .....	184
Address Table .....	192
Basic .....	192
Advanced .....	195
Ports .....	197
Port Configuration .....	198
Port Description .....	200
Link Aggregation Groups .....	201
LAG Configuration .....	201
LAG Membership .....	203

## Chapter 4 Routing

Routing Table .....	205
Basic .....	205
Advanced .....	209
IP .....	213
Basic .....	213
Advanced .....	220
IPv6 .....	229
Basic .....	230
Advanced .....	233
VLAN .....	250
VLAN Routing Wizard .....	251
VLAN Routing Configuration .....	252
ARP .....	252
Basic .....	253
Advanced .....	255
RIP .....	258
Basic .....	258
Advanced .....	260
OSPF .....	266
Basic .....	267



Advanced . . . . .	268
OSPFv3 . . . . .	296
Basic . . . . .	296
Advanced . . . . .	298
Router Discovery . . . . .	323
Router Discovery Configuration . . . . .	324
VRRP . . . . .	325
Basic . . . . .	325
Advanced . . . . .	329
Multicast . . . . .	334
Mroute Table . . . . .	335
Multicast Global Configuration . . . . .	336
Multicast Interface Configuration . . . . .	337
DVMRP . . . . .	338
IGMP . . . . .	346
PIM-DM . . . . .	359
PIM-SM . . . . .	362
Static Routes Configuration . . . . .	370
Admin Boundary Configuration . . . . .	371
IPv6 Multicast . . . . .	371
Mroute Table . . . . .	372
IPv6 PIM-DM . . . . .	374
IPv6 PIM-SM . . . . .	377
MLD . . . . .	385
Static Routes Configuration . . . . .	397

## Chapter 5 Configuring Quality of Service

Class of Service . . . . .	398
Basic . . . . .	399
Advanced . . . . .	401
Differentiated Services . . . . .	407
DiffServ Wizard . . . . .	409
Auto VoIP Configuration . . . . .	411
Basic . . . . .	412
Advanced . . . . .	414

## Chapter 6 Managing Device Security

Management Security Settings . . . . .	427
Local User . . . . .	428
Enable Password Configuration . . . . .	431
Line Password Configuration . . . . .	432
RADIUS . . . . .	433
Configuring TACACS+ . . . . .	440
Authentication List Configuration . . . . .	443
Login Sessions . . . . .	450
Configuring Management Access . . . . .	450
HTTP . . . . .	451

HTTPS .....	453
SSH .....	458
Telnet .....	462
Console Port .....	464
Denial of Service .....	465
Port Authentication .....	466
Basic .....	467
Advanced .....	470
Traffic Control .....	481
MAC Filter .....	481
Port Security .....	484
Private Group .....	490
Protected Ports Configuration .....	492
Storm Control .....	493
Control .....	496
DHCP Snooping .....	497
IP Source Guard .....	503
Dynamic ARP Inspection .....	505
Captive Portal .....	512
Configuring Access Control Lists .....	524
Basic .....	524
Advanced .....	531

## Chapter 7 Monitoring the System

Ports .....	546
Port Statistics .....	546
Port Detailed Statistics .....	549
EAP Statistics .....	557
Cable Test .....	559
Logs .....	560
Buffered Logs .....	561
Command Log Configuration .....	563
Console Log Configuration .....	564
SysLog Configuration .....	565
Trap Logs .....	566
Event Logs .....	568
Persistent Logs .....	570
Port Mirroring .....	571
Multiple Port Mirroring .....	571
sFlow .....	573
Basic .....	573
Advanced .....	575

## Chapter 8 Maintenance

Save Configuration .....	578
Save Configuration .....	578
Auto Install Configuration .....	580

Reset .....	580
Device Reboot .....	580
Factory Default .....	582
Password Reset .....	583
Upload File From Switch .....	583
File Upload .....	583
HTTP File Upload .....	586
USB File Upload .....	587
Download File To Switch .....	587
File Download .....	588
HTTP File Download .....	589
USB File Download .....	592
File Management .....	592
Copy .....	593
Dual Image Configuration .....	594
Troubleshooting .....	595
Ping IPv4 .....	595
Ping IPv6 .....	598
Traceroute IPv4 .....	599
Traceroute IPv6 .....	601

## Chapter 9 Help

Online Help .....	602
Support .....	602
User Guide .....	603

## Appendix A Default Settings

## Appendix B Configuration Examples

Virtual Local Area Networks (VLANs) .....	608
VLAN Example Configuration .....	609
Access Control Lists (ACLs) .....	610
MAC ACL Example Configuration .....	611
Standard IP ACL Example Configuration .....	612
Differentiated Services (DiffServ) .....	613
Class .....	613
DiffServ Traffic Classes .....	614
Creating Policies .....	614
DiffServ Example Configuration .....	616
802.1X .....	617
802.1X Example Configuration .....	619
MSTP .....	620
MSTP Example Configuration .....	621

## Appendix C Notification of Compliance

## **Index**

# Getting Started

---

# 1

This chapter provides an overview of starting your NETGEAR ProSafe® Managed Switches and accessing the user interface. This chapter contains the following sections:

- *Switch Management Interface* on page 9
- *Web Access* on page 9
- *Web Access* on page 9
- *Understanding the User Interfaces* on page 10
- *Interface Naming Convention* on page 18

## Switch Management Interface

The NETGEAR ProSafe® Managed Switches contain an embedded Web server and management software for managing and monitoring switch functions. ProSafe® Managed Switches function as simple switches 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.

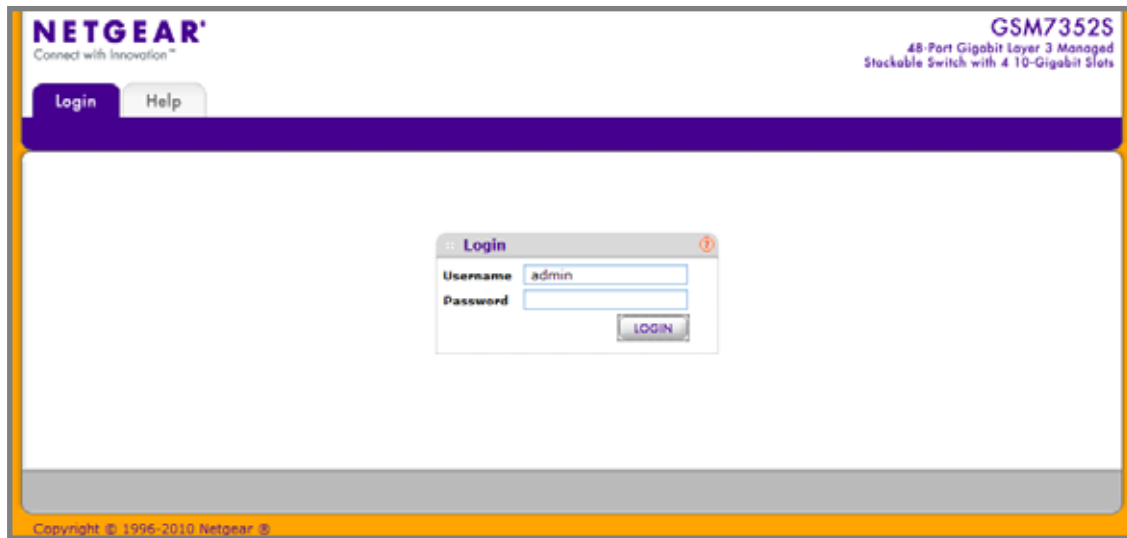
## Web Access

To access the ProSafe® Managed Switches management interface:

- 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 ProSafe® Managed Switches management interface from your administrative system for Web access to be available. If you did not change the IP address of the switch from the default value, enter 169.254.100.100 into the address field.

Accessing the switch directly from your Web browser displays the login screen shown below.



## Understanding the User Interfaces

ProSafe® Managed 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)
- Command Line Interface (CLI)

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

The *ProSafe® Managed Switch Web Management User 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:

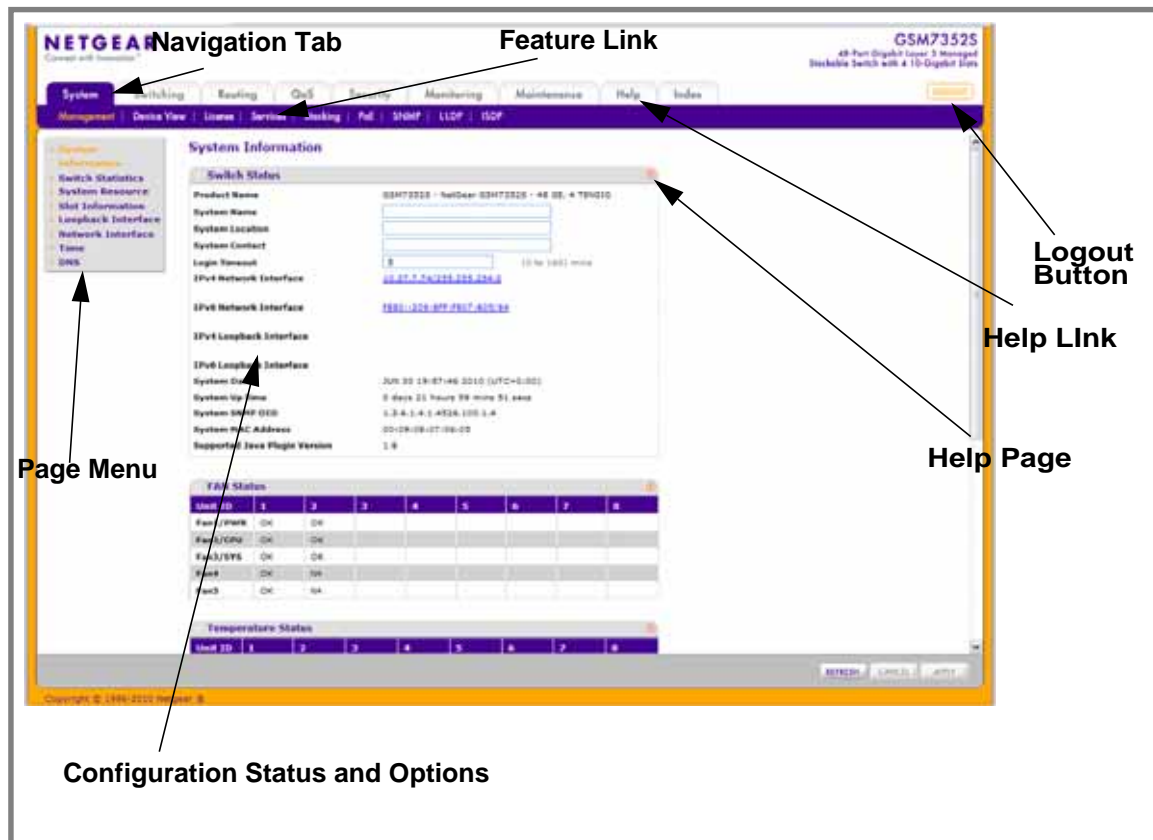
- HTML version 4.0, or later
- HTTP version 1.1, or later
- Java Runtime Environment 1.6 or later

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.

- The default username is **admin**, default password is none (no password). Type the username into the field on the login screen and then click **Login**. Usernames and passwords are case sensitive.
- After the system authenticates you, the System Information page displays.

The figure below shows the layout of the Managed Switch Web interface.

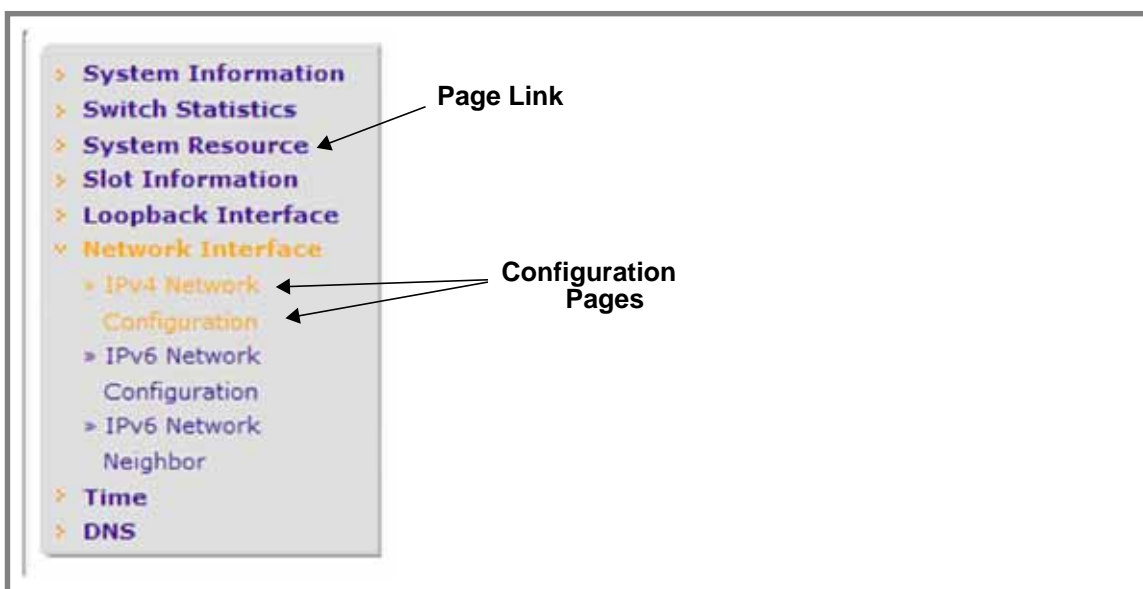


## Navigation Tabs, Feature Links, and Page Menu

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 the following figure 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.





## 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.

**Table 1** shows the command buttons that are used throughout the pages in the Web interface:

**Table 1.**

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

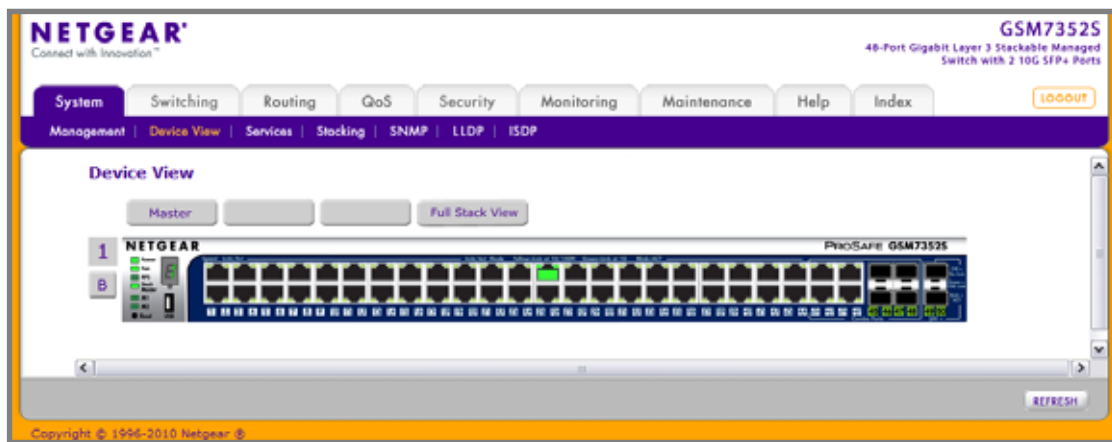
## Device View

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.

The port coloring indicates whether a port is currently active. 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.

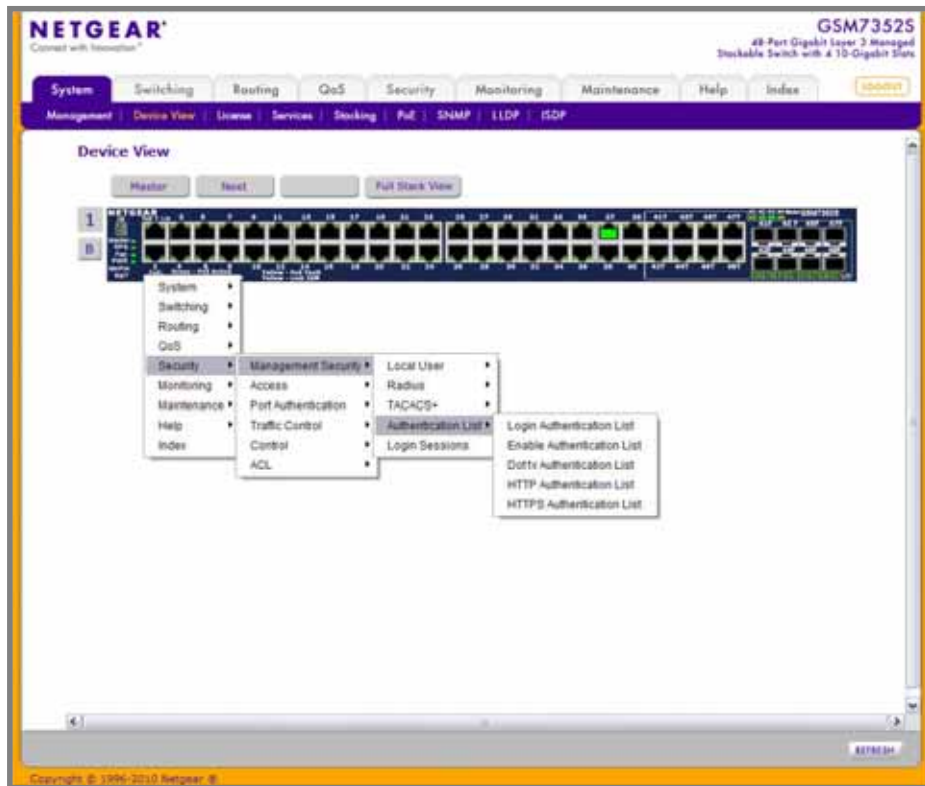
The Device View of the switch is shown below.




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.



If you click the graphic, but do not click a specific port, the main menu appears. 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.

## 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):

**Table 2.**

\	<
/	>
*	
?	

## Using SNMP

The ProSafe® Managed Switches software supports the configuration of SNMP groups and users that can manage traps that the SNMP agent generates.

ProSafe® Managed 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 ProSafe® Managed Switches support physical and logical interfaces. Interfaces are identified by their type and the interface number. The physical ports are gigabit interfaces and are numbered on the front panel. You configure the logical interfaces by using the software. **Table 3** describes the naming convention for all interfaces available on the switch.

**Table 3.**

Interface	Description	Example
Physical	The physical ports are gigabit Ethernet interfaces and are numbered sequentially starting from one.	1/0/1, 1/0/2, 1/0/3, and so on
Link Aggregation Group (LAG)	LAG interfaces are logical interfaces that are only used for bridging functions.	lag 1, lag 2, lag 3, and so on
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.	0/5/1
Routing VLAN Interfaces	This is an interface used for routing functionality.	Vlan 1, Vlan 2, Vlan 3, and so on

## 2. 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 19
- Device View (See [Device View](#) on page 14)
- [License](#) on page 49
- [Services](#) on page 50
- [Stacking](#) on page 79
- [PoE](#) on page 86
- [SNMP](#) on page 93
- [LLDP](#) on page 102
- [ISDP](#) on page 121

### 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 20
- [Switch Statistics](#) on page 26
- [System Resource](#) on page 29
- [Slot Information](#) on page 30
- [Loopback Interface](#) on page 32
- [Network Interface](#) on page 33
- [Time](#) on page 38
- [DNS](#) on page 46

## 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 displays.

**NETGEAR**  
Connect with Innovation

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

System Switching Routing QoS Security Monitoring Maintenance Help Index [LOGOUT](#)

Management | Device View | License | Services | Stacking | PoE | SNMP | LLDP | ISDP

System Information

System Information

Switch Status

Product Name: GSM7352S - NetGear GSM7352S - 48 GE, 4 TENGE

System Name:

System Location:

System Contact:

Login Timeout:  (0 to 160) mins

IPv4 Network Interface: [10.27.7.74/255.255.252.0](#)

IPv6 Network Interface: [FE80::209:8FF:FE07:6D9/64](#)

IPv4 Loopback Interface:

IPv6 Loopback Interface:

System Date: JUN 30 21:35:01 2010 (UTC+0100)

System Up Time: 0 days 23 hours 38 mins 5 secs

System SNMP OID: 1.3.6.1.4.1.4526.100.1.4

System MAC Address: 00:09:08:07:06:05

Supported Java Plugin Version: 1.6

FAN Status

Unit ID	1	2	3	4	5	6	7	8
Fan1/PWR	OK	OK						
Fan2/CPU	OK	OK						
Fan3/SYS	OK	OK						
Fan4	OK	NA						
Fan5	OK	NA						

Temperature Status

Unit ID	1	2	3	4	5	6	7	8
CPU	28°C	58°C						
MAC	38°C	N/A						
MAC 1	N/A	N/A						
MAC 2	N/A	N/A						

Device Status

Unit ID	1	2	3	4	5	6	7	8
Firmware Version	8.0.3.11	8.0.3.11						
Boot Version	29	29						
CPLD Version	0x2	0x2						
Serial Number	11	11						
RPS	Not Present	Not Present						
Power Module	Operational	Operational						
PoE Version	N/A	4.0						
MAX PoE	N/A	OFF						

Copyright © 1996-2010 Netgear, Inc.

[REFRESH](#) [CANCEL](#) [APPLY](#)



The System Information provides various statuses:

## Switch Status

System Information	
Switch Status	
Product Name	GSM7352S - NetGear GSM7352S - 48 GE, 4 TENGIG
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
Login Timeout	<input type="text" value="5"/> (0 to 160) mins
IPv4 Network Interface	<u>10.27.7.74/255.255.254.0</u>
IPv6 Network Interface	<u>FE80::209:8FF:FE07:605/64</u>
IPv4 Loopback Interface	
IPv6 Loopback Interface	
System Date	JUN 30 21:57:34 2010 (UTC+0:00)
System Up Time	0 days 23 hours 59 mins 39 secs
System SNMP OID	1.3.6.1.4.1.4326.100.1.4
System MAC Address	00:09:08:07:06:05
Supported Java Plugin Version	1.6

To define system information:

1. Open the **System Information** page.
2. Define the following fields:
  - a. **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.
  - b. **System Location** - Enter the location of this switch. You may use up to 255 alphanumeric characters. The factory default is blank.
  - c. **System Contact** - Enter the contact person for this switch. You may use up to 25 alphanumeric characters. The factory default is blank.
  - d. **Login Timeout** - Specify how many minutes of inactivity should occur on a serial port connection before the switch closes the connection. Enter a number between 0 and 160; the factory default is 5. Entering 0 disables the timeout.
3. Click **Apply** to send the updated screen to the switch and cause the changes to take effect on the switch. These changes will not be retained across a power cycle unless a save is performed.

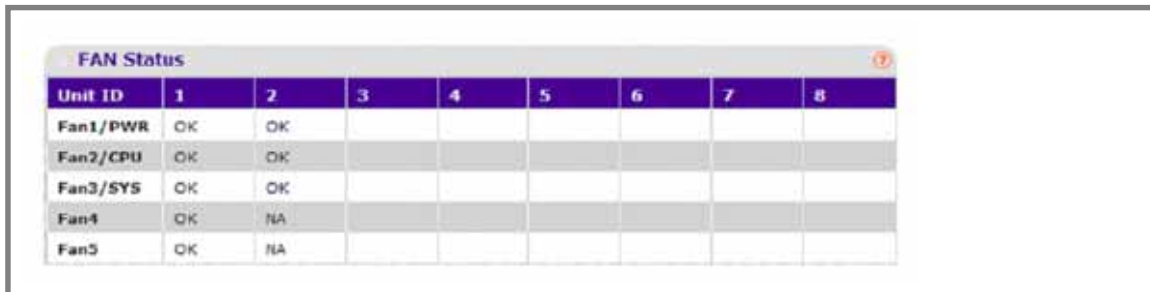
The following table describes the status information the System Page displays.

**Table 2-1.**

Field	Description
Product Name	The product name of this switch.
IPv4 Network Interface	The IPv4 address and mask assigned to the network interface.
IPv6 Network Interface	The IPv6 prefix and prefix length assigned to the network interface.
IPv4 Loopback Interface	The IPv4 address and mask assigned to the loopback interface.
IPv6 Loopback Interface	The IPv6 prefix and prefix length assigned to the loopback interface.
System Date	The current date.
System Up time	The time in days, hours and minutes since the last switch reboot.
System SNMP OID	The base object ID for the switch's enterprise MIB.
System Mac Address	Universally assigned network address.
Supported Java Plugin Version	The supported version of Java plugin.

## FAN Status

The screen shows the status of the fans in all units. These fans remove the heat generated by the power, CPU and other chipsets, make chipsets work normally. Fan status has three possible values: OK, Failure, Not Applicable (NA).



Unit ID	1	2	3	4	5	6	7	8
Fan1/PWR	OK	OK						
Fan2/CPU	OK	OK						
Fan3/SYS	OK	OK						
Fan4	OK	NA						
Fan5	OK	NA						

The following table describes the Fan Status information.

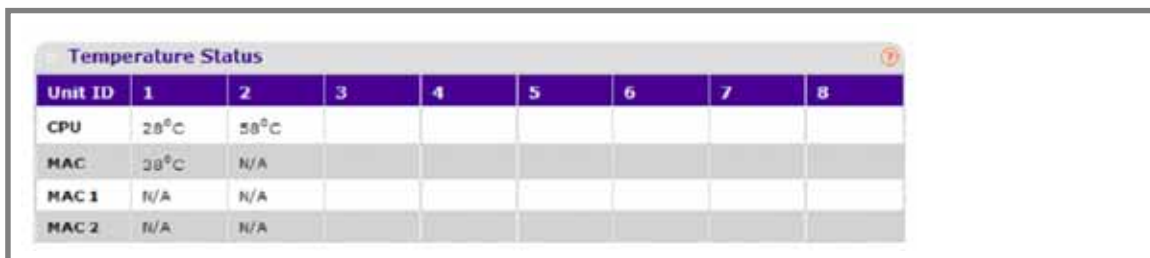
**Table 2-2.**

Field	Description
UNIT ID	The unit identifier is assigned to the switch which the fan belongs to.
FAN	The working status of the fan in each unit.

Click **REFRESH** to refresh the system information of the switch.

## Temperature Status

The screen shows the current temperature of the CPU and MACs. The temperature is instant and can be refreshed when the REFRESH button is pressed. The maximum temperature of CPU and MACs depends on the actual hardware.



Unit ID	1	2	3	4	5	6	7	8
CPU	28°C	58°C						
MAC	38°C	N/A						
MAC 1	N/A	N/A						
MAC 2	N/A	N/A						

The following table describes the Temperature Status information.

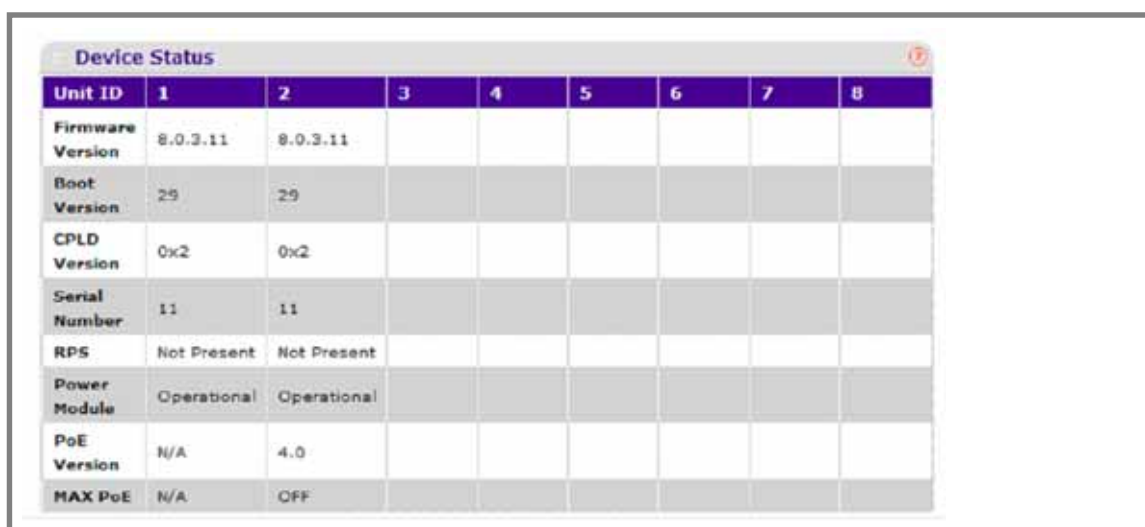
Table 2-3.

Field	Description
CPU	The current temperature of the CPU in the switch.
MAC	The current temperature of the MACs in the switch.

Click **REFRESH** to refresh the system information of the switch.

### Device Status

The screen shows the software version of each device.



Unit ID	1	2	3	4	5	6	7	8
Firmware Version	8.0.3.11	8.0.3.11						
Boot Version	29	29						
CPLD Version	0x2	0x2						
Serial Number	11	11						
RPS	Not Present	Not Present						
Power Module	Operational	Operational						
PoE Version	N/A	4.0						
MAX PoE	N/A	OFF						

The following table describes the Device Status information.

Table 2-4.

Field	Description
Firmware Version	The release.version.maintenance.build number of the code currently running on the switch. For example, if the release was 8, the version was 0, the maintenance number was 3, and the build number was 11, the format would be '8.0.3.11'.
Boot Version	The version of the boot code which is in the flash memory to load the firmware into the memory.
CPLD Version	The version of the software for CPLD.
Serial Number	The serial number of this switch.

Table 2-4.

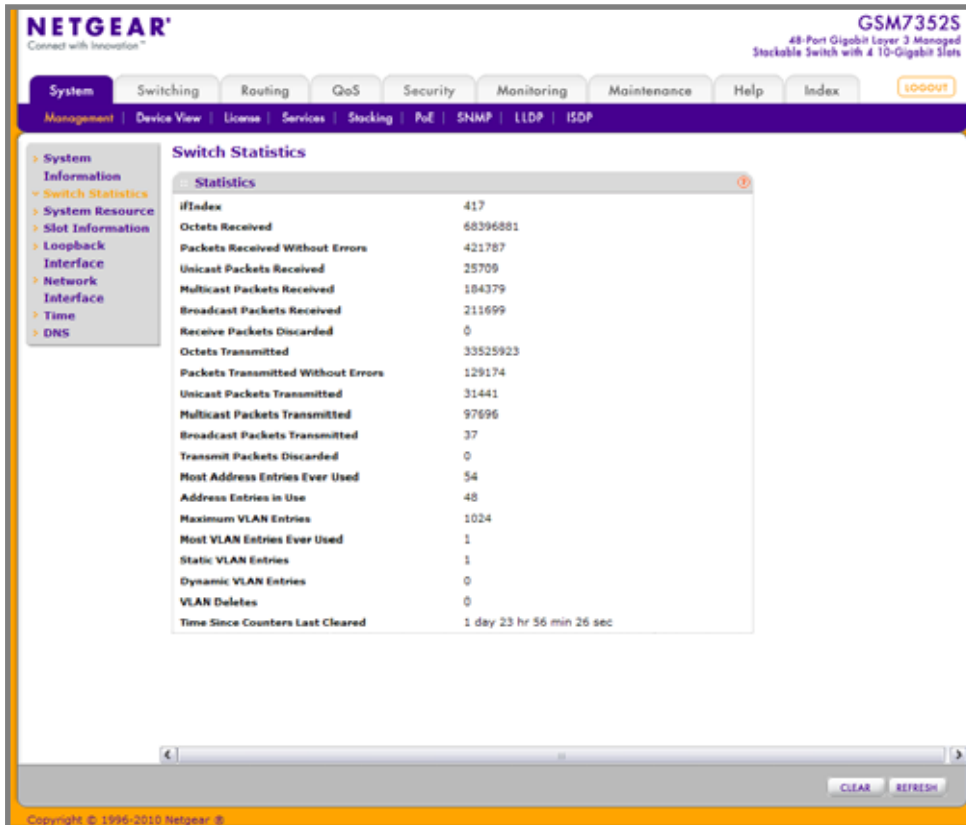
Field	Description
RPS	Indicates the status of the RPS. The status has three possible values: <ul style="list-style-type: none"><li>• Not Present: RPS bank not connected</li><li>• OK: RPS bank connected.</li><li>• FAIL: RPS is present, but power is failed.</li></ul>
Power Module	Indicates the status of the internal power module.
PoE Version	Version of the PoE controller FW image.
MAX PoE	Indicates the status of maximum PoE power available on the switch as follows: <ul style="list-style-type: none"><li>• ON: Indicates less than 7W of PoE power available for another device.</li><li>• OFF: Indicates at least 7W of PoE power available for another device.</li><li>• N/A: Indicates that PoE is not supported by the unit.</li></ul>

Click **REFRESH** to refresh the system information of the switch.

## Switch Statistics

Use this page to display the switch statistics.

To display the Switch Statistics page, click **System > Management > Switch Statistics**. A screen similar to the following displays.



**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management | Device View | License | Services | Stacking | PoE | SNMP | LLDP | ISDP

System  
Information  
Switch Statistics  
System Resource  
Slot Information  
Loopback  
Interface  
Network  
Interface  
Time  
DNS

### Switch Statistics

Statistics

ifIndex	417
Octets Received	68396881
Packets Received Without Errors	421787
Unicast Packets Received	25709
Multicast Packets Received	184379
Broadcast Packets Received	211699
Receive Packets Discarded	0
Octets Transmitted	33525923
Packets Transmitted Without Errors	129174
Unicast Packets Transmitted	31441
Multicast Packets Transmitted	97696
Broadcast Packets Transmitted	37
Transmit Packets Discarded	0
Most Address Entries Ever Used	54
Address Entries in Use	48
Maximum VLAN Entries	1024
Most VLAN Entries Ever Used	1
Static VLAN Entries	1
Dynamic VLAN Entries	0
VLAN Deletes	0
Time Since Counters Last Cleared	1 day 23 hr 56 min 26 sec

← | | →

CLEAR REFRESH

Copyright © 1996-2010 Netgear, Inc.

The following table describes Switch Statistics information.

**Table 2-5.**

Field	Description
ifIndex	This object indicates the ifIndex of the interface table entry associated with the Processor of this switch.
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Errors	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Table 2-5.

Field	Description
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

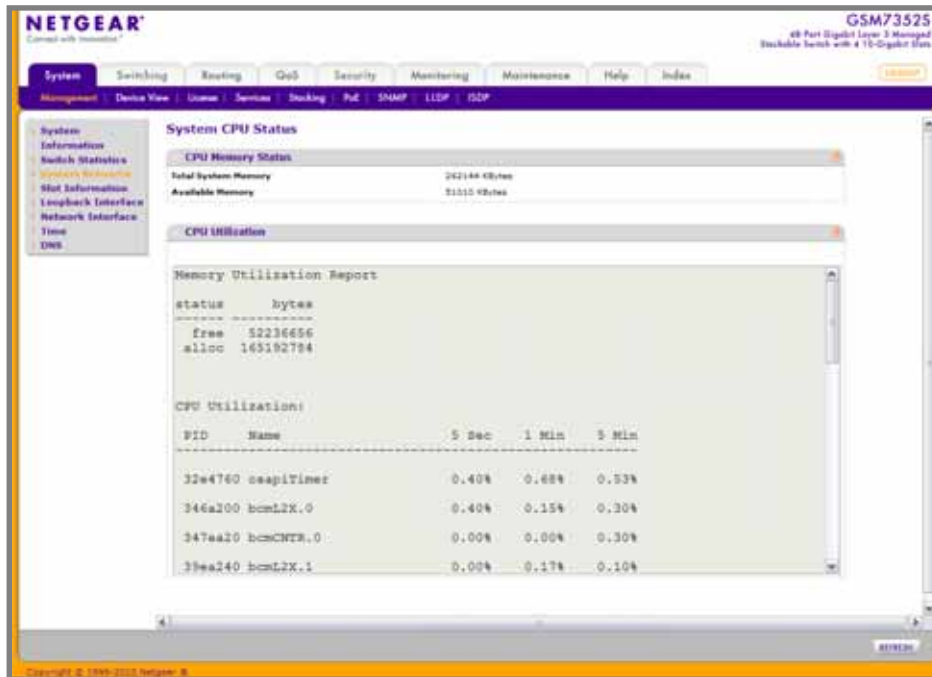
Click **CLEAR** to clear all the counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.



## System Resource

Use this page to display the system resources.

To display the System Resource page, click **System > Management > System Resource**. A screen similar to the following displays.



### CPU Memory Status

The following table describes CPU Memory Status information.

**Table 2-6.**

Field	Description
Total System Memory	The total memory of the switch in KBytes.
Available Memory	The available memory space for the switch in KBytes.

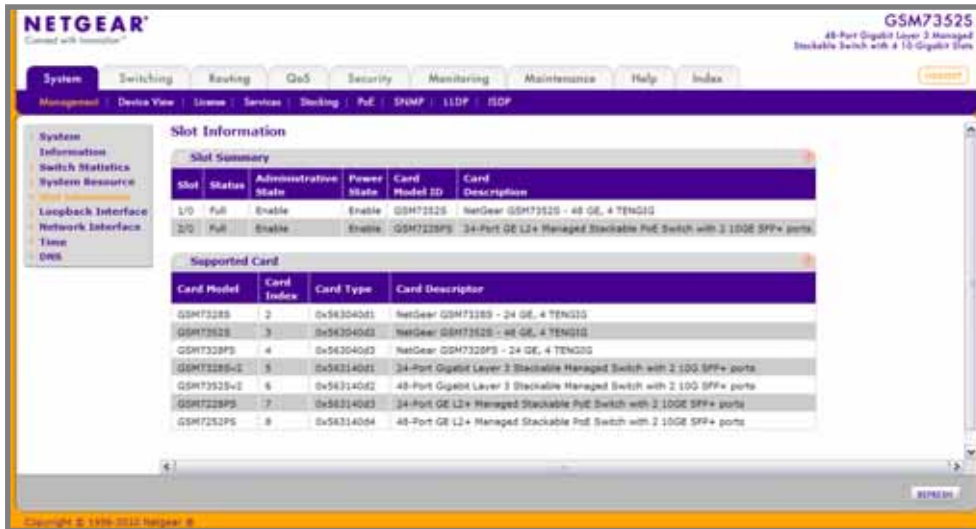
### CPU Utilization Information

This page displays the CPU Utilization information, which contains the memory information, task-related information and percentage of CPU utilization per task.

## Slot Information

Use this page to display slot information and supported cards.

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



### Slot Summary

This screen displays details of the different slots in the different units in the stack.

The following table displays Slot Summary information.

**Table 2-7.**

Field	Description
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 off.
Card Model ID	Displays the model ID of the card configured for the slot.
Card Description	Displays the description of the card configured for the slot.

## Supported Cards

The following table displays Supported Cards information.

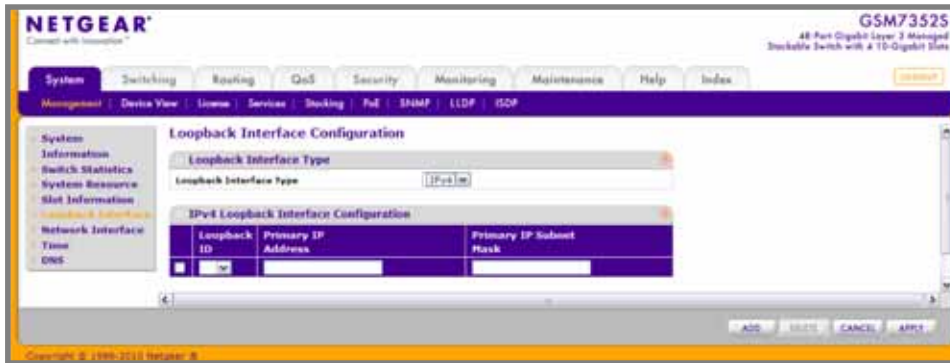
**Table 2-8.**

Field	Description
Card Model	Displays the list of models of all cards that can be supported.
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 a data field used to identify the supported card.

## Loopback Interface

Use this page to create, configure, and remove Loopback interfaces.

To display the Loopback Interface page, click **System > Management > Loopback Interface**. A screen similar to the following displays.



1. Use the **Loopback Interface Type** field to select IPv4 or IPv6 loopback interface to configure the corresponding attributes.
2. Use the **Loopback ID** field to select list of currently configured loopback interfaces.
3. Use the **Primary Address** field to input the primary IPv4 address for this interface in dotted decimal notation. This option only visible when IPv4 loopback is selected.
4. Use the **Primary Mask** field to input the primary IPv4 subnet mask for this interface in dotted decimal notation. This option only visible when IPv4 loopback is selected.
5. Use the **Secondary IP Address** field to input the secondary IP address for this interface in dotted decimal notation. This input field is visible only when 'Add Secondary' is selected. This option only visible when IPv4 loopback is selected.
6. Use the **Secondary Subnet Mask** field to input the secondary subnet mask for this interface in dotted decimal notation. This input field is visible only when 'Add Secondary' is selected. This option only visible when IPv4 loopback is selected.
7. Use the **IPv6 Mode** field to enable IPv6 on this interface using the IPv6 address. This option is only configurable prior to specifying an explicit IPv6 address. This option only visible when IPv6 loopback is selected.
8. Use the **IPv6 Address** field to enter the IPv6 address in the format prefix/length. This option only visible when IPv6 loopback is selected.
9. Use the **EUI64** field to optionally specify the 64-bit extended unique identifier (EUI-64). This option only visible when IPv6 loopback is selected.

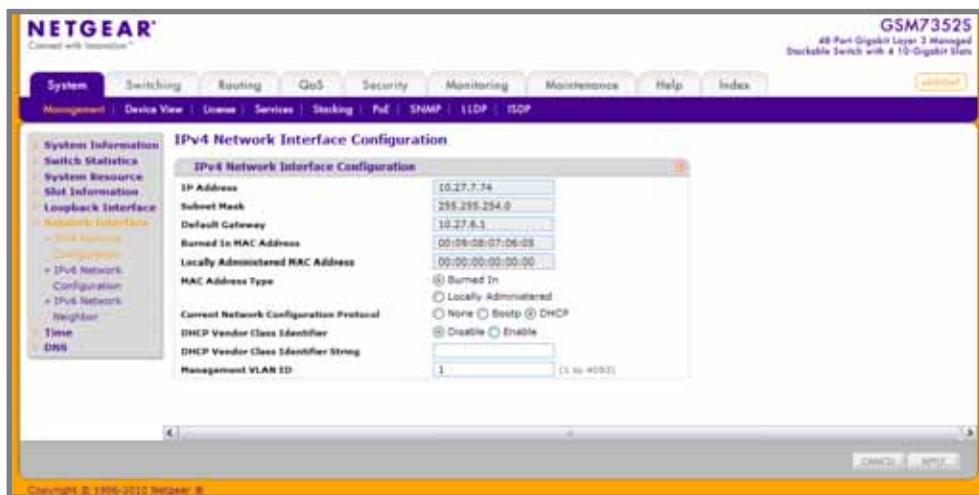
## Network Interface

From the Network Interface link, you can access the following pages:

- [IPv4 Network Configuration](#) on page 33
- [IPv6 Network Configuration](#) on page 35n
- [IPv6 Network Neighbor](#) on page 37

### IPv4 Network Configuration

To display the IPv4 Network Configuration page, click **System > Management > Network Interface > IPv4 Network Configuration**. A screen similar to the following displays.



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

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

- BOOTP
- DHCP
- Terminal interface via the EIA-232 port

Once you have established in-band connectivity, you can change the IP information using any of the following:

- Terminal interface via the EIA-232 port
  - Terminal interface via telnet
  - SNMP-based management
  - Web-based management
1. Use **IP Address** to specify the IP address of the interface. The factory default value is 169.254.100.100.
  2. Use **Subnet Mask** to enter the IP subnet mask for the interface. The factory default value is 255.255.0.0.
  3. Use **Default Gateway** to specify the default gateway for the IP interface. The factory default value is 0.0.0.0
  4. Use **Locally Administered MAC Address** to configure a locally administered MAC address for in-band connectivity instead of using the burned-in universally administered MAC address. In addition to entering an address in this field, you must also set the MAC address type to locally administered. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, in other words, byte 0 must have a value between x'40' and x'7F'.
  5. Use **MAC Address type** to specify whether the burned-in or the locally administered MAC address should be used for in-band connectivity. The factory default is to use the burned-in MAC address
  6. Use **Current Network Configuration Protocol** to specify what the switch should do following power-up: transmit a Bootp request, transmit a DHCP request, or do nothing (none). The factory default is DHCP.
  7. Use **DHCP Vendor Class Identifier** to enable DHCP VendorId option on the client.
  8. Use **DHCP Vendor Class Identifier String** to specify DHCP VendorId option string on the client.
  9. Use **Management VLAN ID** to specify the management VLAN ID of the switch. It may be configured to any value in the range of 1 - 4093. The management VLAN is used for management of the switch. This field is configurable for administrative users and read-only for other users.

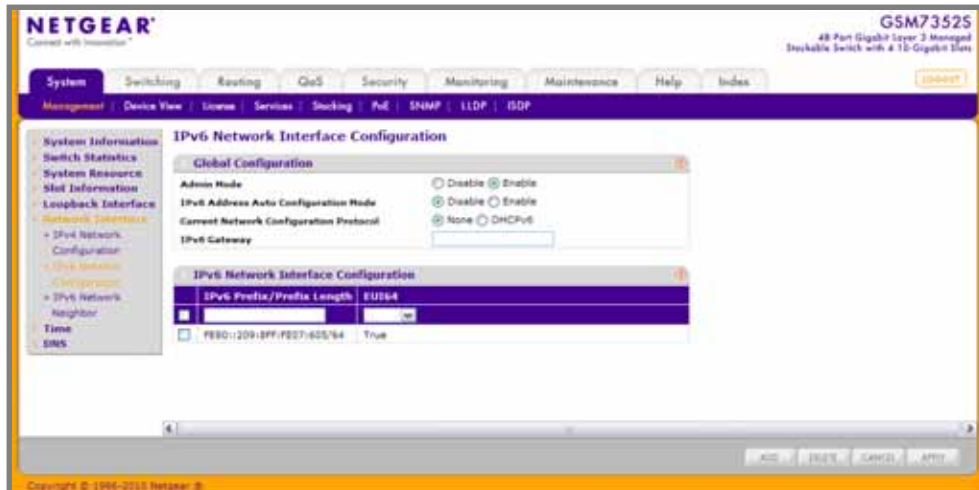
The following table describes IPv4 Network Configuration information.

**Table 2-9.**

Field	Description
<b>Burned In MAC Address</b>	The burned-in MAC address used for in-band connectivity if you choose not to configure a locally administered address.

## IPv6 Network Configuration

To display the IPv6 Network Configuration page, click **System > Management > Network Interface > IPv6 Network Configuration**. A screen similar to the following displays.



The IPv6 network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

To access the switch over an IPv6 network you must first configure it with IPv6 information (IPv6 prefix, prefix length, and default gateway). You can configure the IP information using any of the following:

- IPv6 Auto Configuration
- DHCPv6
- Terminal interface via the EIA-232 port

Once you have established in-band connectivity, you can change the IPv6 information using any of the following:

- Terminal interface via the EIA-232 port
- Terminal interface via telnet
- SNMP-based management
- Web-based management

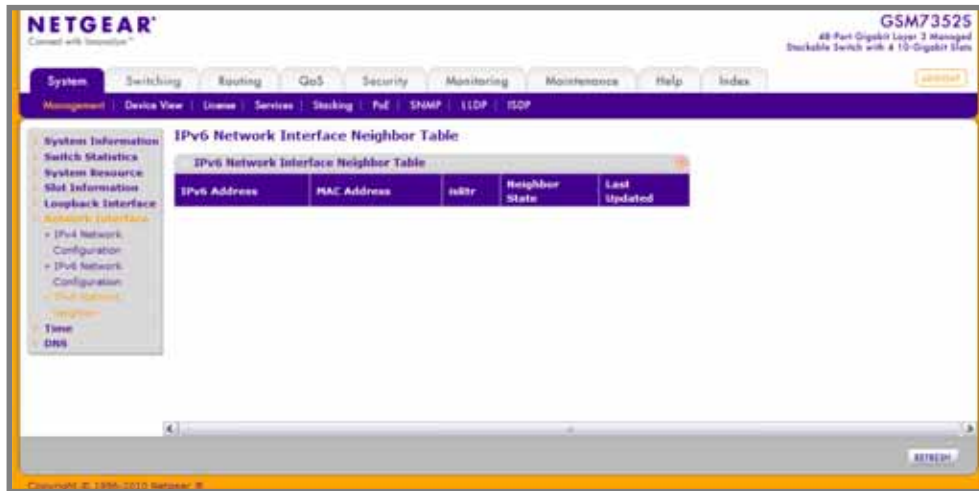
1. Use **Admin Mode** to enable or disable the IPv6 network interface on the switch. The default value is enable.
2. Use **IPv6 Address Auto Configuration Mode** to set the IPv6 address for the IPv6 network interface in auto configuration mode if this option is enabled. The default value is disable. Auto configuration can be enabled only when IPv6 Auto config or DHCPv6 are not enabled on any of the management interfaces.
3. Use **Current Network Configuration Protocol** to configure the IPv6 address for the IPv6 network interface by DHCPv6 protocol if this option is enabled. The default value is None. DHCPv6 can be enabled only when IPv6 Auto config or DHCPv6 are not enabled on any of the management interfaces.
4. Use **DHCPv6 Client DUID** to specify an Identifier used to identify the client's unique DUID value. This option only displays when DHCPv6 is enabled.
5. Use **IPv6 Gateway** to specify the gateway for the IPv6 network interface. The gateway address is in IPv6 global or link-local address format.
6. Use **IPv6 Prefix/Prefix Length** to add the IPv6 prefix and prefix length to the IPv6 network interface. The address is in global address format.
7. Use **EUI64** to specify whether to format the IPv6 address in EUI-64 format. 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.



## IPv6 Network Neighbor

Use this page to display IPv6 Network Port Neighbor entries.

To display the IPv6 Network Neighbor page, click **System > Management > Network Interface > IPv6 Network Neighbor**. A screen similar to the following displays.



The following table displays IPv6 Network Interface Neighbor Table information.

**Table 2-10.**

Field	Description
IPv6 address	The Ipv6 Address of a neighbor switch visible to the network interface.
MAC address	The MAC address of a neighbor switch.
IsRtr	True(1) if the neighbor machine is a router, false(2) otherwise.
Neighbor State	The state of the neighboring switch: <ul style="list-style-type: none"> <li>• reachable(1) - The neighbor is reachable by this switch.</li> <li>• stale(2) - Information about the neighbor is scheduled for deletion.</li> <li>• delay(3) - No information has been received from neighbor during delay period.</li> <li>• probe(4) - Switch is attempting to probe for this neighbor.</li> <li>• unknown(6) - Unknown status.</li> </ul>
Last Updated	The last sysUpTime that this neighbor has been updated.

## Time

ProSafe® Managed Switches 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. ProSafe® Managed Switches software operates only as an SNTP client 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.

## SNTP Global Configuration

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

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

**NETGEAR**  
GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

System Switching Routing QoS Security Monitoring Maintenance Help Index

Management Device View License Services Stacking SNMP LLDP ISDP

**SNTP Global Configuration**

Client Mode: ☐ Disable ☒ Unicast ☐ Broadcast

Port: 123 (1 to 65535)

Unicast Poll Interval: 6 (6 to 10)

Broadcast Poll Interval: 6 (6 to 10)

Unicast Poll Timeout: 5 (1 to 30)

Unicast Poll Retry: 1 (0 to 10)

Time Zone Name:

Offset Hours: 0 (-12 to 12)

Offset Minutes: 0 (0 to 59)

**SNTP Global Status**

Version	4
Supported Mode	Unicast and Broadcast
Last Update Time	JUL 02 17:05:52 2010 (UTC+0:00)
Last Attempt Time	JUL 02 17:05:52 2010 (UTC+0:00)
Last Attempt Status	Success
Server IP Address	216.243.71.251
Address Type	IPv4
Server Stratum	2
Reference Clock Id	NTP Srv: 10.10.0.5
Server Mode	Server
Unicast Server Max Entries	3
Unicast Server Current Entries	1
Broadcast Count	0

Copyright © 1994-2010 Netgear, Inc.

## SNTP Global Configuration

SNTP stands for Simple Network Time Protocol. As its name suggests, it is a less complicated version of Network Time Protocol, which is a system for synchronizing the clocks of networked computer systems, primarily when data transfer is handled via the Internet.

1. Use **Client Mode** to specify the mode of operation of SNTP Client. An SNTP client may operate in one of the following modes.
  - **Disable** - SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed.
  - **Unicast** - SNTP operates in a point to point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally the round-trip delay and local clock offset relative to the server.
  - **Broadcast** - SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has Internet wide scope.

Default value is Disable.

2. Use **Port** to specify the local UDP port to listen for responses/broadcasts. Allowed range is 1 to 65535. Default value is 123.
3. Use **Unicast Poll Interval** to specify the number of seconds between unicast poll requests expressed as a power of two when configured in unicast mode. Allowed range is (6 to 10). Default value is 6.
4. Use **Broadcast Poll Interval** to specify the number of seconds between broadcast poll requests expressed as a power of two when configured in broadcast mode. Broadcasts received prior to the expiry of this interval are discarded. Allowed range is (6 to 10). Default value is 6.
5. Use **Unicast Poll Timeout** to specify the number of seconds to wait for an SNTP response when configured in unicast mode. Allowed range is (1 to 30). Default value is 5.
6. Use **Unicast Poll Retry** to specify the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode. Allowed range is (0 to 10). Default value is 1.
7. When using SNTP/NTP time servers to update the switch's clock, the time data received from the server is based on Coordinated Universal Time (UTC) which is the same as Greenwich Mean Time (GMT). This may not be the time zone in which the switch is located.

Use **Time Zone Name** to configure a timezone specifying the number of hours and optionally the number of minutes difference from UTC with Offset Hours and Offset Minutes. The time zone can affect the display of the current system time. The default value is UTC.

8. Use **Offset Hours** to specify the number of hours difference from UTC. See Time Zone Name ([step 7](#) previous) for more information. Allowed range is (-24 to 24). The default value is 0.
9. Use **Offset Minutes** to specify the number of Minutes difference from UTC. See Time Zone Name ([step 7](#) previous) for more information. Allowed range is 0 to 59. The default value is 0.

## SNTP Global Status

The following table displays SNTP Global Status information.

**Table 2-11.**

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	<p>Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes.</p> <ul style="list-style-type: none"> <li>• Other - None of the following enumeration values.</li> <li>• Success - The SNTP operation was successful and the system time was updated.</li> <li>• Request Timed Out - A directed SNTP request timed out without receiving a response from the SNTP server.</li> <li>• Bad Date Encoded - The time provided by the SNTP server is not valid.</li> <li>• Version Not Supported - The SNTP version supported by the server is not compatible with the version supported by the client.</li> <li>• Server Unsynchronized - The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message.</li> <li>• 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.</li> </ul>
Server IP Address	Specifies the IP address of the server for the last received valid packet. If no message has been received from any server, an empty string is shown.
Address Type	Specifies the address type of the SNTP Server address for the last received valid packet.
Server Stratum	Specifies the claimed stratum of the server for the last received valid packet.
Reference Clock Id	Specifies the reference clock identifier of the server for the last received valid packet.

**Table 2-11.**

Field	Description
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.
Broadcast Count	Specifies the number of unsolicited broadcast SNTP messages that have been received and processed by the SNTP client since last reboot.

## 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**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management | Device View | License | Services | Stacking | **SNMP** | LLDP | ISDP

**SNTP Server Configuration**

Server Type	Address	Port	Priority	Version
<input type="checkbox"/> IP	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input checked="" type="checkbox"/> DNS	time-d.netgear.com	123	1	4

**SNTP Server Status**

Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests
time-d.netgear.com	JUL 02 17:21:55 2010 (UTC+0:00)	JUL 02 17:21:55 2010 (UTC+0:00)	Success	3780	0

ADD DELETE CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

To configure a new SNTP Server:

- 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). Default value is IPv4.
  - Address** - Specify the address of the SNTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this address. If this address is a DNS hostname, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
  - 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** - Specify the priority of this server entry in determining the sequence of servers to which SNTP requests will be sent. The client continues sending requests to different servers until a successful response is received or all servers are exhausted. This object indicates the order in which to query the servers. A server entry with a precedence of 1 will be queried before a server with a priority of 2, and so forth. If more than one server has the same priority then the requesting order will follow the lexicographical ordering of the entries in this table. Allowed range is (1 to 3). Default value is 1.
  - Version** - Enter the NTP version running on the server. The range is 1–4. The default is 4.
- 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.
7. Click **Refresh** to refresh the page with the most current data from the switch.



## SNTP Server Status

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.

The following table displays SNTP Server Status information.

**Table 2-12.**

Field	Description
Address	Specifies all the existing Server Addresses. If no Server configuration exists, a message saying "No SNTP server exists" flashes on the screen.
Last Update Time	Specifies the local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	Specifies the local date and time (UTC) that this SNTP server was last queried.
Last Attempt Status	<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"> <li>• Other - None of the following enumeration values.</li> <li>• Success - The SNTP operation was successful and the system time was updated.</li> <li>• Request Timed Out - A directed SNTP request timed out without receiving a response from the SNTP server.</li> <li>• Bad Date Encoded - The time provided by the SNTP server is not valid.</li> <li>• Version Not Supported - The SNTP version supported by the server is not compatible with the version supported by the client.</li> <li>• Server Unsynchronized - The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message.</li> <li>• 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.</li> </ul>
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.

## 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**.

The screenshot displays the Netgear DNS Configuration web interface. At the top, the Netgear logo and model number GSM7352S are visible. The main navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar lists various system configuration options. The central panel is titled 'DNS Configuration' and contains the following settings:

- DNS Status:** Radio buttons for 'Disable' and 'Enable'.
- DNS Default Name:** A text input field with a placeholder '(1 to 255 Characters)'.
- Retry Number:** A text input field with a placeholder '(0 to 100)'.
- Response Timeout (secs):** A text input field with a placeholder '(0 to 3600 secs)'.
- DNS Server Configuration:** A table with columns for 'Serial No.', 'DNS Server', and 'Preference'.
 

Serial No.	DNS Server	Preference
1	10.27.138.20	0
2	10.27.138.21	1

At the bottom of the page, there are buttons for 'Add', 'Edit', 'Cancel', and 'Apply'.

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. Default value is Enable.
  - **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 length of the name should not be longer than 255 characters.
3. Use **Retry Number** to specify the number of times to retry sending DNS queries to DNS server. This number ranges from 0 to 100. The default value is 2.
4. Use **Response Timeout (secs)** to specify the amount of time, in seconds, to wait for a response to a DNS query. This timeout ranges from 0 to 3600. The default value is 3.
5. 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 precedence is set in the order created.

6. 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.
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. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **ADD** to add the specified DNS Server to the List of DNS Servers. Configuration changes take effect immediately.
10. Click **Delete** to delete the specified DNS Server from the list of DNS Servers. If no DNS Server is specified then it will delete all the DNS Servers

### DNS Server Configuration

The following table displays DNS Server Configuration information.

**Table 2-13.**

Field	Description
Serial No	The sequence number of the DNS server.
Preference	Shows the preference of the DNS Server. The preference is determined by the order they were entered.

## 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**.

The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual. The page is titled "DNS Host Configuration". It features a sidebar with navigation links: System, Information, Switch Statistics, System Resource, Slot Information, Loopback, Interface, Network, Interface, Time, DNS, Configuration, host, and Configuration. The main content area has a form for adding static entries and a table for dynamic host mappings.

Host	Total	Elapsed	Type	Addresses
time-d.netgear.com	28780	1232	IP	216.243.71.251

To add a static entry to the local DNS table:

1. Specify the static host name to add. Its length can not exceed 255 characters and it is a mandatory field for the user.
2. Specify the IP address in standard IPv4 dot 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 Mapping table shows host name-to-IP address entries that the switch has learned. The following table describes the dynamic host fields.

**Table 2-14.**

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.
Addresses	Lists the IP address associated with the host name.

## License

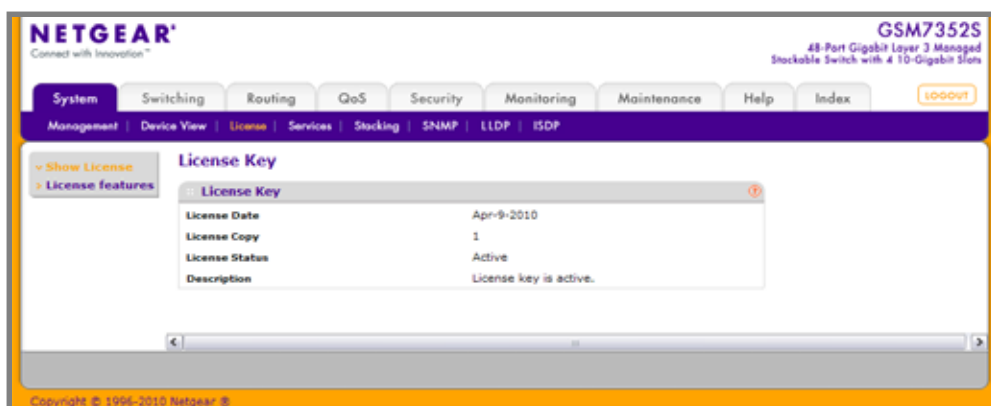
The License link is available only for models GSM7328Sv1, GSM7352Sv1, GSM7328FS, GSM7228PS, and GSM7252PS.

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

- [Show License](#) on page 49
- [License Features](#) on page 50

### Show License

To display the Show License page, click **System > License > Show License**. A screen similar to the following displays.



### License Key

This page provides information about available License Keys for various features. By default those License Keys are not available. If License Key for feature is not available, user will not

be allowed to configure this functionality. Available License Key allows user to configure functionality.

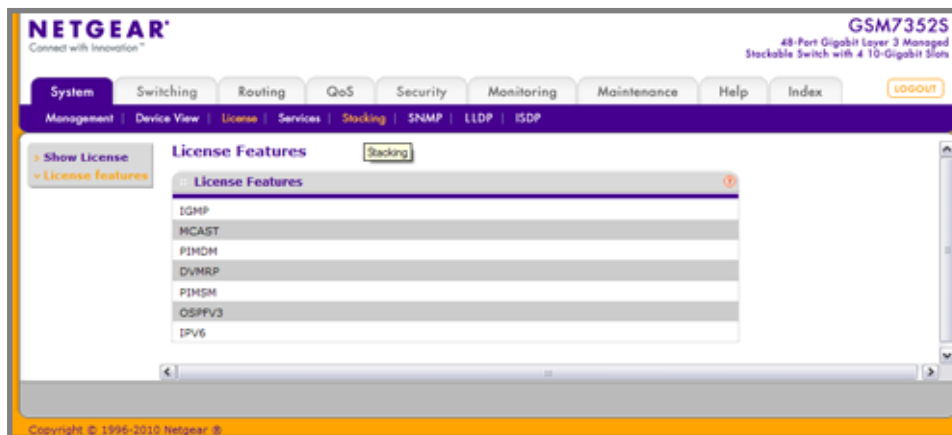
The following table describes the License Key fields.

**Table 2-15.**

Field	Description
License date	The date the license is purchased.
License copy	The information about the number of license.
License Status	Show whether License is Active/Inactive. "Inactive" means that user should download a license file and reboot a system
Description	Show status of License Key.

## License Features

To display the License Features page, click **System > License > License Features**. A screen similar to the following displays.



**Table 2-16.**

Feature	Description
Features	Displays list of features that require licensing.

## Services

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

- [DHCP Server](#) on page 51

- [DHCP Relay](#) on page 62
- [DHCP L2 Relay](#) on page 64
- [UDP Relay](#) on page 67
- [DHCPv6 Server](#) on page 71
- [DHCPv6 Relay](#) on page 79

## DHCP Server

From the DHCP Server link, you can access the following pages:

- [DHCP Server Configuration](#) on page 52
- [DHCP Pool Configuration](#) on page 54
- [DHCP Pool Options](#) on page 57
- [DHCP Server Statistics](#) on page 58
- [DHCP Bindings Information](#) on page 60
- [DHCP Conflicts Information](#) on page 61

## DHCP Server Configuration

To display the DHCP Server Configuration page, click **System > Services > DHCP Server > DHCP Server Configuration**. A screen similar to the following displays.

The screenshot shows the Netgear web interface for a GSM7352S switch. The left sidebar contains a navigation menu with options like DHCP Server Configuration, DHCP Pool Configuration, DHCP Pool Options, DHCP Server Statistics, DHCP Bindings Information, DHCP Conflicts Information, DHCP Relay, DHCP L2 Relay, UDP Relay, DHCPv6 Server, and DHCPv6 Relay. The main content area is titled 'DHCP Server Configuration' and includes the following settings:

- Admin Mode:** Radio buttons for Disable (selected) and Enable.
- Ping Packet Count:** A text box containing the value '2', with a range of '(0, 2 to 10)'.
- Conflict Logging Mode:** Radio buttons for Disable and Enable (selected).
- Bootp Automatic Mode:** Radio buttons for Disable (selected) and Enable.

Below these settings is an 'Excluded Address' section with a table for IP ranges:

IP Range From	IP Range To

At the bottom of the page are buttons for 'ADD', 'DELETE', 'CANCEL', and 'APPLY'.

To enable or disable DHCP service:

1. Use **Admin Mode** to specify whether the DHCP Service is to be Enabled or Disabled. Default value is Disable.
2. Use **Ping Packet Count** to specify the number of packets a server sends to a Pool address to check for duplication as part of a ping operation. Default value is 2. Valid Range is (0, 2 to 10). Setting the value to 0 will disable the function.
3. Use **Conflict Logging Mode** to specify whether conflict logging on a DHCP Server is to be Enabled or Disabled. Default value is Enable.
4. Use **Bootp Automatic Mode** to specify whether Bootp for dynamic pools is to be Enabled or Disabled. Default value is Disable.
5. Click **CANCEL** to cancel the configuration on the screen. Resets 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.



### Excluded Address Configuration

1. Use the **IP Range From** field to specify the low address if you want to exclude a range of addresses. Specify the address to be excluded in case you want to exclude a single address.
2. Use the **IP Range To** field to specify the high address if you want to exclude a range of addresses. To exclude a single address, enter the same IP address as specified in IP range from or leave as 0.0.0.0.
3. Click **ADD** to add the exclude addresses configured on the screen to the switch.
4. Click **DELETE** to delete the exclude address from the switch.

## DHCP Pool Configuration

To display the DHCP Pool Configuration page, click **System > Services > DHCP Server > DHCP Pool Configuration**. A screen similar to the following displays.

The screenshot shows the Netgear web interface for DHCP Pool Configuration. The sidebar on the left lists various configuration options under 'DHCP Server'. The main configuration area includes fields for defining a new DHCP pool, such as Pool Name, Network Address, and Lease Time. The 'Create' option is selected in the Pool Name dropdown menu.

The following table describes the DHCP Pool Configuration fields.

Table 2-17.

Field	Description
Pool Name*	For a user with read/write permission, this field would show names of all the existing pools along with an additional option "Create". When the user selects "Create" another text box "Pool Name" appears where the user may enter name for the Pool to be created. For a user with read only permission, this field would show names of the existing pools only.
Pool Name	This field appears when the user with read-write permission has selected "Create" in the Drop Down list against Pool Name*. Specifies the Name of the Pool to be created. Pool Name can be up to 31 characters in length.

Table 2-17.

Field	Description
Type of Binding	Specifies the type of binding for the pool. <ul style="list-style-type: none"> <li>• Unallocated</li> <li>• Dynamic</li> <li>• Manual</li> </ul>
Network Address	Specifies the subnet address for a DHCP address of a dynamic pool.
Network Mask	Specifies the subnet number for a DHCP address of a dynamic pool. Either Network Mask or Prefix Length can be configured to specify the subnet mask but not both.
Network Prefix Length	Specifies the subnet number for a DHCP address of a dynamic pool. Either Network Mask or Prefix Length can be configured to specify the subnet mask but not both. Valid Range is (0 to 32)
Client Name	Specifies the Client Name for DHCP manual Pool.
Hardware Address	Specifies the MAC address of the hardware platform of the DHCP client.
Hardware Address Type	Specifies the protocol of the hardware platform of the DHCP client. Valid types are ethernet and ieee802. Default value is ethernet.
Client ID	Specifies the Client Identifier for DHCP manual Pool.
Host Number	Specifies the IP address for a manual binding to a DHCP client. Host can be set only if at least one among of Client Identifier or Hardware Address is specified. Deleting Host would delete Client Name, Client ID, Hardware Address for the Manual Pool and set the Pool Type to Unallocated.
Host Mask	Specifies the subnet mask for a manual binding to a DHCP client. Either Host Mask or Prefix Length can be configured to specify the subnet mask but not both.
Host Prefix Length	Specifies the subnet mask for a manual binding to a DHCP client. Either Host Mask or Prefix Length can be configured to specify the subnet mask but not both. Valid Range is (0 to 32)
Lease Time	Can be selected as "Infinite" to specify lease time as Infinite or "Specified Duration" to enter a specific lease period. In case of dynamic binding infinite implies a lease period of 60 days and In case of manual binding infinite implies indefinite lease period. Default Value is "Specified Duration".

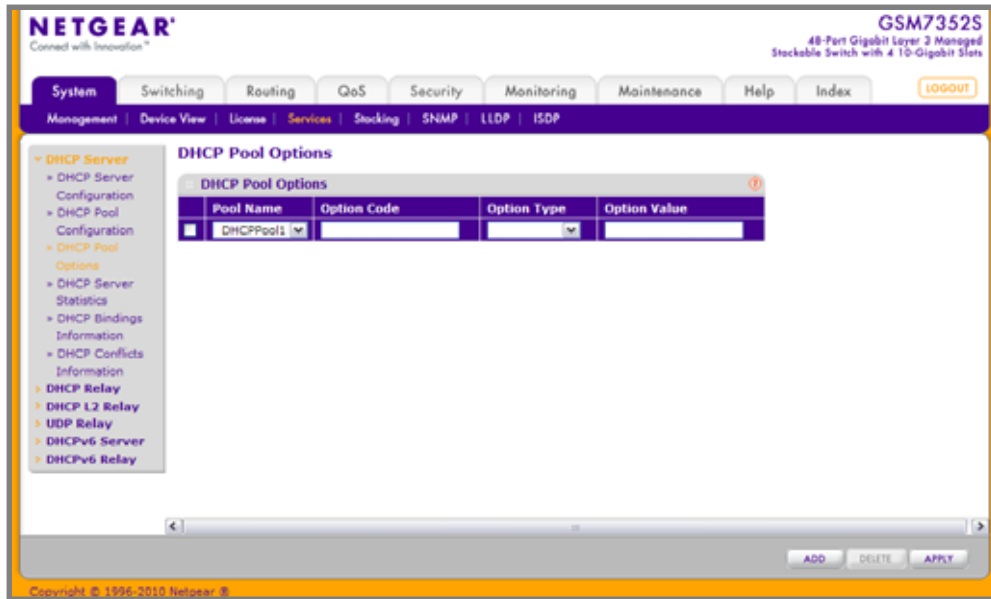
Table 2-17.

Field	Description
Days	Specifies the Number of Days of Lease Period. This field appears only if the user has specified "Specified Duration" as the Lease time. Default Value is 1. Valid Range is (0 to 59)
Hours	Specifies the Number of Hours of Lease Period. This field appears only if the user has specified "Specified Duration" as the Lease time. Valid Range is (0 to 22)
Minutes	Specifies the Number of Minutes of Lease Period. This field appears only if the user has specified "Specified Duration" as the Lease time. Valid Range is (0 to 86399)
Default Router Addresses	Specifies the list of Default Router Addresses for the pool. The user may specify up to 8 Default Router Addresses in order of preference.
DNS Server Addresses	Specifies the list of DNS Server Addresses for the pool. The user may specify up to 8 DNS Server Addresses in order of preference.
NetBIOS Name Server Addresses	Specifies the list of NetBIOS Name Server Addresses for the pool. The user may specify up to 8 NetBIOS Name Server Addresses in order of preference.
NetBIOS Node Type	Specifies the NetBIOS node type for DHCP clients: <ul style="list-style-type: none"> <li>• b-node Broadcast</li> <li>• p-node Peer-to-Peer</li> <li>• m-node Mixed</li> <li>• h-node Hybrid</li> </ul>
Next Server Address	Specifies the Next Server Address for the pool.
Domain Name	Specifies the domain name for a DHCP client. Domain Name can be up to 255 characters in length.
Bootfile	Specifies the name of the default boot image for a DHCP client. File Name can be up to 128 characters in length.

1. Use **ADD** to create the Pool Configuration.
2. Use **APPLY** to change the Pool Configuration. Sends the updated configuration to the switch. Configuration changes take effect immediately.
3. Use **DELETE** to delete the Pool. This field is not visible to a user with read only permission.

## DHCP Pool Options

To display the DHCP Pool Options page, click **System > Services > DHCP Server > DHCP Pool Options**. A screen similar to the following displays.



1. Use **Pool Name** to select the Pool Name.
2. **Option Code** specifies the Option Code configured for the selected Pool.
3. Use **Option Type** to specify the Option Type against the Option Code configured for the selected pool:
  - ASCII
  - Hex
  - IP Address
4. **Option Value** specifies the Value against the Option Code configured for the selected pool.
5. Click **ADD** to add a new Option Code for the selected pool.
6. Click **DELETE** to delete the Option Code for the selected pool.

## DHCP Server Statistics

To display the DHCP Server Statistics page, click **System** > **Services** > **DHCP Server** > **DHCP Server Statistics**. A screen similar to the following displays.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management | Device View | License | Services | **Stacking** | SNMP | LLDP | ISDP

**DHCP Server Statistics**

**Binding Details**

Automatic Bindings	0
Expired Bindings	0
Malformed Messages	0

**Message Received**

DHCPDISCOVER	0
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0

**Message Sent**

DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

CLEAR REFRESH

Copyright © 1996-2010 Netgear, Inc.

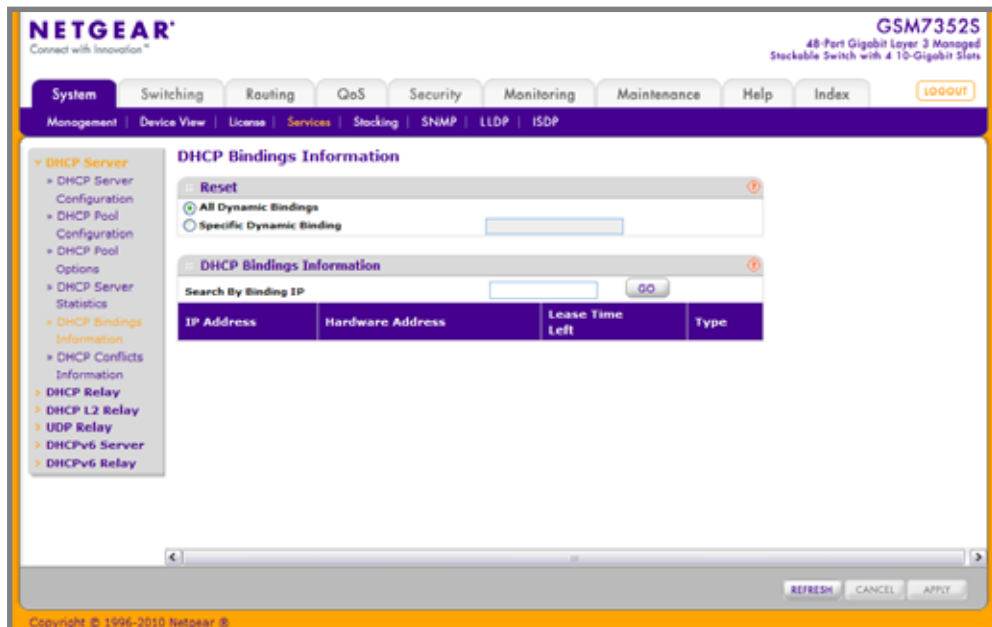
The following table describes the DHCP Server Statistics fields.

**Table 2-18.**

Field	Description
Automatic Bindings	Specifies the number of Automatic Bindings on the DHCP Server.
Expired Bindings	Specifies the number of Expired Bindings on the DHCP Server.
Malformed Messages	Specifies the number of the malformed messages.
DHCPDISCOVER	Specifies the number of DHCPDISCOVER messages received by the DHCP Server.
DHCPREQUEST	Specifies the number of DHCPREQUEST messages received by the DHCP Server.
DHCPDECLINE	Specifies the number of DHCPDECLINE messages received by the DHCP Server.
DHCPRELEASE	Specifies the number of DHCPRELEASE messages received by the DHCP Server.
DHCPINFORM	Specifies the number of DHCPINFORM messages received by the DHCP Server.
DHCPOFFER	Specifies the number of DHCPOFFER messages sent by the DHCP Server.
DHCPACK	Specifies the number of DHCPACK messages sent by the DHCP Server.
DHCNNAK	Specifies the number of DHCNNAK messages sent by the DHCP Server.

## DHCP Bindings Information

To display the DHCP Bindings Information page, click **System > Services > DHCP Server > DHCP Bindings Information**. A screen similar to the following displays.



### 1. Choose:

- **All Dynamic Bindings** to specify all dynamic bindings to be deleted.
- **Specific Dynamic Binding** to specify specific dynamic binding to be deleted.

The following table describes the DHCP Bindings Information fields.

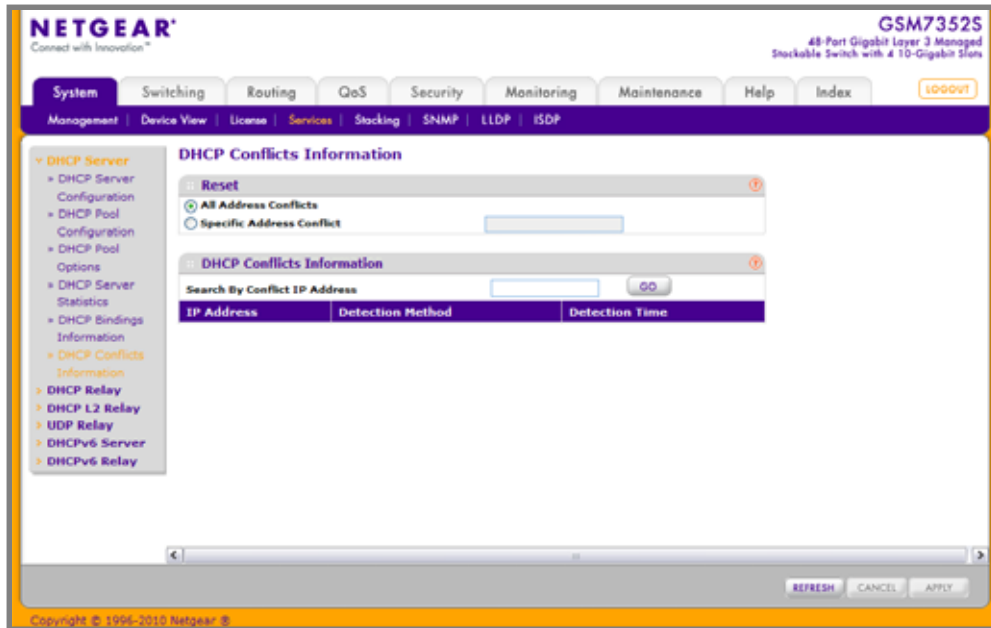
**Table 2-19.**

Field	Description
IP Address	Specifies the Client's IP Address.
Hardware Address	Specifies the Client's Hardware Address.
Lease Time Left	Specifies the Lease time left in Days, Hours and Minutes dd:hh:mm format.
Type	Specifies the Type of Binding: Dynamic / Manual.



## DHCP Conflicts Information

To display the DHCP Conflicts Information page, click **System > Services > DHCP Server > DHCP Conflicts Information**. A screen similar to the following displays.



### 1. Choose:

- **All Address Conflicts** to specify all address conflicts to be deleted.
- **Specific Address Conflict** to specify a specific dynamic binding to be deleted.

The following table describes the DHCP Conflicts Information fields.

**Table 2-20.**

Field	Description
IP Address	Specifies the IP Address of the host as recorded on the DHCP server.
Detection Method	Specifies the manner in which the IP address of the hosts were found on the DHCP Server.
Detection Time	Specifies the time when the conflict was detected in N days NNh:NNm:NNs format with respect to the system up time.

## DHCP Relay

To display the DHCP Relay page, click **System > Services > DHCP Relay**. A screen similar to the following displays.

The screenshot shows the Netgear web interface for a GSM7352S switch. The top navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar lists various services, with DHCP Relay selected. The main content area is titled 'DHCP Relay' and contains the following configuration fields:

- Maximum Hop Count:** A text box with the value '4' and a range '(1 to 16)'.
- Admin Mode:** Radio buttons for 'Disable' (selected) and 'Enable'.
- Minimum Wait Time (secs):** A text box with the value '0' and a range '(0 to 100)'.
- Circuit ID Option Mode:** Radio buttons for 'Disable' (selected) and 'Enable'.

Below these fields is a 'DHCP Status' section with three text boxes, all showing '0':

- Requests Received
- Requests Relayed
- Packets Discarded

At the bottom right of the configuration area are buttons for 'REFRESH', 'CANCEL', and 'APPLY'. The footer shows 'Copyright © 1996-2010 Netgear Inc.'.

### DHCP Relay Configuration

1. Use **Maximum Hop Count** to enter the maximum number of hops a client request can take before being discarded. The range is (1 to 16). The default value is 4.
2. Use **Admin Mode** to select enable or disable radio button. When you select 'enable' DHCP requests will be forwarded to the IP address you entered in the 'Server Address' field.
3. Use **Minimum Wait Time** to enter a Minimum Wait Time in seconds. This value will be compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets will only be forwarded when the time stamp exceeds the minimum wait time. The range is (0 to 100).
4. Use **Circuit ID Option Mode** to enable or disable Circuit ID Option mode. If you select 'enable' Relay Agent options will be added to requests before they are forwarded to the server and removed from replies before they are forwarded to clients.

### *DHCP Relay Status*

The following table describes the DHCP Relay Status fields.

**Table 2-21.**

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

## DHCP L2 Relay

From the DHCP L2 Relay link, you can access the following pages:

- [DHCP L2 Relay Global Configuration](#) on page 64
- [DHCP L2 Relay Interface Configuration](#) on page 65
- [DHCP L2 Relay Interface Statistics](#) on page 66s

### DHCP L2 Relay Global Configuration

To display the DHCP L2 Relay Global Configuration page, click **System > Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration**. A screen similar to the following displays.

The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual interface. The top navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar shows a tree view with options like DHCP Server, DHCP Relay, and DHCP L2 Relay. The main content area displays the DHCP L2 Relay Global Configuration page. It includes a section for Admin Mode with a toggle for Disable/Enable. Below this is a table for DHCP L2 Relay VLAN Configuration with columns for VLAN ID, Admin Mode, Circuit ID Mode, and Remote ID String. The table shows a single entry for VLAN 1 with Admin Mode set to Disable and Circuit ID Mode set to Disable. The bottom of the page has a footer with the copyright notice: Copyright © 1996-2010 Netgear.

### DHCP L2 Relay Global Configuration

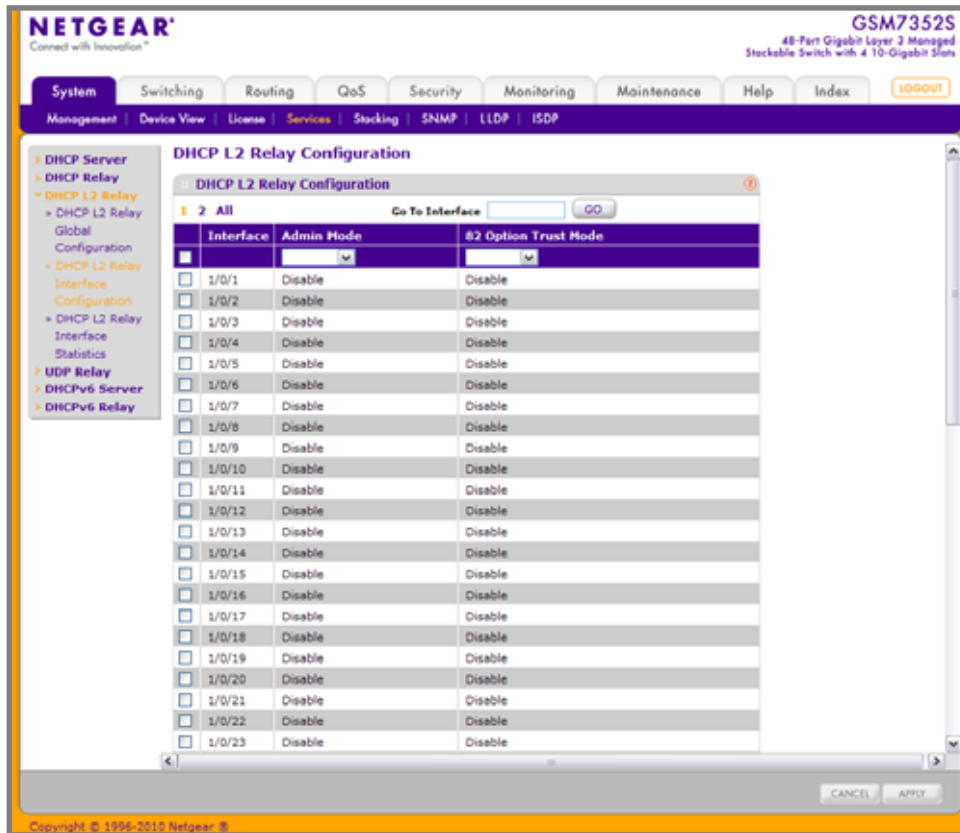
1. Use **Admin Mode** to enable or disable the DHCP L2 Relay on the switch. The default is Disable.

### DHCP L2 Relay VLAN Configuration

1. **VLAN ID** shows the VLAN ID configured on the switch.
2. Use **Admin Mode** to enable or disable the DHCP L2 Relay on the selected VLAN.
3. Use **Circuit ID Mode** to enable or disable the Circuit ID suboption of DHCP Option-82.
4. Use **Remote ID String** to specify the Remote ID when Remote ID mode is enabled.

## DHCP L2 Relay Interface Configuration

To display the DHCP L2 Relay Interface Configuration page, click **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**. A screen similar to the following displays.



1. Use **Admin Mode** to enable or disable the DHCP L2 Relay on the selected interface. Default is disable.
2. Use **82 Option Trust Mode** to enable or disable an interface to be trusted for DHCP L2 Relay (Option-82) received.

## DHCP L2 Relay Interface Statistics

To display the DHCP L2 Relay Interface Statistics page, click **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Statistics**. A screen similar to the following displays.

The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual. The page title is "DHCP L2 Relay Interface Statistics". The table below shows the data for each interface.

Interface	Untrusted Server Messages With Opt82	Untrusted Client Messages With Opt82	Trusted Server Messages Without Opt82	Trusted Client Messages Without Opt82
1/0/1	0	0	0	0
1/0/2	0	0	0	0
1/0/3	0	0	0	0
1/0/4	0	0	0	0
1/0/5	0	0	0	0
1/0/6	0	0	0	0
1/0/7	0	0	0	0
1/0/8	0	0	0	0
1/0/9	0	0	0	0
1/0/10	0	0	0	0
1/0/11	0	0	0	0
1/0/12	0	0	0	0
1/0/13	0	0	0	0
1/0/14	0	0	0	0
1/0/15	0	0	0	0
1/0/16	0	0	0	0
1/0/17	0	0	0	0
1/0/18	0	0	0	0
1/0/19	0	0	0	0
1/0/20	0	0	0	0
1/0/21	0	0	0	0
1/0/22	0	0	0	0
1/0/23	0	0	0	0

The following table describes the DHCP L2 Relay Interface Statistics fields.

**Table 2-22.**

Field	Description
Interface	Shows the interface from which the DHCP message is received.
UntrustedServerMsgsWithOpt82	Shows the number of DHCP message with option82 received from an untrusted server.
UntrustedClientMsgsWithOpt82	Shows the number of DHCP message with option82 received from an untrusted client.
TrustedServerMsgsWithoutOpt82	Shows the number of DHCP message without option82 received from a trusted server.
TrustedClientMsgsWithoutOpt82	Shows the number of DHCP message without option82 received from a trusted client.

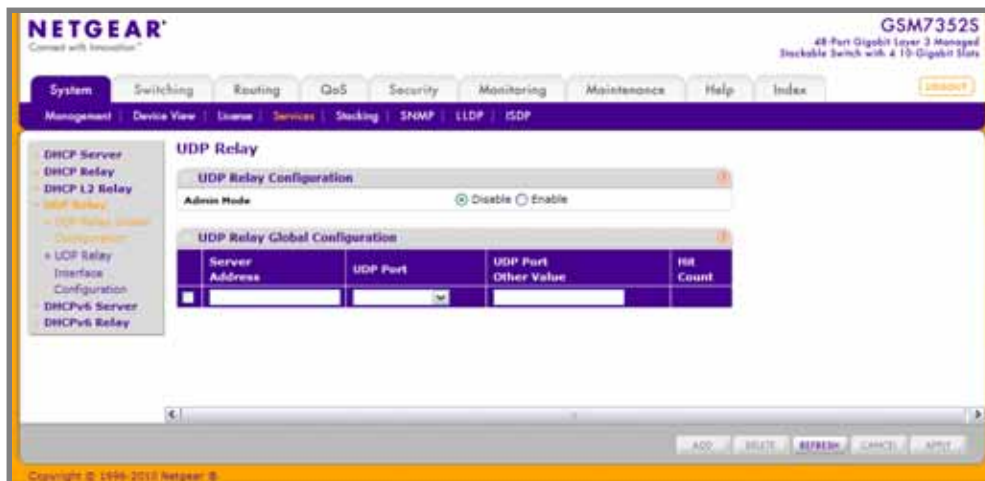
## UDP Relay

From the UDP Relay link, you can access the following pages:

- [UDP Relay Global Configuration](#) on page 67
- [UDP Relay Interface Configuration](#) on page 69

### UDP Relay Global Configuration

To display the UDP Relay Global Configuration page, click **System > Services > UDP Relay > UDP Relay Global Configuration**. A screen similar to the following displays.



1. Use **Admin Mode** to enable or disable the UDP Relay on the switch. The default value is disable.
2. Use **Server Address** to specify the UDP Relay Server Address in x.x.x.x format.
3. Use **UDP Port** to specify the UDP Destination Port. These ports are supported:
  - **DefaultSet** - Relay UDP port 0 packets. This is specified if no UDP port is selected when creating the Relay server.
  - **dhcp** -Relay DHCP (UDP port 67) packets.
  - **domain** - Relay DNS (UDP port 53) packets.
  - **isakmp** - Relay ISAKMP (UDP port 500) packets.
  - **mobile-ip** - Relay Mobile IP (UDP port 434) packets
  - **nameserver** - Relay IEN-116 Name Service (UDP port 42) packets
  - **netbios-dgm** - Relay NetBIOS Datagram Server (UDP port 138) packets
  - **netbios-ns** - Relay NetBIOS Name Server (UDP port 137) packets
  - **ntp** - Relay network time protocol (UDP port 123) packets.
  - **pim-auto-rp** - Relay PIM auto RP (UDP port 496) packets.
  - **rip** - Relay RIP (UDP port 520) packets
  - **tacacs** - Relay TACACS (UDP port 49) packet

- **tftp** - Relay TFTP (UDP port 69) packets
  - **time** - Relay time service (UDP port 37) packets
  - **Other** - If this option is selected, the UDP Port Other Value is enabled. This option permits a user to enter their own UDP port in UDP Port Other Value.
4. Use **UDP Port Other Value** to specify a UDP Destination Port that lies between 0 and 65535.
  5. Click **ADD** to create an entry in UDP Relay Table with the specified configuration.
  6. Click **DELETE** to remove all entries or a specified one from UDP Relay Table.

The following table describes the UDP Relay Global Configuration fields.

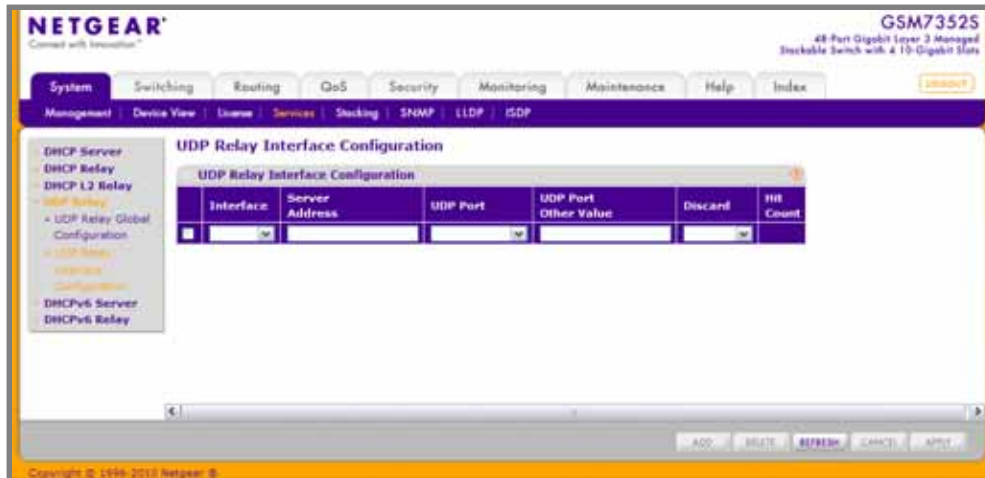
**Table 2-23.**

Field	Description
Hit Count	Show the number of UDP packets hitting the UDP port



## UDP Relay Interface Configuration

To display the UDP Relay Interface Configuration page, click **System > Services > UDP Relay > UDP Relay Interface Configuration**. A screen similar to the following displays.



1. Use **Interface** to select an Interface to be enabled for the UDP Relay.
2. Use **Server Address** to specify the UDP Relay Server Address in x.x.x.x format.
3. Use **UDP Port** to specify UDP Destination Port. The following ports are supported:
  - **DefaultSet** - Relay UDP port 0 packets. This is specified if no UDP port is selected when creating a Relay server.
  - **dhcp** - Relay DHCP (UDP port 67) packets.
  - **domain** - Relay DNS (UDP port 53) packets.
  - **isakmp** - Relay ISAKMP (UDP port 500) packets.
  - **mobile-ip** - Relay Mobile IP (UDP port 434) packets
  - **nameserver** - Relay IEN-116 Name Service (UDP port 42) packets
  - **netbios-dgm** - Relay NetBIOS Datagram Server (UDP port 138) packets
  - **netbios-ns** - Relay NetBIOS Name Server (UDP port 137) packets
  - **ntp** - Relay network time protocol (UDP port 123) packets.
  - **pim-auto-rp** - Relay PIM auto RP (UDP port 496) packets.
  - **rip** - Relay RIP (UDP port 520) packets
  - **tacacs** - Relay TACACS (UDP port 49) packet
  - **tftp** - Relay TFTP (UDP port 69) packets
  - **time** - Relay time service (UDP port 37) packets
  - **Other** - If this option is selected, the UDP Port Other Value is enabled. This option permits the user to enter their own UDP port in UDP Port Other Value.
4. Use **UDP Port Other Value** to specify UDP Destination Port that lies between 0 and 65535.

5. Use **Discard** to enable/disable dropping of matched packets. Enable can be chosen only when a user enters 0.0.0.0 IP address. Discard mode can be set to Disable when user adds a new entry with a non-zero IP address.
6. Click **ADD** to create an entry in UDP Relay Table with the specified configuration.
7. Click **DELETE** to remove all entries or a specified one from UDP Relay Interface Configuration Table.

The following table describes the UDP Relay Interface Configuration fields.

**Table 2-24.**

Field	Description
Hit Count	Show the number of UDP packets hitting the UDP port.

## DHCPv6 Server

From the DHCPv6 Server link, you can access the following pages:

- [DHCPv6 Server Configuration](#) on page 71
- [DHCPv6 Pool Configuration](#) on page 72
- [DHCPv6 Prefix Delegation Configuration](#) on page 73
- [DHCPv6 Interface Configuration](#) on page 75
- [DHCPv6 Bindings Information](#) on page 76
- [DHCPv6 Server Statistics](#) on page 77

### DHCPv6 Server Configuration

To display the DHCPv6 Server Configuration page, click **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**. A screen similar to the following displays.

The screenshot shows the Netgear ProSafe web interface. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Below this is a sub-navigation bar with links for Management, Device View, License, Services, Stacking, SNMP, LLDP, and ISDP. The left sidebar contains a tree view with the following structure:

- DHCP Server
  - DHCP Relay
  - DHCP L2 Relay
  - UDP Relay
  - DHCPv6 Server
    - DHCPv6 Server Configuration (selected)
    - DHCPv6 Pool Configuration
    - DHCPv6 Prefix Delegation Configuration
    - DHCPv6 Interface Configuration
    - DHCPv6 Bindings Information
    - DHCPv6 Server Statistics
  - DHCPv6 Relay

The main content area is titled "DHCPv6 Server Configuration". It contains the following fields:

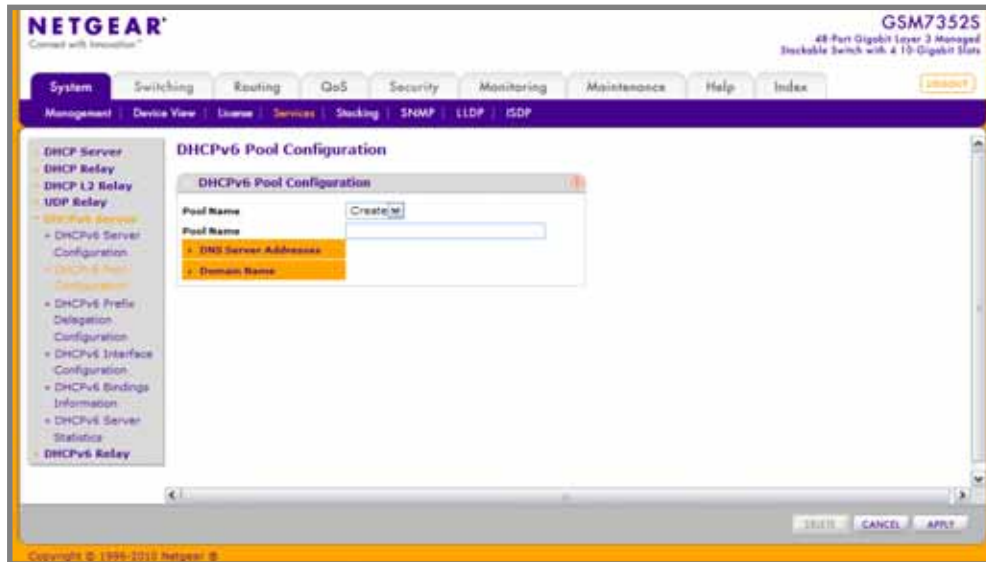
- Admin Mode:** Radio buttons for "Disable" (selected) and "Enable".
- Relay Option:** A text box containing "54" with a range "(54 to 65535)".
- Remote-id Sub-option:** A text box containing "1" with a range "(1 to 65535)".

At the bottom of the form are "CANCEL" and "APPLY" buttons. The footer of the page reads "Copyright © 1996-2010 Netgear Inc."

1. Use **Admin Mode** to specify DHCPv6 operation on the switch. Value is enabled or disabled.
2. Use **Relay Option** to specify Relay Agent Information Option value. The values allowed are between 54 to 65535. The default value is 54.
3. Use **Remote-id Sub-option** to specify the Relay Agent Information Option Remote-ID Sub-option type value. The values allowed are between 1 and 65535. The default value is 1.

## DHCPv6 Pool Configuration

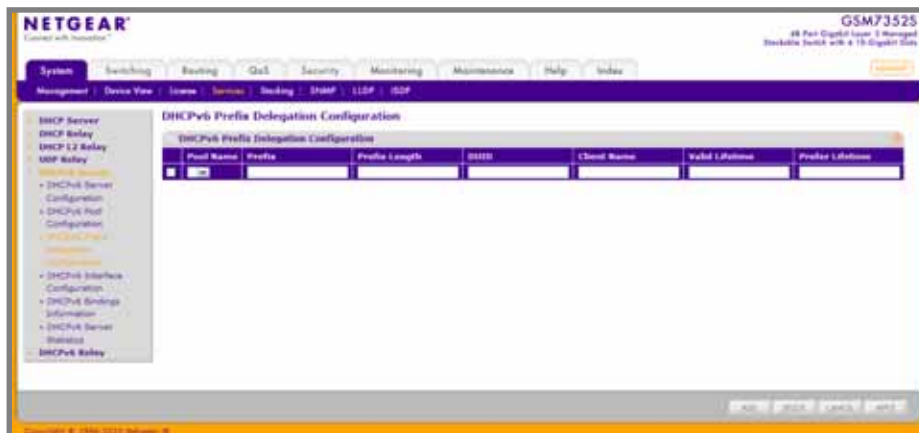
To display the DHCPv6 Pool Configuration page, click **System > Services > DHCPv6 Server > DHCPv6 Pool Configuration**. A screen similar to the following displays.



1. **Pool Name** - For a user with read/write permission, this field would show names of all the existing pools along with an additional option “Create”. When the user selects “Create” another text box “Pool Name” appears where the user may enter name for the Pool to be created. For a user with read only permission, this field would show names of the existing pools only.
2. Use **Pool Name** to specify a unique name for DHCPv6 pool. It may be up to 31 alphanumeric characters.
3. Use **Domain Name** to specify a DNS domain server name. It may be up to 255 alphanumeric characters.
4. Use **DNS Server Address** to specify the IPv6 address of a DNS server.

## DHCPv6 Prefix Delegation Configuration

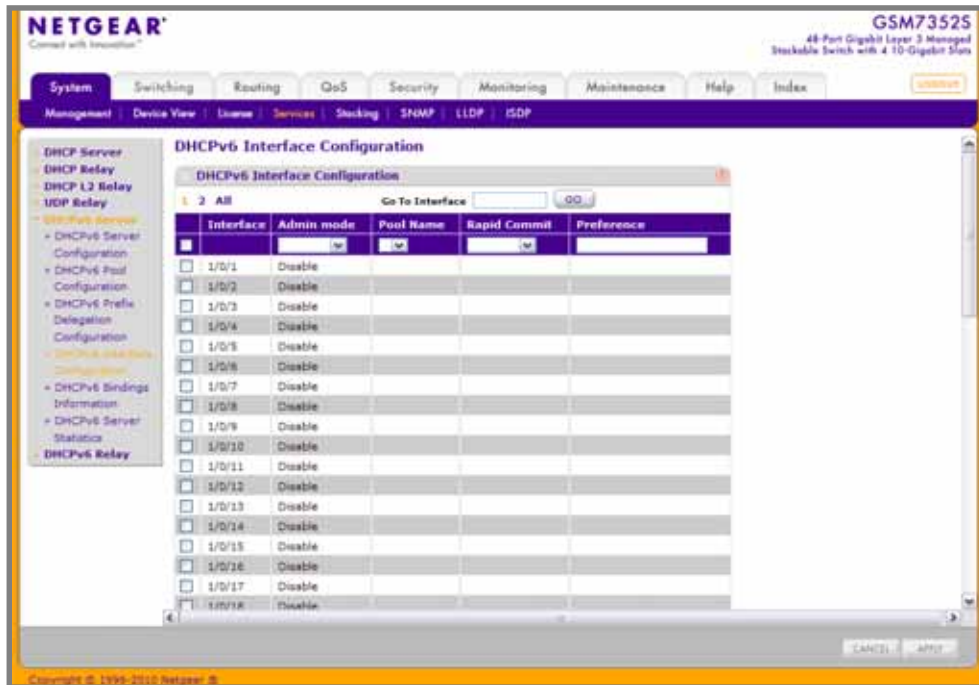
To display the DHCPv6 Prefix Delegation Configuration page, click **System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration**. A screen similar to the following displays.



1. Use **Pool Name** to select one DHCPv6 pool to be configured.
2. Use **Prefix/Prefix Length** to specify the delegated IPv6 prefix.
3. Use **DUID** to identify the client's unique duid value. The format is xx:xx:xx:xx:xx:xx. RFC3315 defines three types:
  - a. Link-layer address plus time:
    - 00:01:hardware type:time:link-layer address
    - hardware type - 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
    - time: 32-bit unsigned integer - The time in seconds when this DUID was generated since 00:00:00 1/1/2000.
    - link-layer address - The link layer address of a device generating the DUID.
  - b. Vendor-assigned unique ID based on Enterprise Number:
    - 00:02:enterprise-number:identifier
    - enterprise-number - 32-bit integer reserved by IANA.
    - identifier - Variable length data for each vendor
  - c. Link-layer address:
    - 00:03:hardware type:link-layer address
    - hardware type - 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
    - link-layer address - The link layer address of a device generating the DUID.
4. Use **Client Name** to specify client's name. This is useful for logging or tracing only. It may be up to 31 alphanumeric characters.
5. Use **Valid Lifetime** to specify the valid lifetime in seconds for delegated prefix.
6. Use **Prefer Lifetime** to specify the prefer lifetime in seconds for delegated prefix.
7. Click **ADD** to add a new delegated prefix for the selected pool.
8. Click **DELETE** to delete the delegated prefix for the selected pool.

## DHCPv6 Interface Configuration

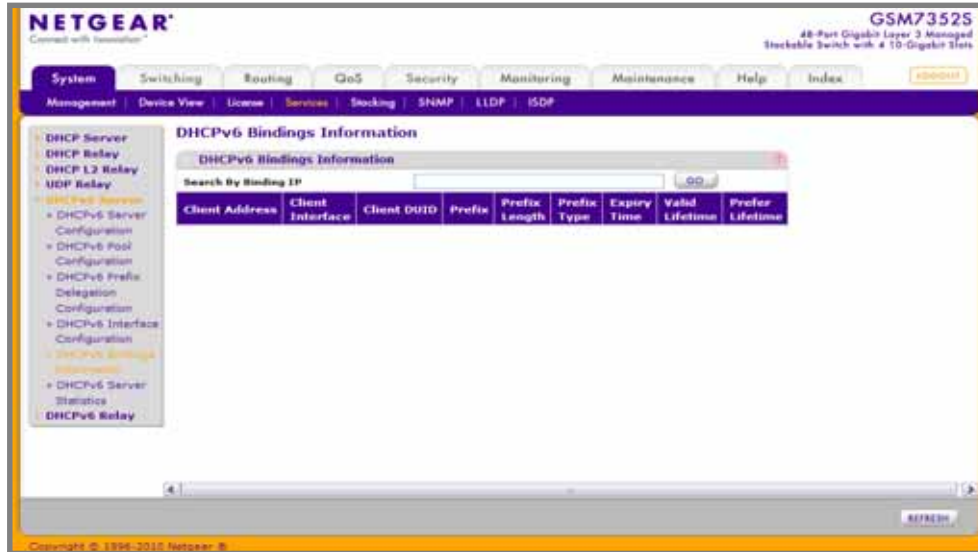
To display the DHCPv6 Prefix Delegation Configuration page, click **System > Services > DHCPv6 Server > DHCPv6 Interface Configuration**. A screen similar to the following displays.



1. Use **Interface** to specify the interface configured for DHCPv6 server functionality.
2. Use **Admin Mode** to specify DHCPv6 mode to configure server functionality. DHCPv6 server and DHCPv6 relay functions are mutually exclusive.
3. Use **Pool Name** to specify the DHCPv6 pool containing stateless and/or prefix delegation parameters.
4. Use the optional **Rapid Commit** parameter to allow abbreviated exchange between the client and server.
5. Use **Preference** to specify the preference value used by clients to determine preference between multiple DHCPv6 servers. The values allowed are between 0 to 4294967295. The default value is 0.

## DHCPv6 Bindings Information

To display the DHCPv6 Bindings Information page, click **System > Services > DHCPv6 Server > DHCPv6 Bindings Information**. A screen similar to the following displays.



The following table describes the DHCPv6 Bindings Information fields.

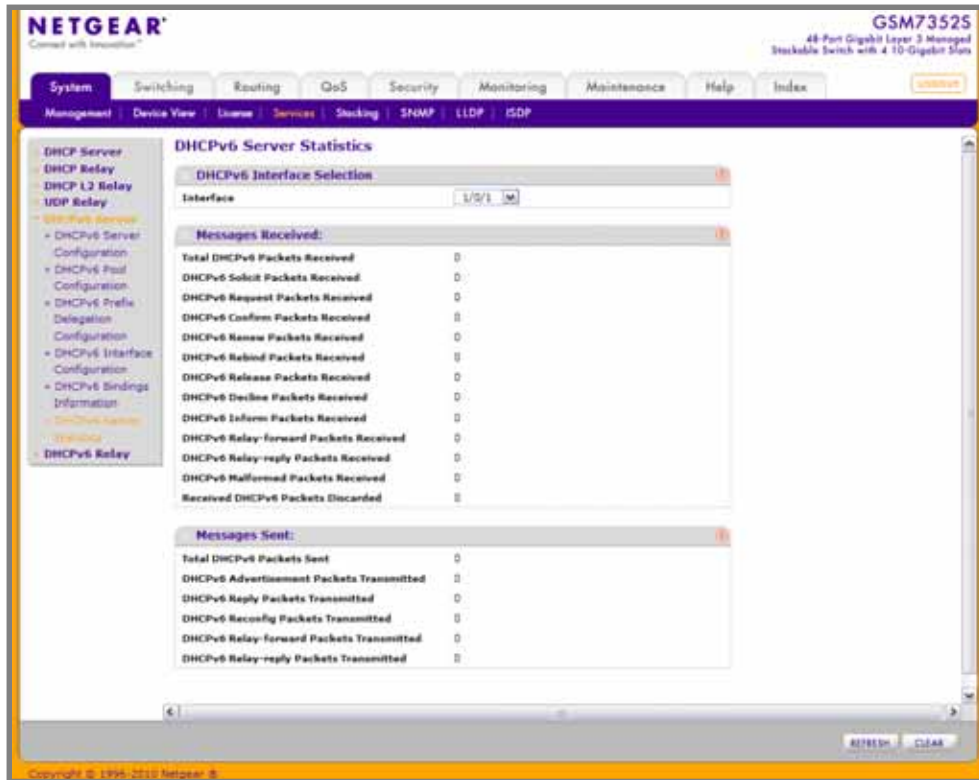
**Table 2-25.**

Field	Description
Client Address	Specifies the IPv6 address of the client associated with the binding.
Client Interface	Specifies the interface number where the client binding occurred.
Client DUID	Specifies client's DHCPv6 unique identifier.
Prefix/PrefixLength	Specifies the IPv6 address and mask length for delegated prefix associated with this binding.
Prefix Type	Specifies the type of prefix associated with this binding.
Expiry Time	Specifies the number of seconds until the prefix associated with a binding will expire.
Valid Lifetime	Specifies the valid lifetime value in seconds of the prefix associated with a binding.
Prefer Lifetime	Specifies the preferred lifetime value in seconds of the prefix associated with a binding.



## DHCPv6 Server Statistics

To display the DHCPv6 Server Statistics page, click **System > Services > DHCPv6 Server > DHCPv6 Server Statistics**. A screen similar to the following displays.



1. Use **Interface** to select the interface for which data is to be displayed or configured. On selecting all, data will be shown for all interfaces.

The following table describes the DHCPv6 Server Statistics fields.

**Table 2-26.**

Field	Description
Messages Received	Specifies the aggregate of all interface level statistics for received messages.
Total DHCPv6 Packets Received	Specifies the total number of Packets Received.
DHCPv6 Solicit Packets Received	Specifies the number of Solicits.
DHCPv6 Request Packets Received	Specifies the number of Requests.
DHCPv6 Confirm Packets Received	Specifies the number of Confirms.
DHCPv6 Renew Packets Received	Specifies the number of Renews.
DHCPv6 Rebind Packets Received	Specifies the number of Rebinds.
DHCPv6 Release Packets Received	Specifies the number of Releases.
DHCPv6 Decline Packets Received	Specifies the number of Declines.
DHCPv6 Inform Packets Received	Specifies the number of Informs.
DHCPv6 Relay-forward Packets Received	Specifies the number of Relay forwards.
DHCPv6 Relay-reply Packets Received	Specifies the number of Relay Replies.
DHCPv6 Malformed Packets Received	Specifies the number of Malformed Packets.
Received DHCPv6 Packets Discarded	Specifies the number of Packets Discarded.
Messages Sent	Specifies the aggregate of all interface level statistics for messages sent.
Total DHCPv6 Packets Sent	Specifies the total number of Packets Transmitted.
DHCPv6 Advertisement Packets Transmitted	Specifies the number of Advertisements.
DHCPv6 Reply Packets Transmitted	Specifies the number of Replies.
DHCPv6 Reconfig Packets Transmitted	Specifies the number of Reconfigurations.
DHCPv6 Relay-forward Packets Transmitted	Specifies the number of Relay forwards.
DHCPv6 Relay-reply Packets Transmitted	Specifies the number of Relay Replies.

## DHCPv6 Relay

To display the DHCPv6 Relay page, click **System > Services > DHCPv6 Relay**. A screen similar to the following displays.

The screenshot shows the Netgear DHCPv6 Relay Configuration page. The page has a sidebar with a tree view containing: DHCP Server, DHCP Relay, DHCP L2 Relay, UDP Relay, DHCPv6 Server, and DHCPv6 Relay (selected). The main content area is titled 'DHCPv6 Relay Configuration'. It features a 'Go To Interface' search bar with a 'GO' button. Below this is a table with the following columns: Interface, Admin Mode, Relay Interface, Destination IP Address, and Remote ID. The table lists 21 interfaces (1/0/1 to 1/0/21). The 'Admin Mode' column is set to 'Disable' for all interfaces. The 'Relay Interface', 'Destination IP Address', and 'Remote ID' columns are empty. At the bottom of the table are 'CANCEL' and 'APPLY' buttons. The page also includes a 'LOGOUT' button in the top right corner.

Interface	Admin Mode	Relay Interface	Destination IP Address	Remote ID
<input type="checkbox"/> 1/0/1	Disable			
<input type="checkbox"/> 1/0/2	Disable			
<input type="checkbox"/> 1/0/3	Disable			
<input type="checkbox"/> 1/0/4	Disable			
<input type="checkbox"/> 1/0/5	Disable			
<input type="checkbox"/> 1/0/6	Disable			
<input type="checkbox"/> 1/0/7	Disable			
<input type="checkbox"/> 1/0/8	Disable			
<input type="checkbox"/> 1/0/9	Disable			
<input type="checkbox"/> 1/0/10	Disable			
<input type="checkbox"/> 1/0/11	Disable			
<input type="checkbox"/> 1/0/12	Disable			
<input type="checkbox"/> 1/0/13	Disable			
<input type="checkbox"/> 1/0/14	Disable			
<input type="checkbox"/> 1/0/15	Disable			
<input type="checkbox"/> 1/0/16	Disable			
<input type="checkbox"/> 1/0/17	Disable			
<input type="checkbox"/> 1/0/18	Disable			
<input type="checkbox"/> 1/0/19	Disable			
<input type="checkbox"/> 1/0/20	Disable			
<input type="checkbox"/> 1/0/21	Disable			

1. Use **Interface** to specify interface configured for DHCPv6 Relay functionality.
2. Use **Admin Mode** to specify DHCPv6 mode to configure DHCPv6 Relay functionality. DHCPv6 server and DHCPv6 relay functions are mutually exclusive.
3. Use **Relay Interface** to specify an interface to reach a relay server.
4. Use **Destination IP Address** to specify an IPv6 Address to reach a relay server.
5. Use **Remote ID** to specify the relay agent information option. Remote ID needs to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user defined string.

## Stacking

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

- [Basic](#) on page 80
- [Advanced](#) on page 83

## Basic

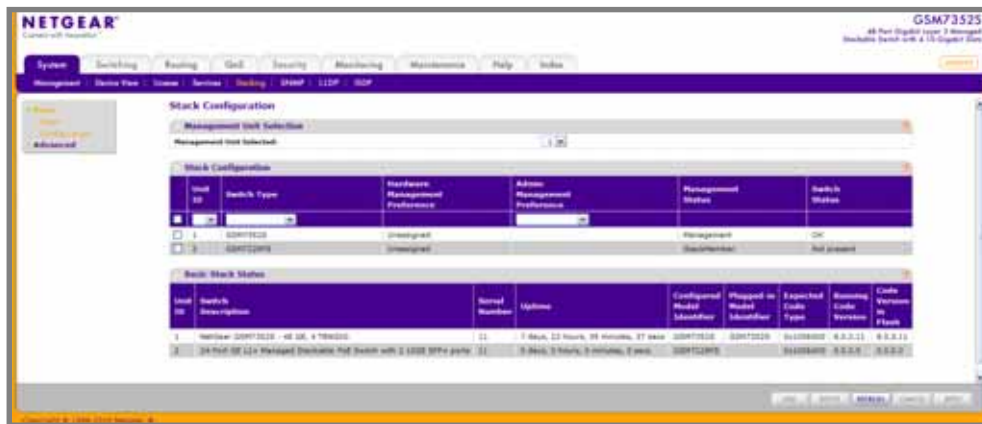
From the Basic link, you can access the following pages:

- [Stack Configuration](#) on page 80

### **Stack Configuration**

This page moves the Primary Management Unit functionality from one unit to another. Upon execution, the entire stack (including all interfaces in the stack) is unconfigured and reconfigured with the configuration on the new Primary Management Unit. After the reload is complete, all stack management capability must be performed on the new Primary Management Unit. To preserve the current configuration across a stack move, save the current configuration to the NVRAM before performing the stack move. 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 displays.



1. Use **Management Unit Selected** to select the unit to be managed unit and click **APPLY** to move the management to the selected unit.
2. **Unit ID** displays the list of units of the stack. Details of the selected unit are displayed. There is also an **ADD** option visible only to Admin users which can be used to pre-configure new members of the stack.
3. Use **Switch Type** to specify the type of switch hardware when creating a new switch in the stack.
4. **Admin Management Preference** is a 2-byte field that indicates whether the administrator wants this unit to become a management unit in preference to another unit. The default value for this setting is one. If the preference level is set to zero then the device cannot become a management unit. This field is non-configurable for users with read-only access.
5. Click **ADD** to add a unit to the stack with the specific switch type.
6. Click **DELETE** to remove the selected unit from the stack.

The following table describes the Stack Configuration fields.

**Table 2-27.**

Field	Description
Hardware Management Preference	The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.
Switch Status	Displays the status of the selected unit. The possible values are: <ul style="list-style-type: none"> <li>• OK</li> <li>• Unsupported</li> <li>• Code Mismatch</li> <li>• Config Mismatch</li> <li>• Not Present</li> </ul>
Management Status	Displays whether the selected switch is the management unit or a normal stacking member or on standby.

The following table describes the Basic Stack Status fields.

**Table 2-28.**

Field	Description
Unit ID	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.
Up Time	Displays the relative time since the last reboot of the switch.
Configured 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.
Running Code Version	This field indicates the detected version of code on this unit.
Code Version in Flash	Displays the Release number and version number of the code stored in flash.

Click **REFRESH** to update the information on the page.

## Advanced

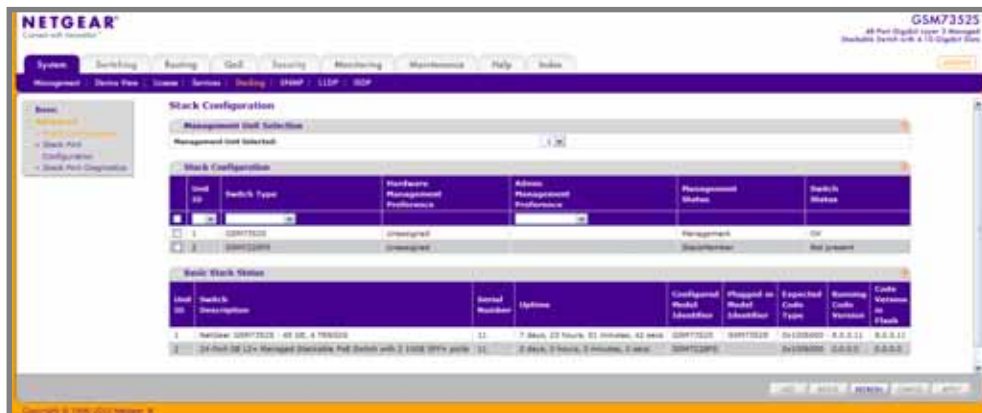
From the Advanced link, you can access the following pages:

- [Stack Configuration](#) on page 80
- [Stack Port Configuration](#) on page 85
- [Stack Port Diagnostics](#) on page 86

### Stack Configuration

This page moves the Primary Management Unit functionality from one unit to another. Upon execution, the entire stack (including all interfaces in the stack) is unconfigured and reconfigured with the configuration on the new Primary Management Unit. After the reload is complete, all stack management capability must be performed on the new Primary Management Unit. To preserve the current configuration across a stack move, please save the current configuration to the nvram before performing the stack move. 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 > Advanced > Stack Configuration**. A screen similar to the following displays.



1. Use **Management Unit Selected** to select the unit to be managed unit and click **APPLY** to move the management to the selected unit.
2. **Unit ID** - Displays the list of units of the stack. Details of the selected unit are displayed. There is also an **ADD** option visible only to Admin users which can be used to pre-configure new members of the stack.
3. Use **Switch Type** to specify the type of switch hardware when creating a new switch in the stack.
4. **Admin Management Preference** is a 2-byte field that indicates whether the administrator wants this unit to become a management unit in preference to another unit. The default value for this setting is one. If the preference level is set to zero then the device cannot become a management unit. This field is non-configurable for users with read-only access.
5. Click **ADD** to add a unit to the stack with the specific switch type.
6. Click **DELETE** to remove the selected unit from the stack.

The following table describes the Stack Configuration fields.

**Table 2-29.**

Field	Description
Hardware Management Preference	The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.
Switch Status	Displays the status of the selected unit. The possible values are: <ul style="list-style-type: none"> <li>• OK</li> <li>• Unsupported</li> <li>• Code Mismatch</li> <li>• Config Mismatch</li> <li>• Not Present</li> </ul>
Management Status	Displays whether the selected switch is the management unit or a normal stacking member or on standby.

### Stack Status

The following table describes the Stack Status fields.

**Table 2-30.**

Field	Description
Unit ID	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.
Up Time	Displays the relative time since the last reboot of the switch.
Configured 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.
Running Code Version	This field indicates the detected version of code on this unit.
Code Version in Flash	Displays the Release number and version number of the code stored in flash.



## Stack Port Configuration

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

Unit ID	Port	Type	XFP/SFP+ Adapter	Configured Stack Mode	Running Stack Mode	Link Status	Link Speed (Gbps)	Transmit Data Rate (Mbps)	Total Transmit Errors	Receive Data Rate (Mbps)	Total
1	S/19	None	None	Stack	Stack	Down	12	0	0	0	0
1	S/20	None	None	Stack	Stack	Down	12	0	0	0	0
1	S/21	AX742	(stack)	Stack	Stack	Down	12	0	0	0	0
1	S/22	None	None	Stack	Stack	Down	12	0	0	0	0

1. **Configured Stack Mode** - Specify the operating mode of the port to be either ethernet or stacking. The default value is set to stacking.

The following table describes Stack Port Configuration fields.

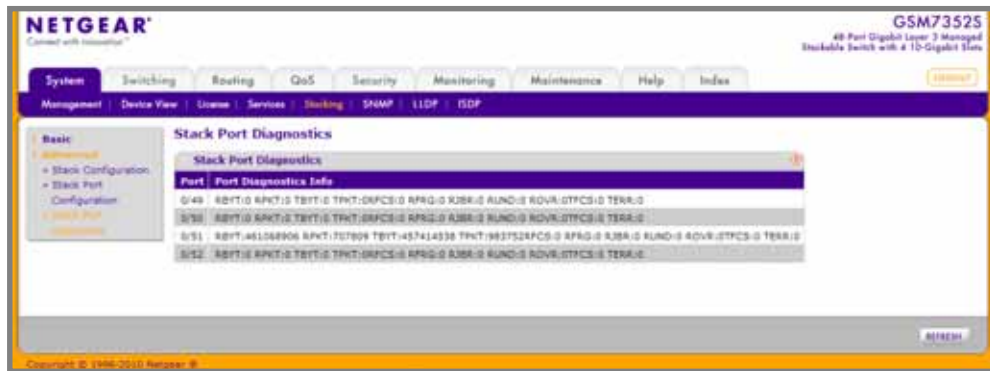
**Table 2-31.**

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.
Total Transmit Errors	Displays the total number of errors in transmit packets since boot. The counter may wrap.
Receive Data Rate (Mbps)	Displays the approximate receive rate on the stacking port.
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 displays.



The following table describes the Stack Port Diagnostics fields.

**Table 2-32.**

Field	Definition
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.

## PoE

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

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

- [Basic](#) on page 86
- [Advanced](#) on page 89

## Basic

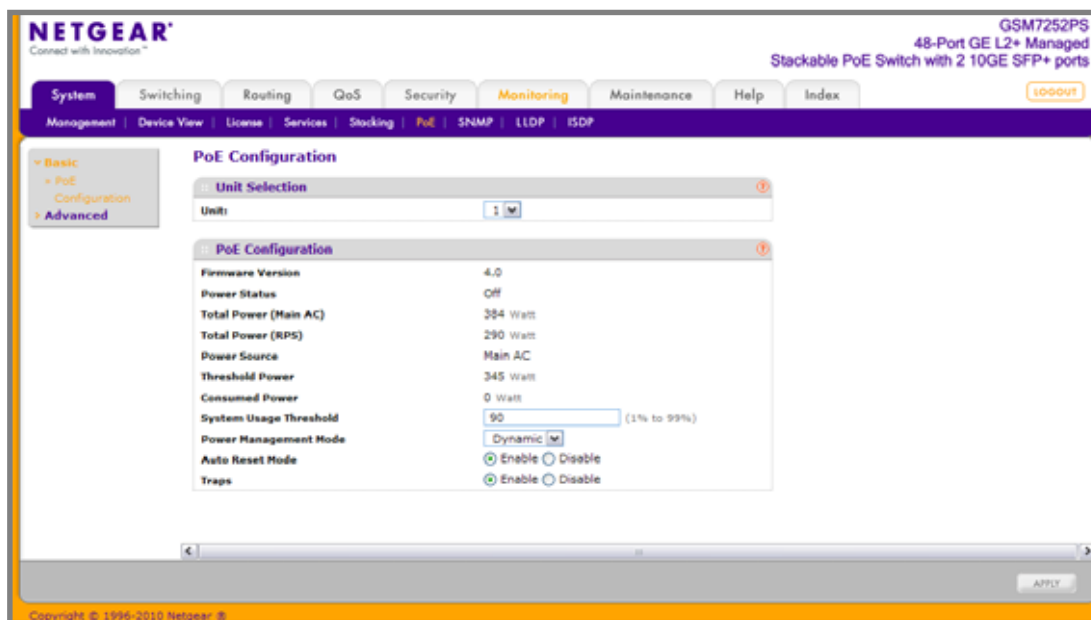
From the Basic link, you can access the following pages:

- [PoE Configuration](#) on page 87

## PoE Configuration

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

To display this page, click **System > PoE > Basic > PoE Configuration**. A screen similar to the following displays.



1. **Unit** - Displays the Current PoE Unit. You can change the PoE Unit by selecting another unit ID listed here.
2. Use **System Usage Threshold** to set a threshold level at which a trap is sent if consumed power is greater than threshold power.
3. Use **Power Management Mode** to describe or control the power management algorithm used by the PSE to deliver power to the requesting PDs. "Static" value means that power allocated for each port depends on the type of power threshold configured on the port. "Dynamic" value means that power consumption of each port is measured and calculated in real-time.
4. Use **Auto Reset Mode** to specify Enable or Disable. When set to "Enable", the PSE port is reset without administrator intervention whenever a fault condition occurs. When set to "Disable", the administrator has to reset the PSE port whenever a fault condition is detected.
5. Use **Traps** to enable or disable activation of PoE traps by selecting the corresponding check box. The factory default is enabled.

**Table 3.**

Field	Definition
Firmware Version	Version of the PoE controller's firmware image.
Power Status	Indicates the power status.

**Table 3.**

Field	Definition
Total Power (Main AC)	Maximum amount of power the system can deliver to all ports when the PoE unit is powered up by Main AC Supply.
Total Power (RPS)	Maximum amount of power the system can deliver to all ports when the PoE unit is powered up by RPS unit.
Power Source	The power source. There are two possible power sources: Main AC or RPS.
Threshold Power	System can powerup one port, if consumed power is less than this power, i.e., Consumed power can be between Nominal and Threshold Power values. The threshold power value is effected by changing System Usage Threshold.
Consumed Power	Total amount of a power which is currently being delivered to all ports.

## Advanced

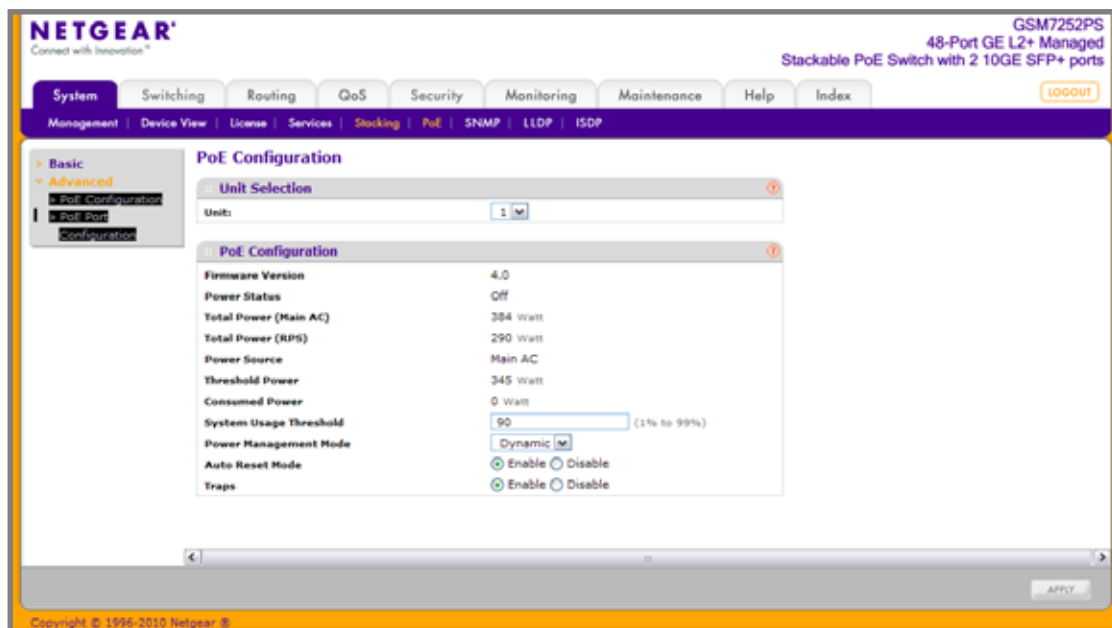
From the Advanced link, you can access the following pages:

- [PoE Configuration](#) on page 89
- [PoE Port Configuration](#) on page 91

### PoE Configuration

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

To display this page, click **System > PoE > Advanced > PoE Configuration**. A screen similar to the following displays.



1. **Unit** - Displays the Current PoE Unit. You can change the PoE Unit by selecting another unit ID listed here.
2. Use **System Usage Threshold** to set a threshold level at which a trap is sent if consumed power is greater than threshold power.
3. Use **Power Management Mode** to describe or control the power management algorithm used by the PSE to deliver power to the requesting PDs. "Static" value means that power allocated for each port depends on the type of power threshold configured on the port. "Dynamic" value means that power consumption of each port is measured and calculated in real-time.
4. Use **Auto Reset Mode** to specify Enable or Disable. When set to "Enable", the PSE port is reset without administrator intervention whenever a fault condition occurs. When set to "Disable", the administrator has to reset the PSE port whenever a fault condition is detected.
5. Use **Traps** to enable or disable activation of PoE traps by selecting the corresponding check box. The factory default is enabled.

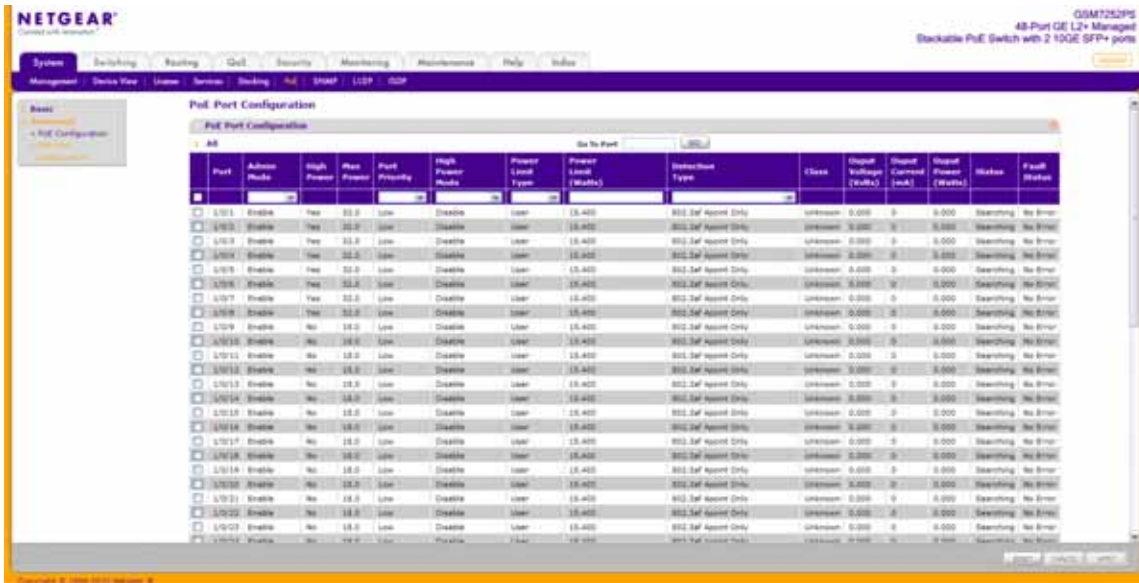
**Table 4.**

Field	Definition
Firmware Version	Version of the PoE controller's firmware image.
Power Status	Indicates the power status.
Total Power (Main AC)	Maximum amount of power the system can deliver to all ports when the PoE unit is powered up by Main AC Supply.
Total Power (RPS)	Maximum amount of power the system can deliver to all ports when the PoE unit is powered up by RPS unit.
Power Source	The power source. There are two possible power sources: Main AC or RPS.
Threshold Power	System can powerup one port, if consumed power is less than this power, i.e., Consumed power can be between Nominal and Threshold Power values. The threshold power value is effected by changing System Usage Threshold.
Consumed Power	Total amount of a power which is currently being delivered to all ports.

## PoE Port Configuration

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

To display this page, click **System > PoE > Advanced > PoE Port Configuration**. A screen similar to the following displays.



1. **Unit** - Displays the Current PoE Unit. You can change the PoE Unit by selecting another unit ID listed here.
2. Use **Admin Mode** to enable/disable the ability of the port to deliver a power.
3. Use **Port Priority** to determine which ports can deliver power when total power delivered by the system crosses a certain threshold. The switch may not be able to supply a power to all connected devices. Priority is used to determine which ports can supply power. The lower numbered port which is one of the ports of the same priority will have a higher priority.
  - low - Low priority.
  - high - High priority.
  - critical - Critical priority.
4. Use **High Power Mode** to specify one of the following:
  - **Disable** value means that a port is powered in the IEEE 802.3af mode.
  - **Legacy** value means that a port is powered using high-inrush current, used by legacy PDs whose power requirement is more than 15W from powerup.
  - **Pre-802.3at** value means that a port is powered in the IEEE 802.3af mode initially, switched to the high-power IEEE 802.3at mode before 75msec. This mode needs to be used, if PD is NOT performing Layer 2 Classification Or PSE is performing 2-Event Layer 1 Classification.
  - **802.3at** value means that a port is powered in the IEEE 802.3at mode, i.e., if class detected by PSE is not the class4, then the PSE port will not power up the PD.

5. Use **Power Limit Type** to describe or control the maximum power that a port can deliver. "Dot3AF" value means that the port power limit is equal to the dot3af class of the PD attached. "User" value means that the port power limit is equal to the value specified by "Power Limit". "None" value means that there is no power provided to the port.
6. Use **Power Limit** to define the maximum power which can be delivered by a port.
7. Use **Detection Type** to describe a PD detection mechanism performed by the PSE port:
  - **None** value means that no detection is done.
  - **Legacy Only** value means that only legacy capacitive detection scheme is used.
  - **802.3af 4point Only** value means that the IEEE 802.3af 4point detection scheme is used.
  - **802.3af 4point and Legacy** value means that the IEEE 802.3af 4point detection scheme is used and when it fails to detect a connected PD, legacy capacity detection is used.
  - **802.3af 2point Only** value means that the IEEE 802.3af 2point detection scheme is used.
  - **802.3af 2point and Legacy** value means that the IEEE 802.3af 2point detection scheme is used and when it fails to detect a connected PD, legacy capacity detection is used.
8. Click **RESET** to forcibly reset the PSE port.

Table 5.

Field	Definition
Port	The interface for which data is to be displayed or configured.
High Power	Enabled when particular port supports High Power Mode.
Max Power	The maximum power in Watts that can be provided by the port.
Class	The class of the Powered Device (PD) defines the range of power a PD is drawing from the system. Class definitions: <ul style="list-style-type: none"> <li>• 0 - 0.44-12.95(watts)</li> <li>• 1 - 0.44-3.83(watts)</li> <li>• 2 - 0.44-6.48(watts)</li> <li>• 3 - 0.44-12.95(watts)</li> <li>• 4 - 0.44-25.5(watts)</li> </ul>
Output Voltage	Current voltage being delivered to device in volts.
Output Current	Current being delivered to device in mA.
Output Power	Current power being delivered to device in Watts.



Table 5.

Field	Definition
Status	Operational status of the port PD detection. <ul style="list-style-type: none"> <li>• Disabled - indicates no power being delivered.</li> <li>• DeliveringPower - indicates power is being drawn by device.</li> <li>• Fault - indicates a problem with the port.</li> <li>• Test - indicates port is in test mode.</li> <li>• otherFault - indicates port is idle due to error condition.</li> <li>• Searching - indicates port is not in one of the above states.</li> </ul>
Fault Status	Describes the error description when the PSE port is in fault status. "No Error" value specifies that the PSE port is not in any error state. "MPS Absent" value specifies that the PSE port has detected an absence of main power supply. "Short" value specifies that the PSE port has detected a short circuit condition. "Overload" value specifies that the pd connected to the PSE port had tried to provide more power than it is permissible by the hardware. "Power Denied" value specifies that the PSE port has been denied power because of shortage of power or due to administrative action.

## SNMP

From SNMP link under the System tab, you can configure SNMP settings for SNMP V1/V2 and SNMPv3.

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

- [SNMPV1/V2](#) on page 93
- [SNMP V3](#) on page 101

### SNMPV1/V2

The pages under the SNMPV1/V2 menu allow you to configure SNMP community information, traps, and trap flags.

From the SNMP V1/V2 link, you can access the following pages:

- [Community Configuration](#) on page 94
- [Trap Configuration](#) on page 96
- [Trap Flags](#) on page 97
- [Supported MIBs](#) on page 99

## Community Configuration

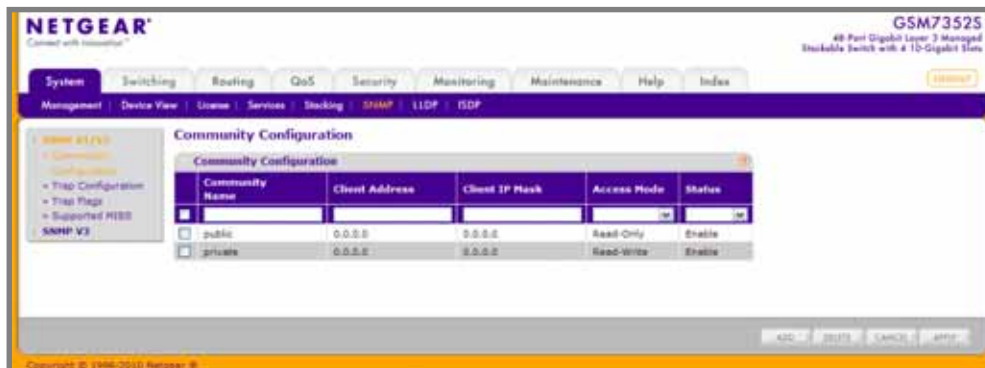
By default, two SNMP Communities exist:

- 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. If you want to use SNMP v3 you should use the User Accounts menu.

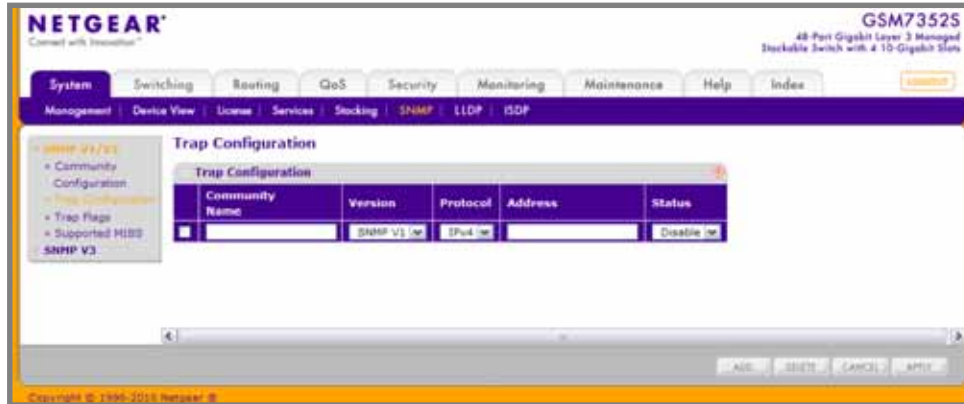
To display this page, click **System > SNMP > SNMP V1/V2 > Community Configuration**. A screen similar to the following displays.



1. Use **Community Name** to reconfigure an existing community, or to create a new one. Use this pull-down menu to select one of the existing community names, or select 'Create' to add a new one. A valid entry is a case-sensitive string of up to 16 characters.
2. **Client Address** - Taken together, the Client Address and Client IP Mask denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (Client Address or 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 Client Address, and, if the values are equal, access is allowed. For example, if the Client Address and Client 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 Client IP Mask value of 255.255.255.255, and use that machine's IP address for Client Address.
3. **Client IP Mask** - Taken together, the Client Address and Client IP Mask denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (Client Address or 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 Client Address, and, if the values are equal, access is allowed. For example, if the Client Address and Client IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose IP address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Client IP Mask value of 255.255.255.255, and use that machine's IP address for Client Address.
4. Use **Access Mode** to specify the access level for this community by selecting Read/Write or Read Only from the pull-down menu.
5. Use **Status** to 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.
6. Click **ADD** to add the currently selected community to the switch.
7. Click **DELETE** to delete the currently selected Community Name.

## Trap Configuration

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



1. To add a host that will receive SNMP traps, enter trap configuration information in the available fields described below, and then click **Add**.
  - a. **Community Name** - Enter the community string for the SNMP trap packet to be sent to the trap manager. This may be up to 16 characters and is case sensitive.
  - b. **Version** - Select the trap version to be used by the receiver from the pull down menu:
    - **SNMP v1** - Uses SNMP v1 to send traps to the receiver.
    - **SNMP v2** - Uses SNMP v2 to send traps to the receiver.
  - c. **Protocol** - Select the protocol to be used by the receiver from the pull down menu. Select the IPv4 if the receiver's address is IPv4 address or IPv6 if the receiver's address is IPv6.
  - d. **Address** - Enter the IPv4 address in x.x.x.x format or IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx or a hostname starting with an alphabet to receive SNMP traps from this device. Length of address can not exceed 158 characters.
  - e. **Status** - Select the receiver's status from the pull-down menu:
    - **Enable** - Send traps to the receiver
    - **Disable** - Do not send traps to the receiver.
2. 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.
3. To delete a recipient, select the check box next to the recipient 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 Flags

Use the Trap Flags page to enable or disable traps. 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**.

**Trap Flags**

Authentication	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Link Up/Down	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Multiple Users	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Spanning Tree	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ACL	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Captive Portal	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
DVHRP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
PIM	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>OSPFv2 Traps:</b>	
errors:	
authentication-failure	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
bad-packet	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
config-error	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-authentication-failure	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-bad-packet	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-config-error	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
lsa:	
lsa-maxage	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
lsa-originate	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
overflow:	
lsdb-overflow	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
lsdb-approaching-overflow	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
retransmit:	
packets	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-packets	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
state-change:	
if-state-change	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
neighbor-state-change	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virtif-state-change	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virtneighbor-state-change	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>OSPFv3 Traps:</b>	
errors:	
bad-packet	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
config-error	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-bad-packet	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-config-error	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
lsa:	
lsa-maxage	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
lsa-originate	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
overflow:	
lsdb-overflow	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
lsdb-approaching-overflow	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
retransmit:	
packets	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-packets	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
state-change:	
if-state-change	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
neighbor-state-change	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virtif-state-change	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virtneighbor-state-change	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

To configure the trap flags:

1. Use **Authentication** to enable or disable activation of authentication failure traps by selecting the corresponding radio button. The factory default is enabled.
2. Use **Link Up/Down** to enable or disable activation of link status traps by selecting the corresponding radio button. The factory default is enabled.
3. Use **Multiple Users** to enable or disable activation of multiple user traps by selecting the corresponding radio button. The factory default is enabled. This trap is triggered when the same user ID is logged into the switch more than once at the same time (either via telnet or the serial port).
4. Use **Spanning Tree** to enable or disable activation of spanning tree traps by selecting the corresponding radio button. The factory default is enabled.
5. Use **ACL** to enable or disable activation of ACL traps by selecting the corresponding radio button. The factory default is disabled.
6. Use **DVMRP** to enable or disable activation of DVMRP traps by selecting the corresponding radio button. The factory default is disabled.
7. Use **PIM** to enable or disable activation of spanning tree traps by selecting the corresponding radio button. The factory default is disabled.
8. Use **OSPF** to enable or disable activation of OSPF traps by selecting the corresponding radio button. The factory default is enabled. This field can be configured only if the OSPF admin mode is enabled.
9. Click **CANCEL** to cancel the configuration on the screen. Resets the data on the screen to the latest value of the switch.
10. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

## Supported MIBs

This page displays all the MIBs supported by the switch. To access this page, click **System > SNMP > SNMP V1/V2 > Supported MIBs**.

SNMP Supported MIBs	
Status	
Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
NETGEAR-REF-MIB	Netgear Reference
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-FRAMEWORK-MIB	The SNMP Management Architecture MIB
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-NOTIFICATION-MIB	The Notification MIB Module
SNMP-TARGET-MIB	The Target MIB Module
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
USM-TARGET-TAG-MIB	SNMP Research, Inc.
FASTPATH-POWER-ETHERNET-MIB	Fastpath Power Ethernet Extensions MIB
POWER-ETHERNET-MIB	Power Ethernet MIB
SFLOW-MIB	sFlow MIB
FASTPATH-ISDP-MIB	Industry Standard Discovery Protocol MIB
LAG-MIB	The Link Aggregation module for managing IEEE 802.3ad
RFC 1213 - RFC1213-MIB	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1493 - BRIDGE-MIB	Definitions of Managed Objects for Bridges (dot1d)
RFC 2674 - P-BRIDGE-MIB	The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998.
RFC 2674 - Q-BRIDGE-MIB	The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks
RFC 2737 - ENTITY-MIB	Entity MIB (Version 2)
RFC 2863 - IF-MIB	The Interfaces Group MIB using SMIV2
RFC 3635 - Etherlike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types
FASTPATH-SWITCHING-MIB	FASTPATH Switching - Layer 2
FASTPATH-INVENTORY-MIB	Unit and Slot configuration.
FASTPATH-PORTSECURITY-PRIVATE-MIB	Port Security MIB.
IEEE Draft P802.1AB/D13	LLDP basic MIB
IEEE8021-PAE-MIB	Port Access Entity module for managing IEEE 802.1X.
FASTPATH-RADIUS-AUTH-CLIENT-MIB	Netgear FastPath Radius MIB
RADIUS-ACC-CLIENT-MIB	RADIUS Accounting Client MIB
RADIUS-AUTH-CLIENT-MIB	RADIUS Authentication Client MIB
FASTPATH-CAPTIVE-PORTAL-MIB	FastPath Captive Portal MIB
FASTPATH-MGMT-SECURITY-MIB	Netgear Private MIB for FastPath Mgmt Security
IANA-ADDRESS-FAMILY-NUMBERS-MIB	The MIB module defines the AddressFamilyNumbers textual convention.
RFC 1724 - RIPv2-MIB	RIP Version 2 MIB Extension
RFC 1850 - OSPF-MIB	OSPF Version 2 Management Information Base
RFC 1850 - OSPF-TRAP-MIB	The MIB module to describe traps for the OSPF Version 2 Protocol.
RFC 2787 - VRRP-MIB	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
FASTPATH-ROUTING-MIB	FASTPATH Routing - Layer 3
FASTPATH-QOS-MIB	FASTPATH Flex QOS Support
FASTPATH-QOS-ACL-MIB	FASTPATH Flex QOS ACL
FASTPATH-QOS-COS-MIB	FASTPATH Flex QOS COS
FASTPATH-QOS-AUTOVOIP-MIB	FASTPATH Flex QOS VOIP
RFC 3289 - DIFFSERV-DSCP-TC	Management Information Base for the Textual Conventions used in DIFFSERV-MIB
RFC 3289 - DIFFSERV-MIB	Management Information Base for the Differentiated Services Architecture
FASTPATH-QOS-DIFFSERV-EXTENSIONS-MIB	FASTPATH Flex QOS DiffServ Private MIBs' definitions
FASTPATH-QOS-DIFFSERV-PRIVATE-MIB	FASTPATH Flex QOS DiffServ Private MIBs' definitions
RFC 2932 - IPMRROUTE-MIB	IPv4 Multicast Routing MIB
draft-ietf-magma-mgmd-mib-03	MGMD MIB, includes IGMIPv3 and MLDv2.
RFC 2934 - PIM-MIB	Protocol Independent Multicast MIB for IPv4
DVMRP-STD-MIB	Distance-Vector Multicast Routing Protocol MIB
IANA-RTPROTO-MIB	IANA IP Route Protocol and IP MRoute Protocol Textual Conventions
RFC 2465 - IPV6-MIB	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC 2466 - IPV6-ICMP-MIB	Management Information Base for IP Version 6: ICMPv6 Group
RFC 3419 - TRANSPORT-ADDRESS-MIB	Textual Conventions for Transport Addresses
FASTPATH-ROUTING6-MIB	Netgear Private MIB for FastPath Ipv6 Routing

The following table describes the SNMP Supported MIBs Status fields.

**Table 2-33.**

Field	Description
Name	The RFC number if applicable and the name of the MIB.
Description	The RFC title or MIB description.



## SNMP V3

This is the configuration for SNMP v3.

From the SNMP V3 link, you can access the following pages:

- [User Configuration](#) on page 101

### User Configuration

To access this page, click **System** > **SNMP** > **SNMP V3** > **User Configuration**. A screen similar to the following displays.

The screenshot displays the Netgear web management interface for a GSM7352S switch. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Below this, a secondary bar shows Management, Device View, License, Services, Stacking, SNMP, LLDP, and ISDP. The left sidebar shows a tree view with 'SNMP V1/V2' expanded, and 'SNMP V3' > 'User Configuration' selected. The main content area is titled 'User Configuration' and contains two sections: 'User Names' with a text field for 'User Name' containing 'admin', and 'User Configuration' with a dropdown for 'SNMP v3 Access Mode' set to 'Read/Write', and radio buttons for 'Authentication Protocol' (None selected, MDS, SHA) and 'Encryption Protocol' (None selected, DES). At the bottom right are 'CANCEL' and 'APPLY' buttons. The footer shows 'Copyright © 1996-2010 Netgear, Inc.'

To configure SNMPv3 settings for the user account:

1. Use **User Name** to specify the user account to be configured.
2. **SNMP v3 Access Mode** - Indicates the SNMPv3 access privileges for the user account. The admin account always has 'Read/Write' access, and all other accounts have 'Read Only' access.
3. Use **Authentication Protocol** to 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.
  - If you select **MD5** or **SHA**, the user login password will be used as the SNMPv3 authentication password, and you must therefore specify a password, and it must be eight characters long.
4. Use **Encryption Protocol** to specify the SNMPv3 Encryption Protocol setting for the selected user account. The valid Encryption Protocols are None or DES:
  - If you select the DES Protocol you must enter a key in the **Encryption Key** field.
  - If **None** is specified for the Protocol, the Encryption Key is ignored.
5. **Encryption Key** - If you selected **DES** in the **Encryption Protocol** field enter the SNMPv3 Encryption Key here, otherwise, this field is ignored. Valid keys are 0 to 15 characters long. The Apply checkbox must be checked in order to change the Encryption Protocol and Encryption Key.
6. Click **CANCEL** to cancel the configuration on the screen. Resets the data on the screen to the latest value of the switch.
7. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

## LLDP

The IEEE 802.1AB-defined standard, Link Layer Discovery Protocol (LLDP), allows stations 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](#) on page 103
- [LLDP-MED](#) on page 113

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

The 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

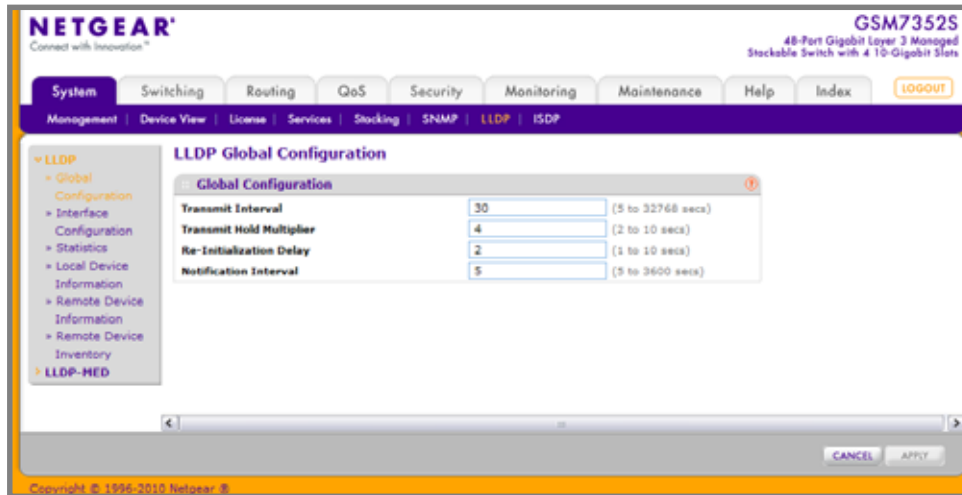
From the LLDP link, you can access the following pages:

- [\*LLDP Global Configuration\*](#) on page 104
- [\*LLDP Interface Configuration\*](#) on page 105
- [\*LLDP Statistics\*](#) on page 106
- [\*LLDP Local Device Information\*](#) on page 108
- [\*LLDP Remote Device Information\*](#) on page 110
- [\*LLDP Remote Device Inventory\*](#) on page 112

## LLDP Global Configuration

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

To display this page, click **System > LLDP > LLDP > Global Configuration**. A screen similar to the following displays.

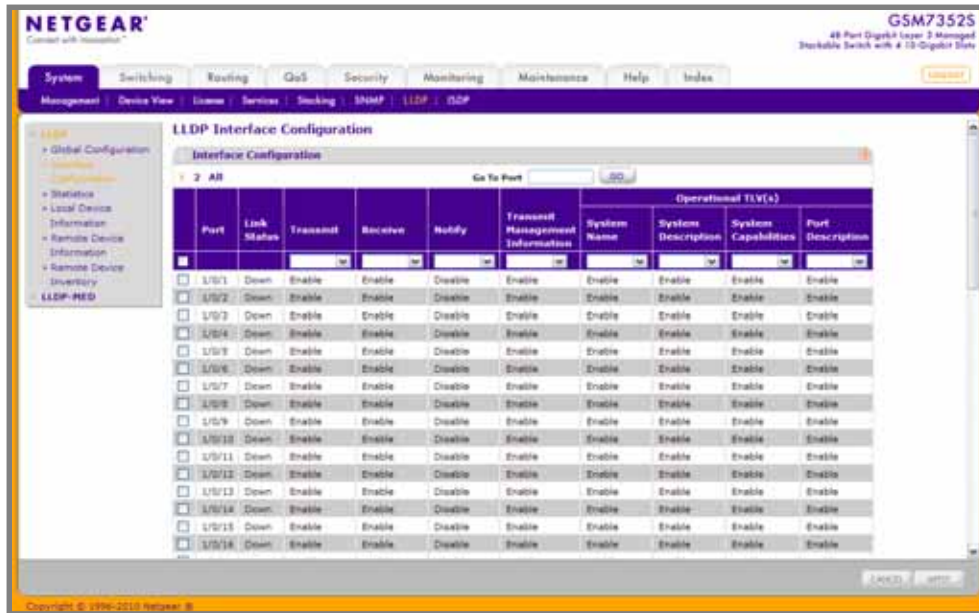


To configure global LLDP settings:

1. Use **Transmit Interval** to specify the interval in seconds to transmit LLDP frames. The range is from 5 to 32768 secs. Default value is 30 seconds.
2. Use **Transmit Hold Multiplier** to specify the multiplier on Transmit Interval to assign TTL. The range is from 2 to 10 secs. Default value is 4.
3. Use **Re-Initialization Delay** to specify the delay before re-initialization. The range is from 1 to 10 secs. Default value is 2 seconds.
4. Use **Notification Interval** to specify the interval in seconds for transmission of notifications. The range is from 5 to 3600 secs. Default value is 5 seconds.
5. Click **CANCEL** to cancel the configuration on the screen. Resets the data on the screen to the latest value of the switch.
6. Click **APPLY** to send the updated configuration to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.

## LLDP Interface Configuration

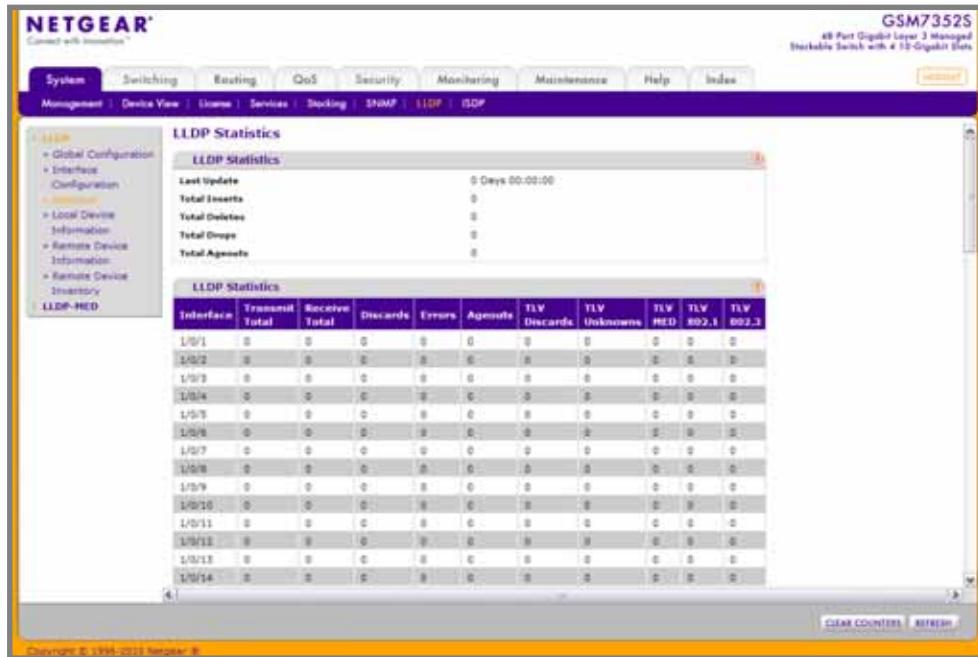
To display this page, click **System > LLDP > LLDP > Interface Configuration**. A screen similar to the following displays.



1. Use **Port** to specify the list of ports on which LLDP - 802.1AB can be configured.
2. **Link Status** indicates whether the Link is up or down.
3. Use **Transmit** to specify the LLDP - 802.1AB transmit mode for the selected interface.
4. Use **Receive** to specify the LLDP - 802.1AB receive mode for the selected interface.
5. Use **Notify** to specify the LLDP - 802.1AB notification mode for the selected interface.
6. Use **Transmit Management Information** to specify whether management address is transmitted in LLDP frames for the selected interface.
7. Optional TLV(s):
  - Use **System Name** to include system name TLV in LLDP frames.
  - Use **System Description** to include system description TLV in LLDP frames.
  - Use **System Capabilities** to include system capability TLV in LLDP frames.
  - Use **Port Description** to include port description TLV in LLDP frames.

## LLDP Statistics

To display this page, click **System > LLDP > LLDP > Statistics**. A screen similar to the following displays.



The following table describes the LLDP Statistics fields.

**Table 2-34.**

Field	Description
Last Update	Specifies the time when an entry was created, modified or deleted in the tables associated with the remote system.
Total Inserts	Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Total Deletes	Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with the remote systems.
Total Drops	Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) could not be entered into tables associated with the remote systems because of insufficient resources.

Table 2-34.

Field	Description
Total Age outs	Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with the remote systems because the information timeliness interval has expired.
Interface	Specifies the unit/slot/port for the interfaces.
Transmit Total	Specifies the number of LLDP frames transmitted by the LLDP agent on the corresponding port.
Receive Total	Specifies the number of valid LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
Discards	Specifies the number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.
Errors	Specifies the number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Age outs	Specifies the number of age-outs that occurred on a given port. An age-out is the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with the remote entries because information timeliness interval had expired.
TLV Discards	Specifies the number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.
TLV Unknowns	Specifies the number of LLDP TLVs received on the local ports which were not recognized by the LLDP agent on the corresponding port.
TLV MED	Specifies the total number of LLDP-MED TLVs received on the local ports.
TLV 802.1	Specifies the total number of LLDP TLVs received on the local ports which are of type 802.1.
TLV 802.3	Specifies the total number of LLDP TLVs received on the local ports which are of type 802.3.

## LLDP Local Device Information

To display this page, click **System > LLDP > LLDP > Local Device Information**. A screen similar to the following displays.

The screenshot shows the NetGear web interface for a GSM7352S switch. The navigation menu on the left includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The main content area is titled 'LLDP Local Device Information'. It contains two sections: 'LLDP Interface Selection' and 'Local Device Information'.

**LLDP Interface Selection**

Interface:

**Local Device Information**

Chassis ID Subtype	MAC Address
Chassis ID	00:09:08:07:06:05
Port ID Subtype	Local
Port ID	1/0/1
System Name	
System Description	GSM7352S - NetGear GSM7352S - 48 GE, 4 TENGIG
Port Description	
System Capabilities Supported	bridge, router
System Capabilities Enabled	bridge
Management Address	10.27.7.74
Management Address Type	IPv4

At the bottom of the page, there is a 'REFRESH' button and a copyright notice: 'Copyright © 1999-2010 Netgear'.

1. Use **Interface** to specify the list of all the ports on which LLDP - 802.1AB frames can be transmitted.



The following table describes the LLDP Local Device Information fields.

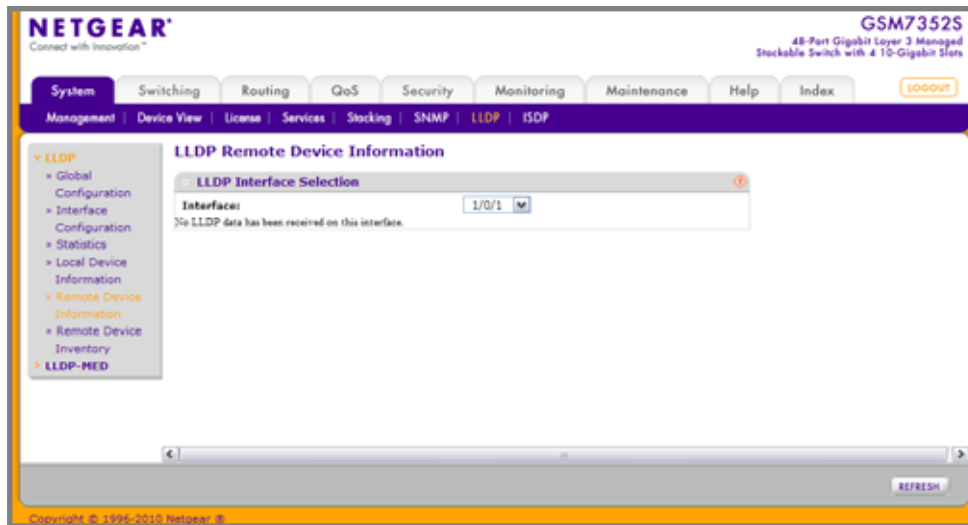
**Table 2-35.**

Field	Description
Chassis ID Subtype	Specifies the string that describes the source of the chassis identifier.
Chassis ID	Specifies the string value used to identify the chassis component associated with the local system.
Port ID Subtype	Specifies the string describes the source of the port identifier.
Port ID	Specifies the string that describes the source of the port identifier.
System Name	Specifies the system name of the local system.
System Description	Specifies the description of the selected port associated with the local system.
Port Description	Specifies the description of the selected port associated with the local system.
System Capabilities Supported	Specifies the system capabilities of the local system.
System Capabilities Enabled	Specifies the system capabilities of the local system which are supported and enabled.
Management Address	Specifies the advertised management address of the local system.
Management Address Type	Specifies the type of the management address.

## LLDP Remote Device Information

This page displays information on remote devices connected to the port.

To display this page, click **System > LLDP > LLDP > Remote Device Information**. A screen similar to the following displays.



1. Use **Interface** to select the local ports which can receive LLDP frames.

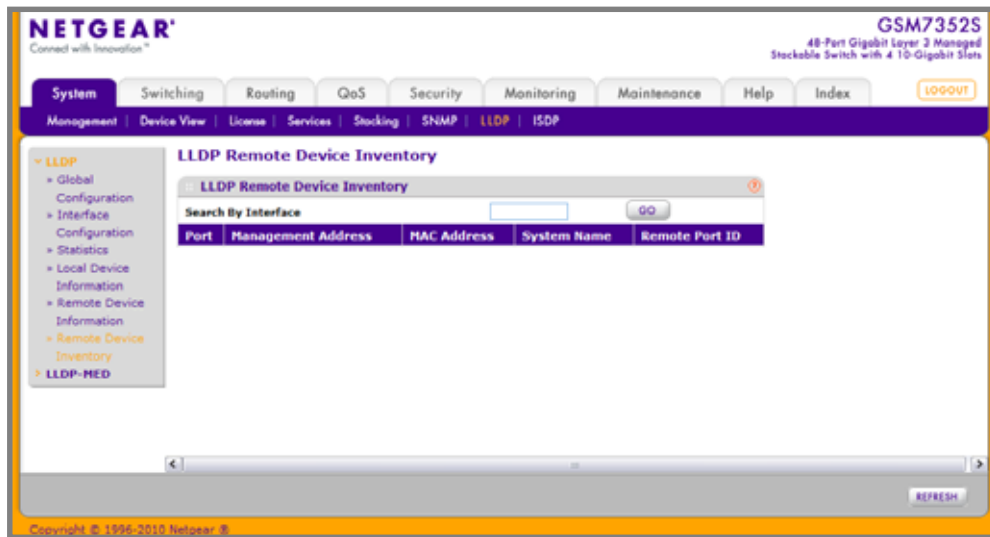
The following table describes the LLDP Remote Device Information fields.

**Table 2-36.**

Field	Description
Chassis ID Subtype	Specifies the source of the chassis identifier.
Chassis ID	Specifies the chassis component associated with the remote system.
Port ID Subtype	Specifies the source of port identifier.
Port ID	Specifies the port component associated with the remote system.
System Name	Specifies the system name of the remote system.
System Description	Specifies the description of the given port associated with the remote system.
Port Description	Specifies the description of the given port associated with the remote system.
System Capabilities Supported	Specifies the system capabilities of the remote system.
System Capabilities Enabled	Specifies the system capabilities of the remote system which are supported and enabled.
Time to Live	Specifies the Time To Live value in seconds of the received remote entry.
Management Address	<ul style="list-style-type: none"><li>• Management Address - Specifies the advertised management address of the remote system.</li><li>• Type - Specifies the type of the management address.</li></ul>

## LLDP Remote Device Inventory

To display this page, click **System > LLDP > LLDP > Remote Device Inventory**. A screen similar to the following displays.



The following table describes the LLDP Remote Device Inventory fields.

**Table 2-37.**

Field	Description
Port	Specifies the list of all the ports on which LLDP frame is enabled.
Management Address	Specifies the advertised management address of the remote system.
MAC Address	Specifies the MAC Address associated with the remote system.
System Name	Specifies model name of the remote device.
Remote Port ID	Specifies the port component associated with the remote system.

## LLDP-MED

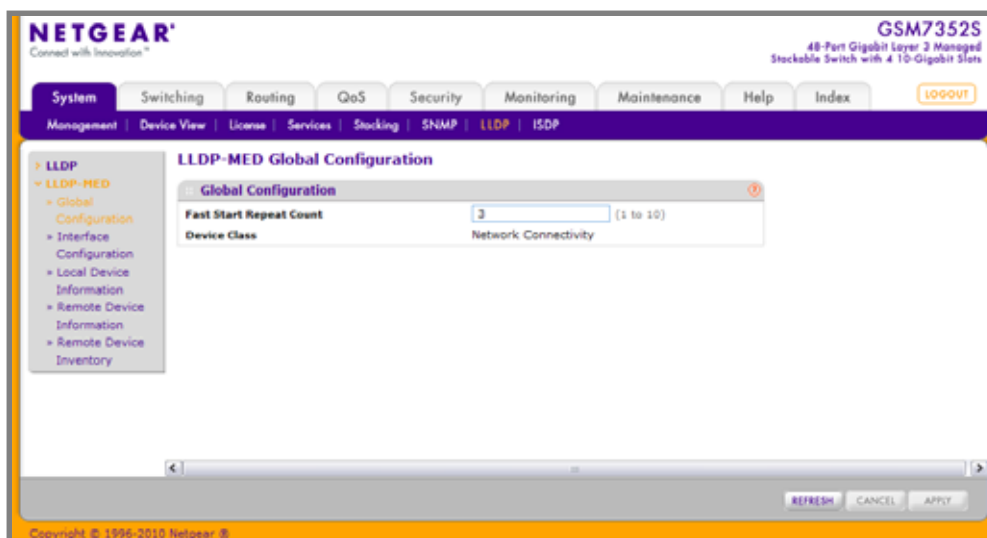
From the LLDP-MED link, you can access the following pages:

- [LLDP-MED Global Configuration](#) on page 113
- [LLDP-MED Interface Configuration](#) on page 115
- [LLDP-MED Local Device Information](#) on page 116
- [LLDP-MED Remote Device Information](#) on page 118
- [LLDP-MED Remote Device Inventory](#) on page 121

### LLDP-MED Global Configuration

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

To display this page, click **System > LLDP > LLDP-MED > Global Configuration**. A screen similar to the following displays.



1. Use **Fast Start Repeat Count** to specify the number of LLDP PDUs that will be transmitted when the protocol is enabled. The range is from (1 to 10). Default value of fast repeat count is 3.

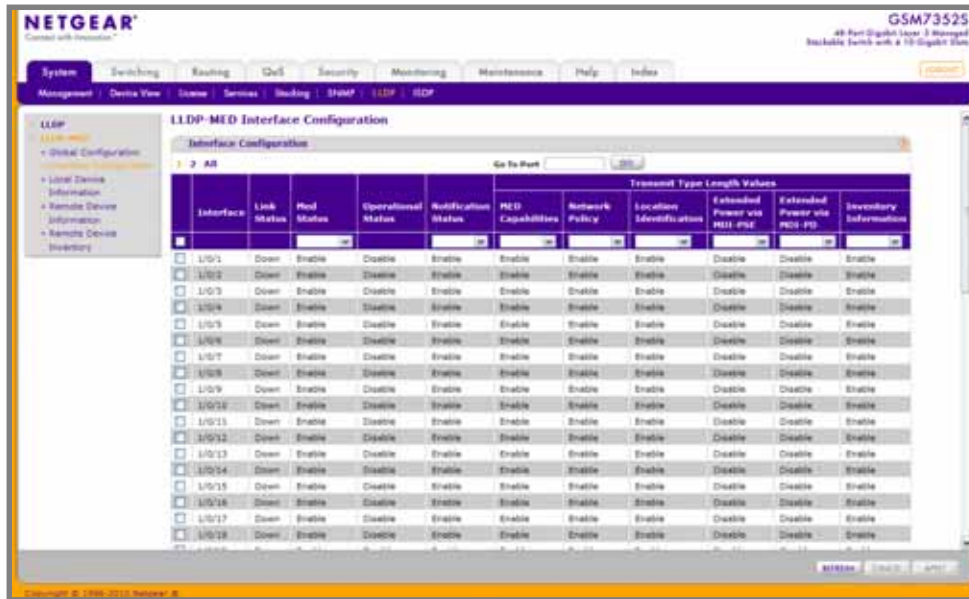
The following table describes the LLDP-MED Global Configuration fields.

**Table 2-38.**

Field	Description
<b>Device Class</b>	Specifies local device's MED Classification. There are four different kinds of devices, three of them represent the actual end points (classified as Class I Generic [IP Communication Controller etc.], Class II Media [Conference Bridge etc.], Class III Communication [IP Telephone etc.]). The fourth device is Network Connectivity Device, which is typically a LAN Switch/Router, IEEE 802.1 Bridge, IEEE 802.11 Wireless Access Point etc.

## LLDP-MED Interface Configuration

To display this page, click **System > LLDP > LLDP-MED > Interface Configuration**. A screen similar to the following displays.



1. Use **Interface** to specify the list of ports on which LLDP-MED - 802.1AB can be configured.
2. Use **MED Status** to specify whether LLDP-MED mode is enabled or disabled on this interface.
3. Use **Notification Status** to specify the LLDP-MED topology notification mode of the interface.
4. Use **Transmit Type Length Values** to specify which optional type length values (TLVs) in the LLDP-MED will be transmitted in the LLDP PDUs frames for the selected interface:
  - **MED Capabilities** - To transmit the capabilities TLV in LLDP frames.
  - **Network Policy** - To transmit the network policy TLV in LLDP frames.
  - **Location Identification** - To transmit the location TLV in LLDP frames.
  - **Extended Power via MDI - PSE** - To transmit the extended PSE TLV in LLDP frames.
  - **Extended Power via MDI - PD** - To transmit the extended PD TLV in LLDP frames.
  - **Inventory Information** - To transmit the inventory TLV in LLDP frames.

The following table describes the LLDP-MED Interface Configuration fields.

Table 2-39.

Field	Description
Link Status	Specifies the link status of the ports whether it is Up/Down.
Operational Status	Specifies the LLDP-MED TLVs are transmitted or not on this interface.

### LLDP-MED Local Device Information

To display this page, click **System** > **LLDP** > **LLDP-MED** > **Local Device Information**. A screen similar to the following displays.

The screenshot shows the Netgear web interface for a GSM7352S switch. The left sidebar shows the navigation menu with 'LLDP' > 'LLDP-MED' > 'Local Device Information' selected. The main content area is titled 'LLDP-MED Local Device Information' and contains several sections:

- LLDP-MED Interface Selection:** A dropdown menu for 'Interface' showing '1/0/1'.
- Network Policies Information:** A table with columns: Media Application Type, VLAN ID, Priority, DSCP, Unknown Bit Status, and Tagged Bit Status.
- Inventory Information:** A table with fields: Hardware Revision (0x2), Firmware Revision (29), Software Revision (8.0.3.11), Serial Number (11), Manufacturer Name (Netgear), Model Name (GSM7352S), and Asset Id (asset 1717).
- Location Information:** A table with columns: Sub Type and Location Information. It includes fields for Coordinate Based (100777100777), Civic Address (100777100777), and ELIN (100777100777).
- Extended PoE:** A table with columns: Device Type, Power Source, Power Priority, and Power Value. It shows 'Unknown' for Power Source and '0 Watts' for Power Value.

At the bottom of the page, there is a 'REFRESH' button and a copyright notice: 'Copyright © 1996-2010 Netgear, Inc.'.

1. Use **Interface** to select the ports on which LLDP-MED frames can be transmitted.



The following table describes the LLDP-MED Local Device Information fields.

**Table 2-40.**

Field		Description
<b>Network Policy Information: Specifies if network policy TLV is present in the LLDP frames.</b>		
	Media Application Type	Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, vidoesignalling.  Each application type that is received has the VLAN id, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types.  If a network policy TLV has been transmitted only then would this information be displayed
<b>Inventory: Specifies if inventory TLV is present in LLDP frames.</b>		
	Hardware Revision	Specifies hardware version.
	Firmware Revision	Specifies Firmware version.
	Software Revision	Specifies Software version.
	Serial Number	Specifies serial number.
	Manufacturer Name	Specifies manufacturers name.
	Model Name	Specifies model name.
	Asset ID	Specifies asset id.
<b>Location Information: Specifies if location TLV is present in LLDP frames.</b>		
	Sub Type	Specifies type of location information.
	Location Information	Specifies the location information as a string for given type of location id.

## LLDP-MED Remote Device Information

To display this page, click **System > LLDP > LLDP-MED > Remote Device Information**. A screen similar to the following displays.

**NETGEAR**  
Connected with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management | Device View | License | Services | Stacking | SNMP | LLDP | ISDP

LLDP  
 > LLDP-MED  
   > Global Configuration  
   > Interface Configuration  
   > Local Device Information  
   > Remote Device Information  
   > Remote Device Inventory

### LLDP-MED Remote Device Information

**LLDP-MED Interface Selection**

Interface:

**Capability Information**

Supported Capabilities  
 Enabled Capabilities  
 Device Class

**Network Policies Information**

Media Application Type	VLAN ID	Priority	OSCP	Unknown Bit Status	Tagged Bit Status

**Inventory Information**

Hardware Revision  
 Firmware Revision  
 Software Revision  
 Serial Number  
 Manufacturer Name  
 Model Name  
 Asset Id

**Location Information**

Sub Type	Location Information

**Extended PoE**

Device Type	Power Source	Power Priority	Power Value

REFRESH

Copyright © 1996-2010 Netgear, Inc.

1. Use **Interface** to select the ports on which LLDP-MED is enabled.

The following table describes the LLDP-MED Remote Device Information fields.

**Table 2-41.**

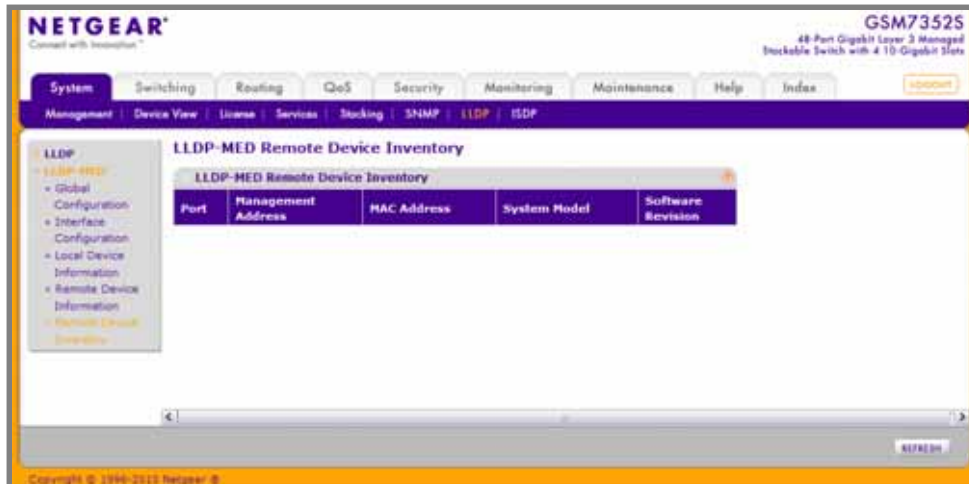
Field		Description
<b>Capability Information: Specifies the supported and enabled capabilities that was received in MED TLV on this port.</b>		
	Supported Capabilities	Specifies supported capabilities that was received in MED TLV on this port.
	Enabled Capabilities	Specifies enabled capabilities that was received in MED TLV on this port.
	Device Class	Specifies device class as advertised by the device remotely connected to the port.
<b>Network Policy Information: Specifies if network policy TLV is received in the LLDP frames on this port.</b>		
	Media Application Type	Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, vidoesignalling. Each application type that is received has the VLAN id, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been receive on this port only then would this information be displayed.
	VLAN Id	Specifies the VLAN id associated with a particular policy type.
	Priority	Specifies the priority associated with a particular policy type.
	DSCP	Specifies the DSCP associated with a particular policy type.
	Unknown Bit Status	Specifies the unknown bit associated with a particular policy type.
	Tagged Bit Status	Specifies the tagged bit associated with a particular policy type.

Table 2-41.

Field		Description
<b>Inventory Information: Specifies if inventory TLV is received in LLDP frames on this port.</b>		
	Hardware Revision	Specifies hardware version of the remote device.
	Firmware Revision	Specifies Firmware version of the remote device.
	Software Revision	Specifies Software version of the remote device.
	Serial Number	Specifies serial number of the remote device.
	Manufacturer Name	Specifies manufacturers name of the remote device.
	Model Name	Specifies model name of the remote device.
	Asset ID	Specifies asset id of the remote device.
<b>Location Information: Specifies if location TLV is received in LLDP frames on this port.</b>		
	Sub Type	Specifies type of location information.
	Location Information	Specifies the location information as a string for given type of location id.
<b>Extended POE: Specifies if remote device is a PoE device.</b>		
	Device Type	Specifies remote device's PoE device type connected to this port.
<b>Extended POE PSE: Specifies if extended PSE TLV is received in LLDP frame on this port.</b>		
	Available	Specifies the remote ports PSE power value in tenths of watts.
	Source	Specifies the remote ports PSE power source.
	Priority	Specifies the remote ports PSE power priority.
<b>Extended POE PD: Specifies if extended PD TLV is received in LLDP frame on this port.</b>		
	Required	Specifies the remote port's PD power requirement.
	Source	Specifies the remote port's PD power source.
	Priority	Specifies the remote port's PD power priority.

## LLDP-MED Remote Device Inventory

To display this page, click **System > LLDP > LLDP-MED > Remote Device Inventory**. A screen similar to the following displays.



The following table describes the LLDP-MED Remote Device Inventory fields.

**Table 2-42.**

Field	Definition
Port	Specifies the list of all the ports on which LLDP-MED is enabled.
Management Address	Specifies the advertised management address of the remote system.
MAC Address	Specifies the MAC Address associated with the remote system.
System Model	Specifies model name of the remote device.
Software Revision	Specifies Software version of the remote device.

## ISDP

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

- [Basic](#) on page 121
- [Advanced](#) on page 124

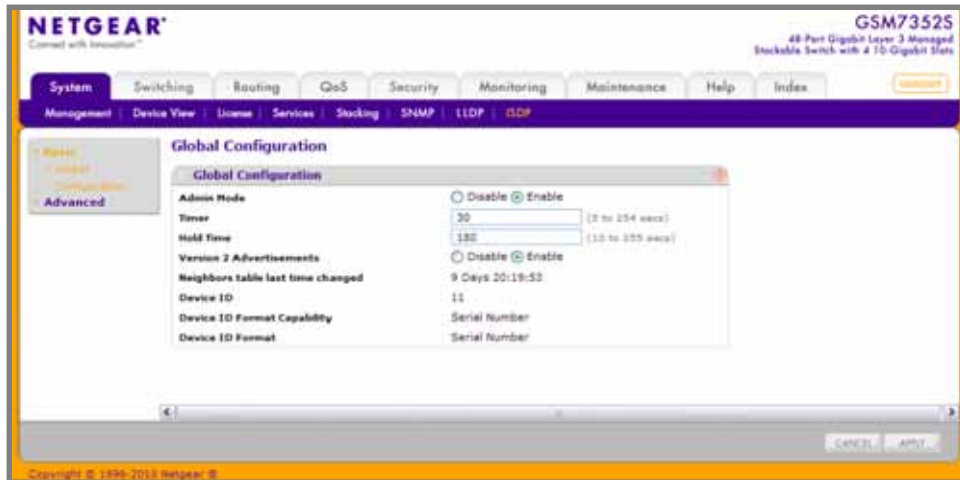
## Basic

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

- [Global Configuration](#) on page 123

## Global Configuration

To display this page, click **System > ISDP > Basic > Global Configuration**. A screen similar to the following displays.



1. Use **Admin Mode** to specify whether the ISDP Service is to be Enabled or Disabled. The default value is Enabled.
2. Use **Timer** to specify the period of time between sending new ISDP packets. The range is 5 to 254 seconds. Default value is 30 seconds.
3. Use **Hold Time** to specify the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range 10 to 255 seconds. Default value is 180 seconds.
4. Use **Version 2 Advertisements** to enable or disable the sending of ISDP version 2 packets from the device. The default value is Enabled.

The following table describes the ISDP Basic Global Configuration fields.

**Table 2-43.**

Field	Description
Neighbors table last time changed	Specifies if
Device ID	Displays the device ID of this switch.
Device ID format capability	Displays the device ID format capability.
Device ID format	Displays the device ID format.

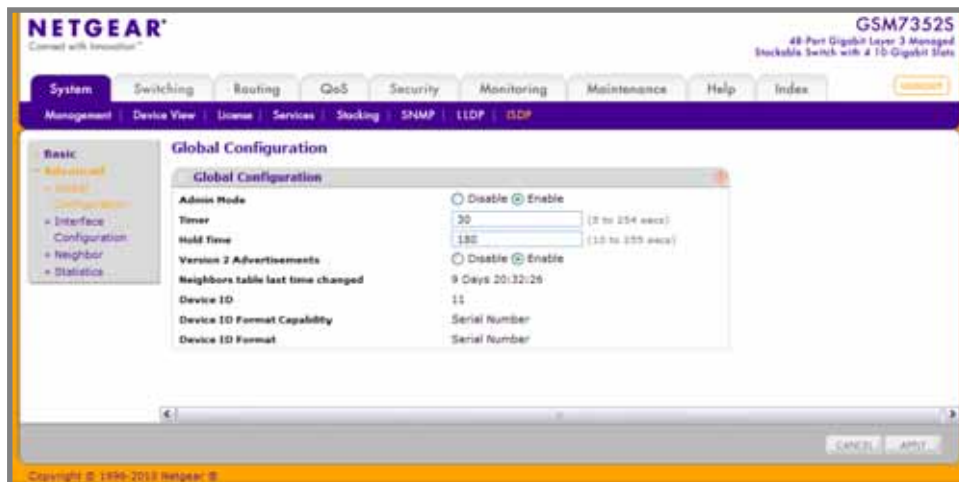
## Advanced

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

- [Global Configuration](#) on page 124
- [Interface Configuration](#) on page 126
- [ISDP Neighbor](#) on page 127
- [ISDP Statistics](#) on page 128

### Global Configuration

To display this page, click **System** > **ISDP** > **Advanced** > **Global Configuration**. A screen similar to the following displays.



1. Use **Admin Mode** to specify whether the ISDP Service is to be Enabled or Disabled. The default value is Enabled.
2. Use **Timer** to specify the period of time between sending new ISDP packets. The range is 5 to 254 seconds. Default value is 30 seconds.
3. Use **Hold Time** to specify the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range 10 to 255 seconds. Default value is 180 seconds.
4. Use **Version 2 Advertisements** to enable or disable the sending of ISDP version 2 packets from the device. The default value is Enabled.



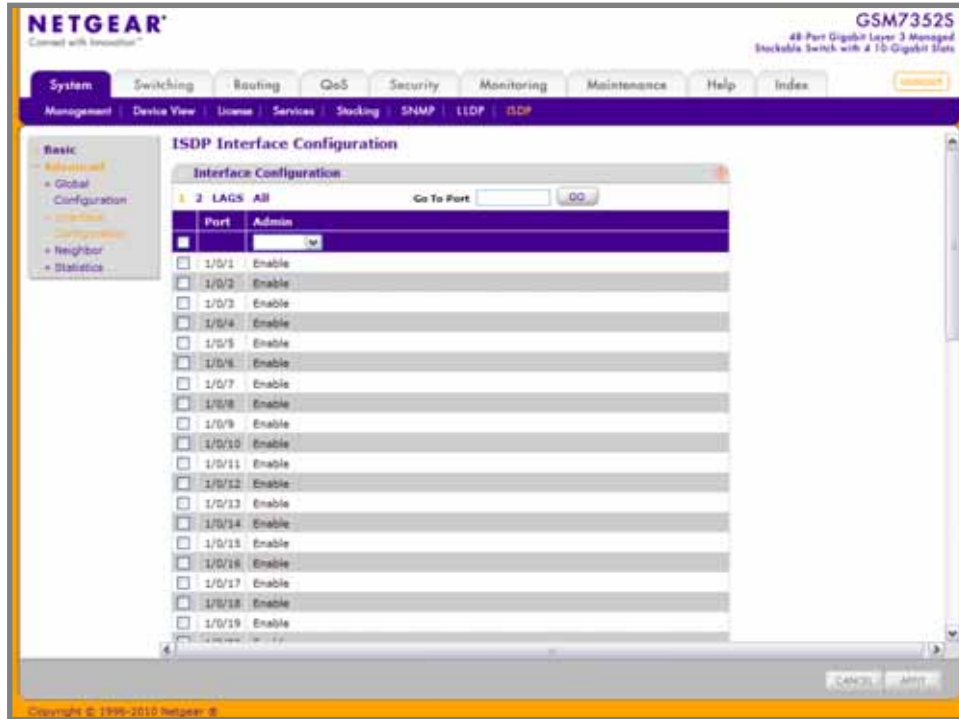
The following table describes the ISDP Advanced Global Configuration fields.

**Table 2-44.**

Field	Description
Neighbors table last time changed	Displays when the Neighbors table last changed.
Device ID	Displays the device ID of this switch.
Device ID format capability	Displays the device ID format capability.
Device ID format	Displays the device ID format.

## Interface Configuration

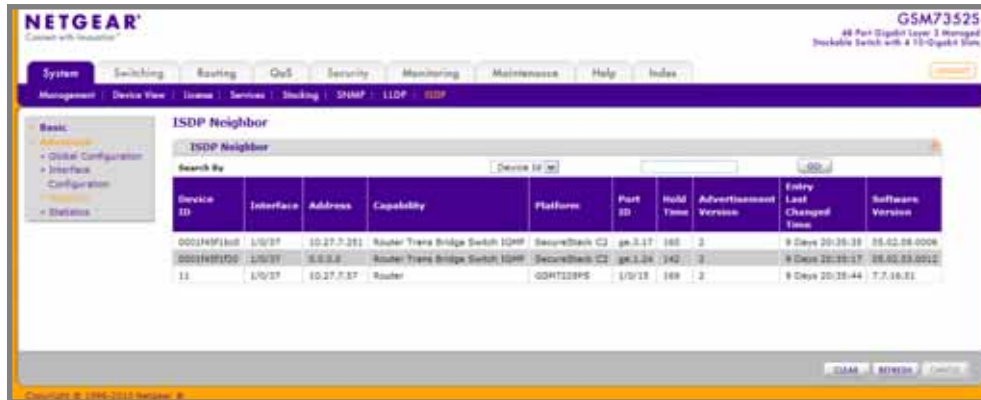
To display this page, click **System > ISDP > Advanced > Interface Configuration**. A screen similar to the following displays.



1. Use **Port** to select the port on which the admin mode is configured.
2. Use **Admin Mode** to enable or disable ISDP on the port. The default value is enable.

## ISDP Neighbor

To display this page, click **System > ISDP > Advanced > Neighbor**. A screen similar to the following displays.



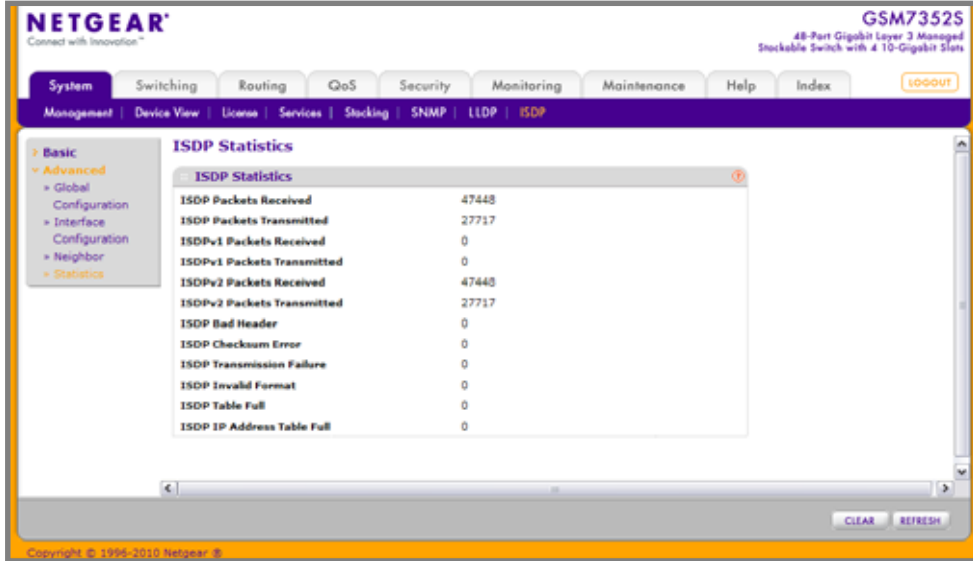
The following table describes the ISDP Neighbor fields.

**Table 2-45.**

Field	Description
Device ID	The device ID of the ISDP neighbor.
Interface	The interface on which the neighbor is discovered.
Address	Displays the address of the neighbor.
Capability	Displays the capability of the neighbor. These are supported: <ul style="list-style-type: none"> <li>• Router</li> <li>• Trans Bridge</li> <li>• Source Route</li> <li>• Switch</li> <li>• Host</li> <li>• IGMP</li> <li>• Repeater</li> </ul>
Platform	Display the model type of the neighbor. (0 to 32)
Port ID	Display the port ID on the neighbor.
Hold Time	Displays the hold time for ISDP packets that the neighbor transmits.
Advertisement Version	Displays the ISDP version sending from the neighbor.
Entry Last Changed Time	Displays the time since last entry is changed.
Software Version	Displays the software version on the neighbor.

## ISDP Statistics

To display this page, click **System > ISDP > Advanced > Statistics**. A screen similar to the following displays.



The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual interface. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar shows a tree view with Basic, Advanced, Global, Configuration, Interface, Configuration, Neighbor, and Statistics. The main content area displays the ISDP Statistics page for the GSM7352S switch. The page title is "ISDP Statistics" and it shows a table of statistics.

ISDP Statistics	
ISDP Packets Received	47448
ISDP Packets Transmitted	27717
ISDPv1 Packets Received	0
ISDPv1 Packets Transmitted	0
ISDPv2 Packets Received	47448
ISDPv2 Packets Transmitted	27717
ISDP Bad Header	0
ISDP Checksum Error	0
ISDP Transmission Failure	0
ISDP Invalid Format	0
ISDP Table Full	0
ISDP IP Address Table Full	0

At the bottom of the table, there are "CLEAR" and "REFRESH" buttons. The footer of the page shows "Copyright © 1996-2010 Netgear, Inc."

The following table describes the ISDP Statistics fields.

**Table 2-46.**

Field	Description
ISDP Packets Received	Displays the ISDP packets received including ISDPv1 and ISDPv2 packets.
ISDP Packets Transmitted	Displays the ISDP packets transmitted including ISDPv1 and ISDPv2 packets.
ISDPv1 Packets Received	Displays the ISDPv1 packets received.
ISDPv1 Packets Transmitted	Displays the ISDPv1 packets transmitted.
ISDPv2 Packets Received	Displays the ISDPv2 packets received.
ISDPv2 Packets Transmitted	Displays the ISDPv2 packets transmitted.
ISDP Bad Header	Displays the ISDP bad packets received.
ISDP Checksum Error	Displays the number of the checksum error.
ISDP Transmission Failure	Displays the number of the transmission failure.
ISDP Invalid Format	Displays the number of the invalid format ISDP packets received.
ISDP Table Full	Displays the table size of the ISDP table.
ISDP Ip Address Table Full	Displays the table size of the ISDP IP address table.

# 3. 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:

- [VLANs](#) on page 130
- [Spanning Tree Protocol](#) on page 151
- [Multicast](#) on page 168
- [Address Table](#) on page 192
- [Ports](#) on page 197
- [Link Aggregation Groups](#) on page 201

## 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:

- [Basic](#) on page 131
- [Advanced](#) on page 134

## Basic

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

- [VLAN Configuration](#) on page 132

## VLAN Configuration

Use the VLAN Configuration page to define VLAN groups stored in the VLAN membership table. Each switch in the ProSafe® Managed Switches family supports up to 1024 VLANs. Only one VLAN is created by default, VLAN 1 is the only one created:

- VLAN 1 is the default VLAN of which all ports are members.

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

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

System Switching Routing QoS Security Monitoring Maintenance Help Index LOGOUT

VLAN STP Multicast Address Table Ports LAG

Basic  
VLAN Configuration  
Advanced

### VLAN Configuration

**Reset**

☐ Reset Configuration

**Internal VLAN Configuration**

Internal VLAN Allocation Base: 4093

Internal VLAN Allocation Policy: ☐ Ascending ☒ Descending

VLAN ID	VLAN Name	VLAN Type	Make Static
<input type="checkbox"/> 1	Default	Default	<input type="button" value="Disable"/>

ADD DELETE CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

1. **Reset Configuration** - If you select this checkbox and click the **APPLY** button, all VLAN configuration parameters will be reset to their factory default values. Also, all VLANs, except for the default VLAN, will be deleted. The factory default values are:

- All ports are assigned to the default VLAN of 1.
- All ports are configured with a PVID of 1.
- All ports are configured to an Acceptable Frame Types value of Admit All Frames.
- All ports are configured with Ingress Filtering disabled.
- All ports are configured to transmit only untagged frames.
- GVRP is disabled on all ports and all dynamic entries are cleared.



## Internal VLAN Configuration

This section displays the allocation base and the allocation mode of internal VLAN. The internal VLAN is reserved by port-based routing interface and invisible to the end user. Once these internal VLANs are allocated by port-based routing interface, they are cannot be assigned to a routing VLAN interface.

1. Use **Internal VLAN Allocation Base** to specify the VLAN Allocation Base for the routing interface. The default base of the internal VLAN is 1 to 4093.
2. Use the optional **Internal VLAN Allocation Policy** field to specify a policy for the internal VLAN allocation. There are two policies supported: ascending and descending.

## VLAN Configuration

1. Use **VLAN ID** to specify the VLAN Identifier for the new VLAN. The range of the VLAN ID is 1 to 4093.
2. Use the optional **VLAN Name** 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 always has a name of 'Default'.
3. Click **ADD** to add a new VLAN to the switch.
4. Click **DELETE** to delete a selected VLAN from the switch.

Table 3-47.

Field	Description
VLAN Type	This field identifies the type of the VLAN you are configuring. You cannot change the type of the default VLAN (VLAN ID = 1): it is always type 'Default'. When you create a VLAN, using this screen, its type will always be 'Static'. A VLAN that is created by GVRP registration initially has a type of 'Dynamic'. When configuring a Dynamic VLAN, you can change its type to 'Static'.

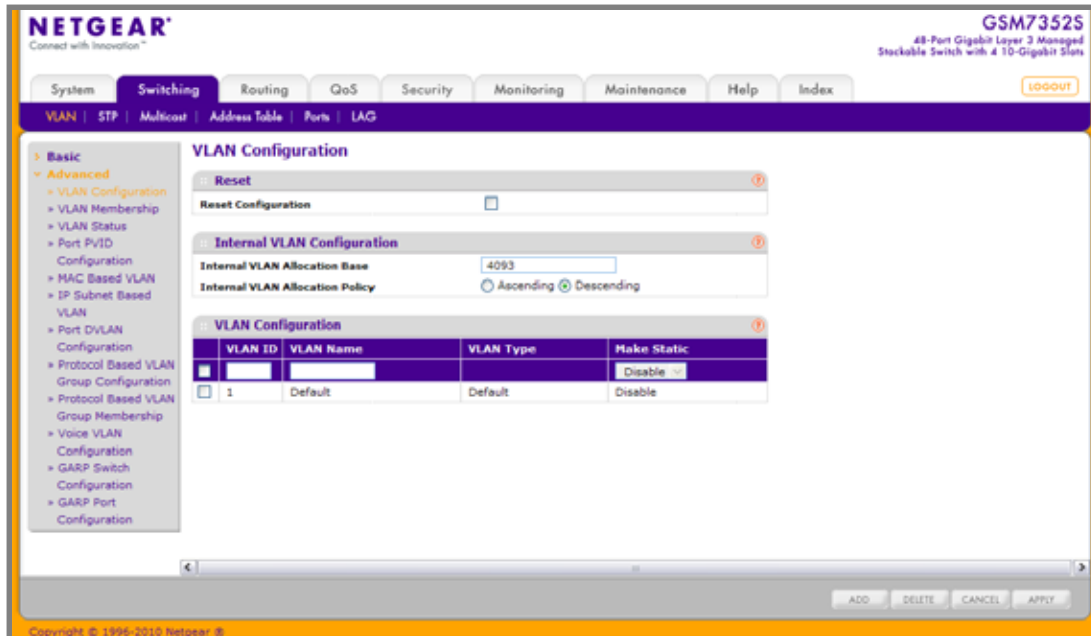
## Advanced

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

- [VLAN Configuration](#) on page 132
- [VLAN Membership](#) on page 136
- [VLAN Status](#) on page 138
- [Port PVID Configuration](#) on page 139
- [MAC Based VLAN](#) on page 141
- [IP Subnet Based VLAN](#) on page 142
- [Port DVLAN Configuration](#) on page 143
- [Protocol Based VLAN Group Configuration](#) on page 144
- [Protocol Based VLAN Group Membership](#) on page 146
- [Voice VLAN Configuration](#) on page 147
- [GARP Switch Configuration](#) on page 149
- [GARP Port Configuration](#) on page 150

## VLAN Configuration

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



**Reset Configuration** - If you select this button and confirm your selection on the next screen, all VLAN configuration parameters will be reset to their factory default values. Also, all VLANs, except for the default VLAN, will be deleted. The factory default values are:

- All ports are assigned to the default VLAN of 1.
- All ports are configured with a PVID of 1.
- All ports are configured to an Acceptable Frame Types value of Admit All Frames.
- All ports are configured with Ingress Filtering disabled.
- All ports are configured to transmit only untagged frames.
- GVRP is disabled on all ports and all dynamic entries are cleared.

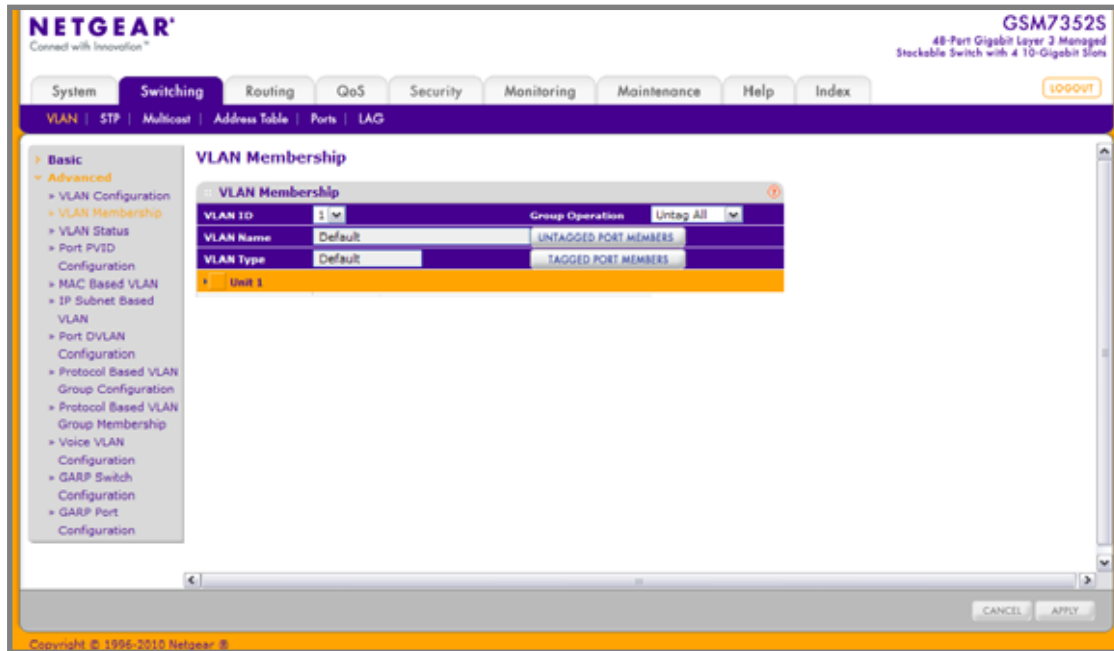
## Internal VLAN Configuration

This page displays the allocation base and the allocation mode of internal VLAN. The internal VLAN is reserved by port-based routing interface and invisible to the end user. Once these internal VLANs are allocated by port-based routing interface, they cannot be assigned to a routing VLAN interface.

1. Use **Internal VLAN Allocation Base** to specify the VLAN Allocation Base for the routing interface. The default base of the internal VLAN is 1 to 4093.
2. Use the optional **Internal VLAN Allocation Policy** field to specify a policy for the internal VLAN allocation. There are two policies supported: ascending and descending.

## VLAN Membership

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



To configure VLAN membership:

1. Use **VLAN ID** to select the VLAN ID for which you want to display or configure data.
2. Use **Group Operation** to select all the ports and configure them:
  - **Untag All** - Select all the ports on which all frames transmitted for 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** - All the ports that may be dynamically registered in this VLAN via GVRP. This selection has the effect of excluding all ports from the selected VLAN.
3. Use **Port List** to add the ports you selected to this VLAN. Each port has three modes:
  - **T(Tagged)** - Select the ports on which all frames transmitted for this VLAN will be tagged. The ports that are selected will be included in the VLAN.
  - **U(Untagged)** - Select the ports on which all frames transmitted for this VLAN will be untagged. The ports that are selected will be included in the VLAN.
  - **BLANK(Autodetect)** - Select the ports that may be dynamically registered in this VLAN via GVRP. This selection has the effect of excluding a port from the selected VLAN.

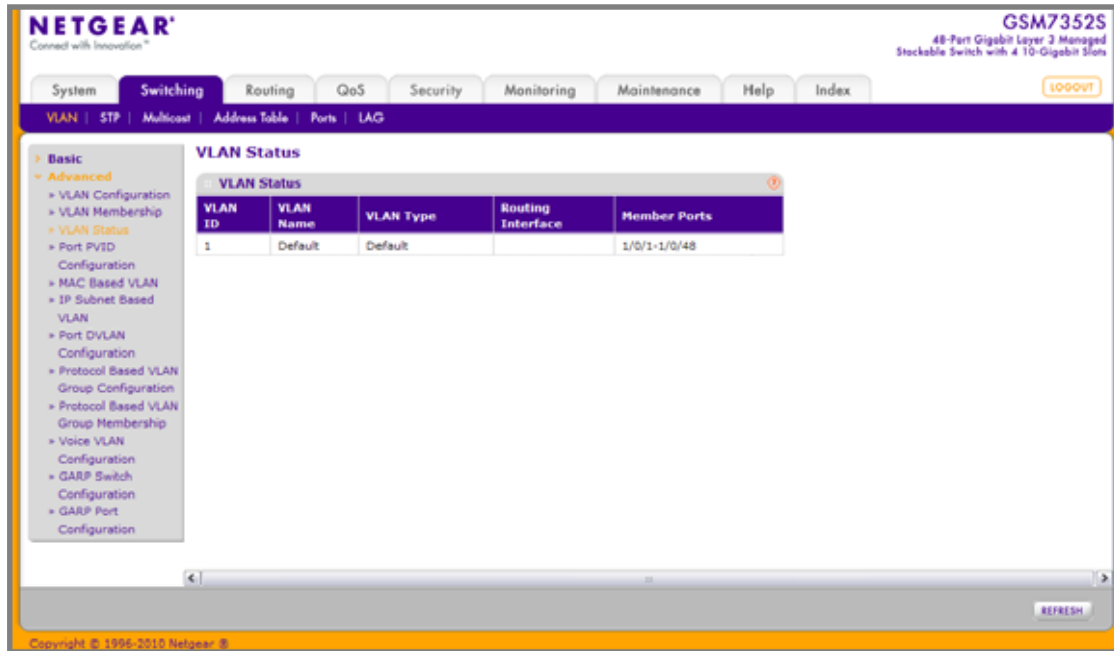
Table 3-48.

Field	Definition
VLAN Name	This field identifies the name for the VLAN you selected. It can be up to 32 alphanumeric characters long, including blanks. VLAN ID 1 always has a name of 'Default'.
VLAN Type	This field identifies the type of the VLAN you selected. The VLAN type: Default (VLAN ID = 1) -- always present Static -- a VLAN you have configured Dynamic -- a VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore remove.

## VLAN Status

Use this page to display the status of all currently configured VLANs.

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



**Table 3-49.**

Field	Definition
VLAN ID	The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named 'Default'.
VLAN Type	The VLAN type: <ul style="list-style-type: none"> <li>• Default (VLAN ID = 1) -- always present</li> <li>• Static -- a VLAN you have configured</li> <li>• Dynamic -- a VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore remove</li> </ul>
Routing Interface	The interface associated with the VLAN, in the case that VLAN routing is configured for this VLAN.
Member Ports	The ports that are included in the VLAN.

## Port PVID Configuration

The Port PVID Configuration screen lets you assign a port VLAN ID (PVID) to an interface. There are certain requirements for a PVID:

- All ports must have a defined PVID.
- If no other value is specified, the default VLAN PVID is used.
- If you want to change the port's default PVID, you must first create a VLAN that includes the port as a member.
- Use the Port VLAN ID (PVID) Configuration page to configure a virtual LAN on a port.

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

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

System Switching Routing QoS Security Monitoring Maintenance Help Index

VLAN STP Multicast Address Table Ports LAG

Basic  
Advanced  
VLAN Configuration  
VLAN Membership  
VLAN Status  
Port PVID Configuration  
MAC Based VLAN  
IP Subnet Based VLAN  
Port DVLAN Configuration  
Protocol Based VLAN Group Configuration  
Protocol Based VLAN Group Membership  
Voice VLAN Configuration  
GARP Switch Configuration  
GARP Port Configuration

**Port PVID Configuration**

PVID Configuration

Go To Interface  GO

Interface	PVID	Acceptable Frame Types	Ingress Filtering	Port Priority
<input type="checkbox"/> 1/0/1	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/2	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/3	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/4	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/5	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/6	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/7	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/8	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/9	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/10	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/11	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/12	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/13	1	Admit All	Disable	0
<input type="checkbox"/> 1/0/14	1	Admit All	Disable	0

CANCEL APPLY

Copyright © 1999-2010 Netgear, Inc.

To configure PVID information:

1. Click **ALL** to display information for all Physical ports and LAGs.
2. 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.
3. Use **Interface** to select the interface you want to configure.
4. Use **PVID** to specify the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The factory default is 1.
5. Use **Acceptable Frame Types** to specify the types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All':
  - When set to '**VLAN only**', untagged frames or priority tagged frames received on this port are discarded.
  - When set to '**Admit All**', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
6. **Ingress Filtering:**
  - When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is 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.
  - When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
7. Use **Port Priority** to specify the default 802.1p priority assigned to untagged packets arriving at the port. The possible value is from 0 to 7.



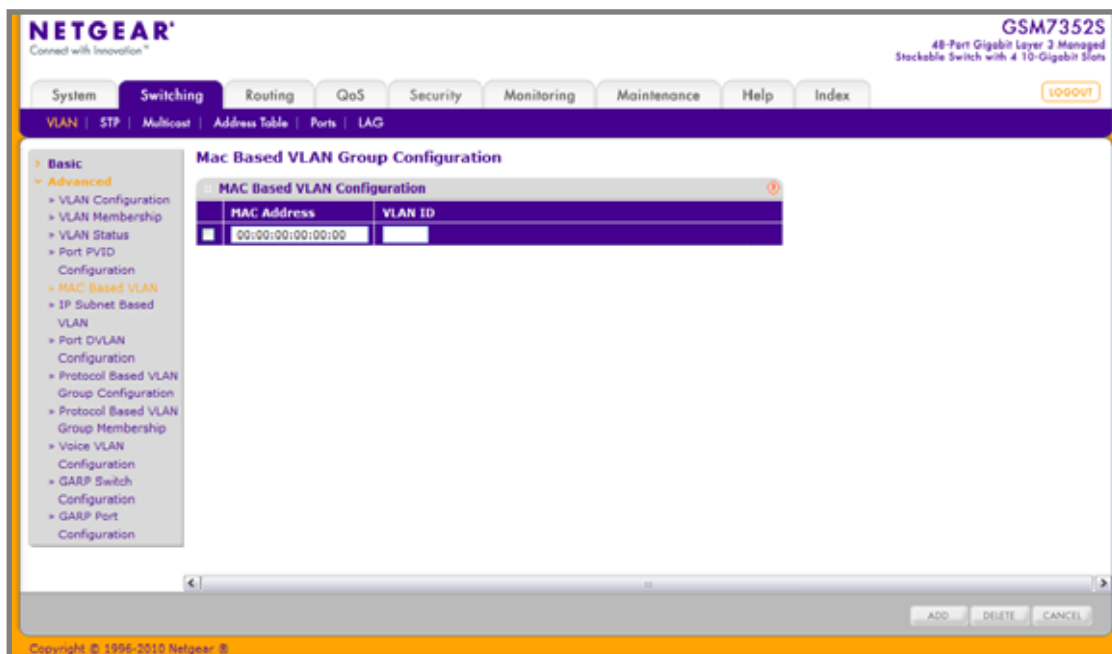
## MAC Based VLAN

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

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. This implies that the user is allowed to configure a MAC address mapping to a VLAN that has not been created on the system.

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



1. **MAC Address** - Valid MAC Address which is to be bound to a VLAN ID. This field is configurable only when a MAC Based VLAN is created.
2. Use **VLAN ID** to specify a VLAN ID in the range of 1 to 4093.
3. Click **ADD** to add an entry of MAC Address to VLAN mapping.
4. Click **DELETE** to delete an entry of MAC Address to VLAN mapping.

## IP Subnet Based VLAN

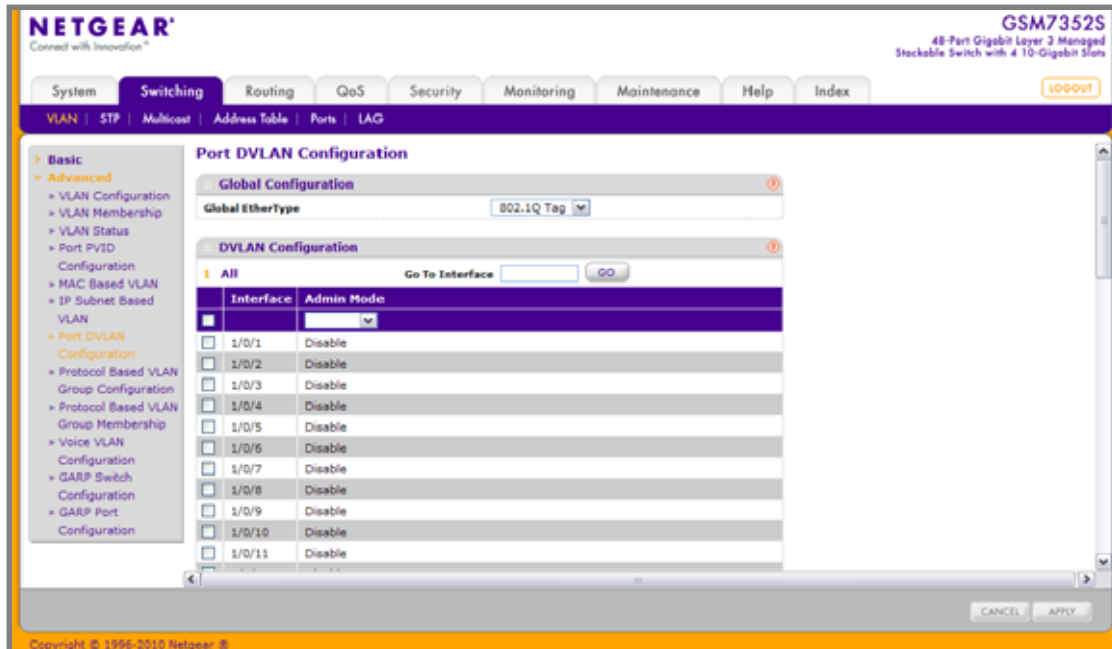
IP Subnet to VLAN mapping is defined by configuring an entry in the IP Subnet to VLAN table. An entry is specified via a source IP address, network mask, and the desired VLAN ID. The IP Subnet to VLAN configurations are shared across all ports of the device.

To display the MAC Based VLAN page, click **Switching** > **VLAN** > **Advanced** > **IP Subnet Based VLAN**.

1. Use **IP Address** to specify a valid IP Address bound to VLAN ID. Enter the IP Address in dotted decimal notation.
2. Use **Subnet Mask** to specify a valid Subnet Mask of the IP Address. Enter the Subnet mask in dotted decimal notation.
3. Use **VLAN ID** to specify a VLAN ID in the range of (1 to 4093).
4. Click **ADD** to add a new IP subnet-based VLAN.
5. Click **DELETE** to delete the IP subnet-based VLAN selected.

## Port DVLAN Configuration

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



1. Use **Interface** to select the physical interface for which you want to display or configure data. Select 'All' to set the parameters for all ports to same values.
2. Use **Admin Mode** to specify the administrative mode via which Double VLAN Tagging can be enabled or disabled. The default value for this is Disabled.
3. Use the 2-byte hex Global EtherType as the first 16 bits of the DVlan tag.
  - **802.1Q Tag** - Commonly used tag representing 0x8100
  - **vMAN Tag** - Commonly used tag representing 0x88A8
  - **Custom Tag** - Configure the EtherType in any range from 0 to 65535

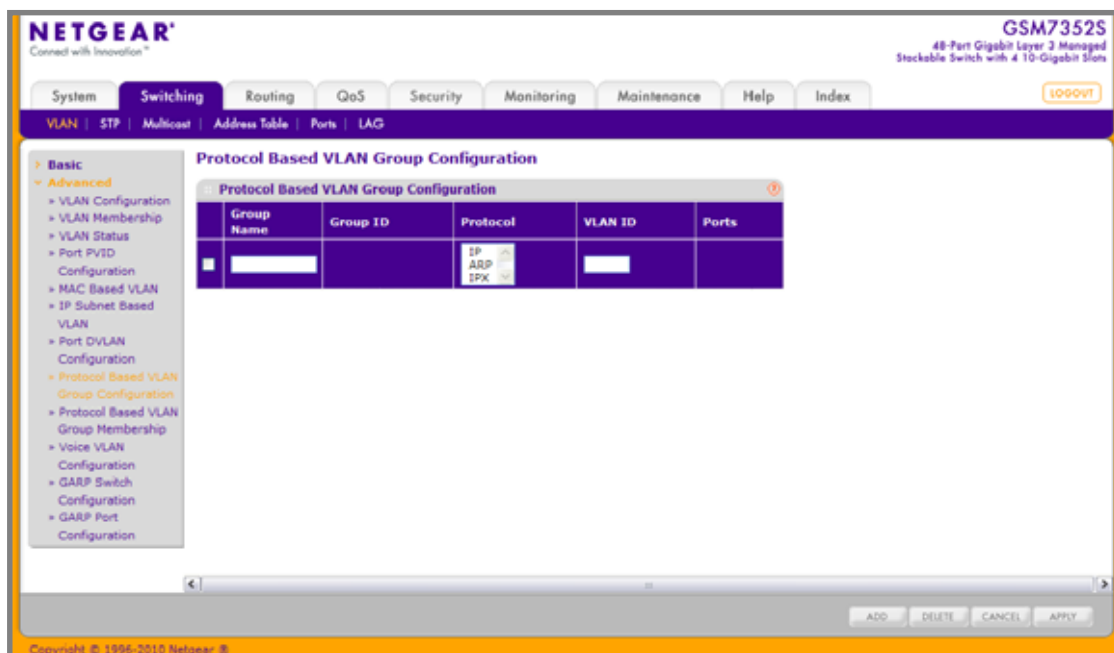
## Protocol Based VLAN Group Configuration

You can use a protocol based VLAN to define filtering criteria for untagged packets. 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. Untagged frames received on the port for other protocols will be assigned the Port VLAN ID - 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 three protocol definitions, and can include multiple ports. When you create a group you will choose a name and a Group ID will be assigned automatically.

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



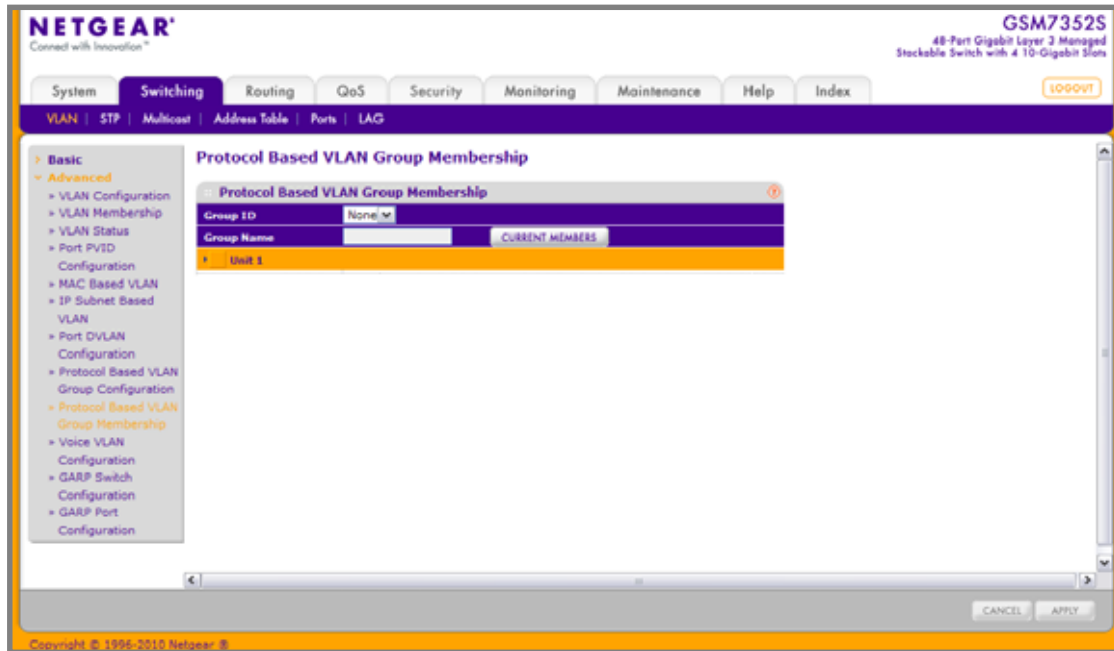
1. Use **Group Name** to assign a name to a new group. You may enter up to 16 characters.
2. Use **Protocol(s)** to select the protocols you want to be associated with the group. There are three configurable protocols: IP, IPX, ARP.
  - **IP** - IP is a network layer protocol that provides a connectionless service for the delivery of data.
  - **ARP** - Address Resolution Protocol (ARP) is a low-level protocol that dynamically maps network layer addresses to physical medium access control (MAC) addresses
  - **IPX** - The Internetwork Packet Exchange (IPX) is a connectionless datagram Network-layer protocol that forwards data over a network.
3. Use **VLAN ID** to select the VLAN ID. It can be any number in the range of 1 to 4093. All the ports in the group will assign this VLAN ID to untagged packets received for the protocols you included in this group.
4. Click **ADD** to add a new Protocol Based VLAN group to the switch.
5. Click **DELETE** to remove the Protocol Based VLAN group identified by the value in the Group ID field.

Table 3-50.

Field	Description
Group ID	A number used to identify the group created by the user. Group IDs are automatically assigned when a group is created by the user.
Ports	Display all the member ports which belong to the group.

## Protocol Based VLAN Group Membership

To display the Protocol Based VLAN Group Membership page, click **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership**.



1. Use **Group ID** to select the protocol-based VLAN Group ID for which you want to display or configure data.
2. Use **Port List** to add the ports you selected to this Protocol Based VLAN Group. Note that a given interface can only belong to one group for a given protocol. 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.

**Table 3-51.**

Field	Description
Group Name	This field identifies the name for the protocol-based VLAN you selected. It can be up to 32 alphanumeric characters long, including blanks.
Current Members	This button can be click to show the current numbers in the selected protocol based VLAN Group.

## Voice VLAN Configuration

Use this menu to configure the parameters for Voice VLAN Configuration. Note that only a user with Read/Write access privileges may change the data on this screen.

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

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

VLAN | STP | Multicast | Address Table | Ports | LAG

**Basic**  
 - Advanced  
 - VLAN Configuration  
 - VLAN Membership  
 - VLAN Status  
 - Port PVID Configuration  
 - MAC Based VLAN  
 - IP Subnet Based VLAN  
 - Port D/VLAN Configuration  
 - Protocol Based VLAN Group Configuration  
 - Protocol Based VLAN Group Membership  
 - **Voice VLAN**  
 - Configuration  
 - GARP Switch Configuration  
 - GARP Port Configuration

**Voice VLAN Configuration**

Voice VLAN Global Admin  
Admin Mode: ☒ Disable ☐ Enable

Voice VLAN Configuration  
Go To Interface:

Interface	Interface Mode	Value	CoS Override Mode	DSCP Value	Operational State
<input type="checkbox"/> 1/5/1	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/2	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/3	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/4	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/5	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/6	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/7	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/8	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/9	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/10	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/11	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/12	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/13	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/14	Disable	0	Disable	0	Disable
<input type="checkbox"/> 1/5/15	Disable	0	Disable	0	Disable

Copyright © 1999-2013 Netgear, Inc.

1. Use **Admin Mode** to select the administrative mode for Voice VLAN for the switch. The default is disable.
2. Use **Interface** to select the physical interface for which you want to configure data.
3. Use **Interface Mode** to select the Voice VLAN mode for selected interface:
  - **Disable** - Default value
  - **None** - Allow the IP phone to use its own configuration to send untagged voice traffic
  - **VLAN ID** - Configure the phone to send tagged voice traffic.
  - **dot1p** - Configure Voice Vlan 802.1p priority tagging for voice traffic. When this is selected, please enter the dot1p value in the Value field.
  - **Untagged** - Configure the phone to send untagged voice traffic.
4. Use **Value** to enter the VLAN ID or dot1p value. This is enable only when VLAN ID or dot1p is selected as Interface Mode.
5. Use **CoS Override Mode** to select the Cos Override mode for selected interface. The default is disable.

Table 3-52.

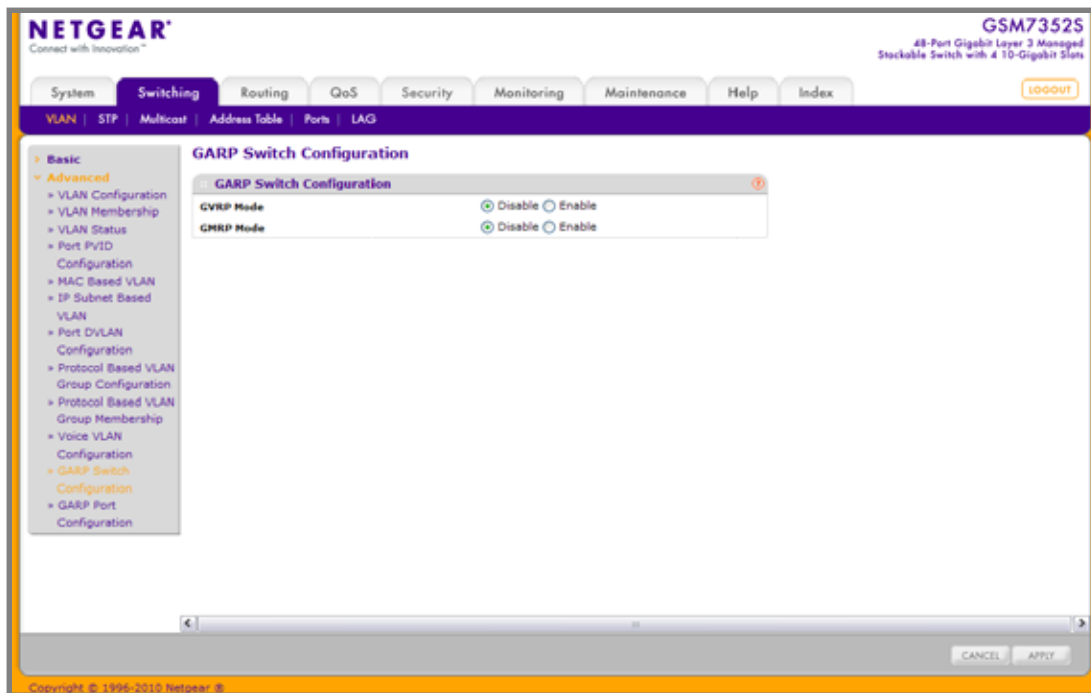
Field	Description
Operational State	This is the operational status of the voice vlan on the given interface.



## GARP Switch Configuration

**Note:** It can take up to 10 seconds for GARP configuration changes to take effect.

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

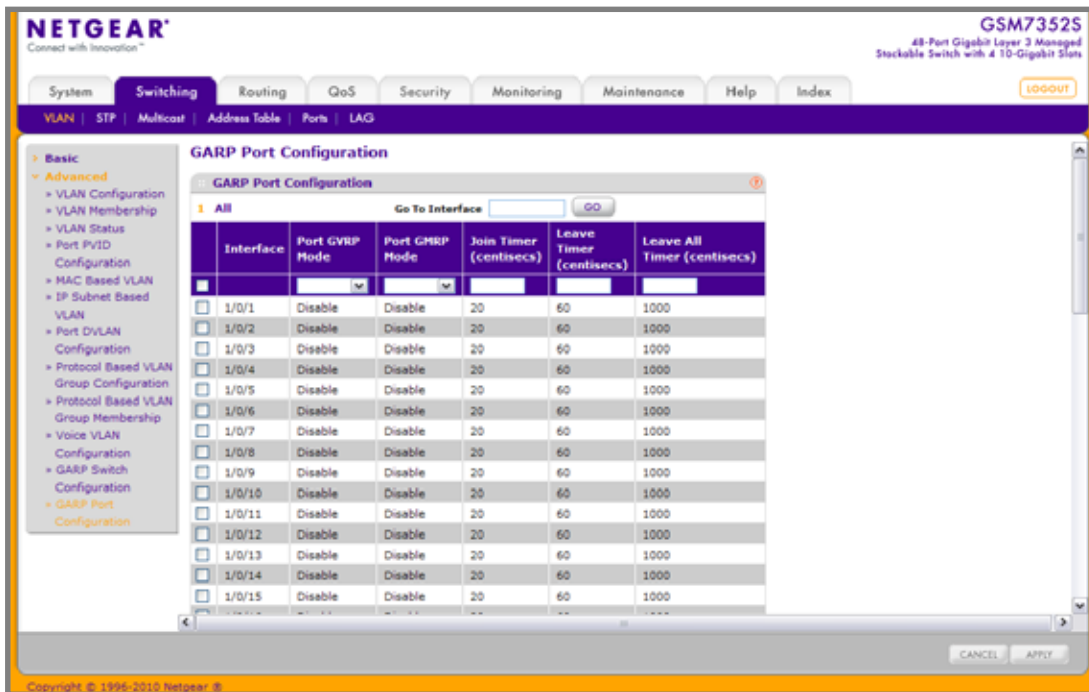


1. Use **GVRP Mode** to choose the GARP VLAN Registration Protocol administrative mode for the switch by selecting enable or disable from the radio button. The factory default is disable.
2. Use **GMRP Mode** to choose the GARP Multicast Registration Protocol administrative mode for the switch by selecting enable or disable from the radio button. The factory default is disable.

## GARP Port Configuration

**Note:** It can take up to 10 seconds for GARP configuration changes to take effect.

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



**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

VLAN | STP | Multicast | Address Table | Ports | LAG

**GARP Port Configuration**

Go To Interface:

Interface	Port GVRP Mode	Port GMRP Mode	Join Timer (centiseconds)	Leave Timer (centiseconds)	Leave All Timer (centiseconds)
<input type="checkbox"/> 1/0/1	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/2	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/3	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/4	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/5	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/6	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/7	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/8	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/9	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/10	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/11	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/12	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/13	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/14	Disable	Disable	20	60	1000
<input type="checkbox"/> 1/0/15	Disable	Disable	20	60	1000

Copyright © 1994-2015 Netgear, Inc.

1. Use **Interface** to select the physical interface for which data is to be displayed or configured.
2. Use **Port GVRP Mode** to choose the GARP VLAN Registration Protocol administrative mode for the port by selecting enable or disable from the dropdown list. If you select disable, the protocol will not be active and the Join Time, Leave Time and Leave All Time will have no effect. The factory default is disable.
3. Use **Port GMRP Mode** to choose the GARP Multicast Registration Protocol administrative mode for the port by selecting enable or disable from the dropdown list. If you select disable, the protocol will not be active, and Join Time, Leave Time and Leave All Time have no effect. The factory default is disable.
4. Use **Join Time (centiseconds)** to specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. Enter a number between 10 and 100 (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). An instance of this timer exists for each GARP participant for each port.
5. Use **Leave Time (centiseconds)** to specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 20 and 600 (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.
6. Use **Leave All Time (centiseconds)** to control how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5\*LeaveAllTime. The timer is specified in centiseconds. Enter a number between 200 and 6000 (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). An instance of this timer exists for each GARP participant for each port.

## 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 <pdf>“CST Port Configuration” on page 3-159.

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 VLAN link, you can access the following pages:

- [Basic](#) on page 152
- [Advanced](#) on page 155

## Basic

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

- [STP Configuration](#) on page 153

## STP Configuration

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

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

The screenshot displays the Netgear web interface for a GSM7352S switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under Switching, the STP configuration page is selected. The left sidebar shows a tree view with Basic, STP, Configuration, and Advanced options. The main content area is titled 'STP Configuration' and contains the following settings:

- Spanning Tree Admin Mode: ☐ Disable ☒ Enable
- Force Protocol Version: ☐ IEEE 802.1d ☐ IEEE 802.1w ☒ IEEE 802.1s
- Configuration Name: 60-09-08-07-06-05
- Configuration Revision Level: 0 (0 to 65535)
- Forward BPDUs while STP Disabled: ☒ Disable ☐ Enable
- BPDUs Guard: ☒ Disable ☐ Enable
- BPDUs Filter: ☒ Disable ☐ Enable
- Configuration Digest Key: 0xac36177f50283cd4b83821d8ab26de62

Below the configuration fields is the 'STP Status' section, which contains a table with the following data:

MST ID	VID	PID
0	1	1

At the bottom of the page, there are 'CANCEL' and 'APPLY' buttons, and a copyright notice: Copyright © 1996-2010 Netgear, Inc.

1. Use **Spanning Tree Admin Mode** to specify whether spanning tree operation is enabled on the switch. Value is enabled or disabled.
2. Use **Force Protocol Version** to specify the Force Protocol Version parameter for the switch. The options are IEEE 802.1d, IEEE 802.1w and IEEE 802.1s.
3. Use **Configuration Name** to specify an identifier used to identify the configuration currently being used. It may be up to 32 alphanumeric characters.
4. Use **Configuration Revision Level** to specify an identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0.
5. Use **Forward BPDU while STP Disabled** to specify whether spanning tree BPDUs should be forwarded or not while spanning-tree is disabled on the switch. Value is enabled or disabled.
6. Use **BPDU Guard** to specify whether the BPDU guard feature is enabled. The STP BPDU guard allows a network administrator to enforce the STP domain borders and keep the active topology consistent and predictable. The switches behind the edge ports that have STP BPDU guard enabled will not be able to influence the overall STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that is configured with this option and transitions the port into disable state. This would lead to administrative disable of the port.
7. Use **BPDU Filter** to specify whether the BPDU Filter feature is enabled. STP BPDU filtering applies to all operational edge ports. Edge Port in an operational state is supposed to be connected to hosts that typically drop BPDUs. If an operational edge port receives a BPDU, it immediately loses its operational status. In that case, if BPDU filtering is enabled on this port then it drops the BPDUs received on this port.

Table 3-53.

Field	Description
Configuration digest key	Identifier used to identify the configuration currently being used.
MST ID	Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID ID	Table consisting of the VLAN IDs and the corresponding FID associated with each of them.
FID ID	Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

## Advanced

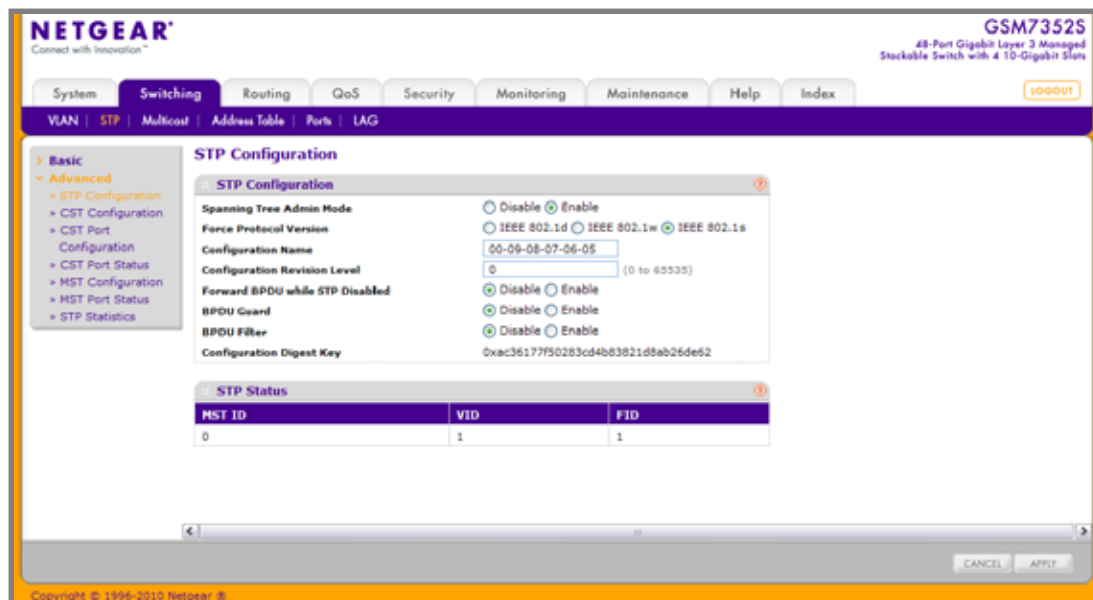
From the Advanced link, you can access the following pages:

- [STP Configuration](#) on page 155
- [CST Configuration](#) on page 157
- [CST Port Configuration](#) on page 159
- [CST Port Status](#) on page 161
- [MST Configuration](#) on page 163
- [MST Port Status](#) on page 165
- [STP Statistics](#) on page 167

### STP Configuration

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

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



**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

System Switching Routing QoS Security Monitoring Maintenance Help Index

VLAN STP Multicast Address Table Ports IAG

Basic  
Advanced  
STP Configuration  
CST Configuration  
CST Port Configuration  
CST Port Status  
MST Configuration  
MST Port Status  
STP Statistics

### STP Configuration

STP Configuration

Spanning Tree Admin Mode ☐ Disable ☒ Enable

Force Protocol Version ☐ IEEE 802.1d ☐ IEEE 802.1w ☒ IEEE 802.1s

Configuration Name 00-09-08-07-06-05

Configuration Revision Level 0 (0 to 65535)

Forward BPDUs while STP Disabled ☒ Disable ☐ Enable

BPDUs Guard ☒ Disable ☐ Enable

BPDUs Filter ☒ Disable ☐ Enable

Configuration Digest Key 0xac36177f50283cd4b83821d8ab26de62

### STP Status

MST ID	VID	FID
0	1	1

CANCEL APPLY

Copyright © 1999-2019 Netgear, Inc.

1. Use **Spanning Tree Admin Mode** to specify whether spanning tree operation is enabled on the switch. Value is enabled or disabled.
2. Use **Force Protocol Version** to specify the Force Protocol Version parameter for the switch. The options are IEEE 802.1d, IEEE 802.1w, and IEEE 802.1s.
3. Use **Configuration Name** to specify the identifier used to identify the configuration currently being used. It may be up to 32 alphanumeric characters.
4. Use **Configuration Revision Level** to specify the identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0.
5. Use **Forward BPDU while STP Disabled** to specify whether spanning tree BPDUs should be forwarded while spanning-tree is disabled on the switch. Value is enabled or disabled.
6. Use **BPDU Guard** to specify whether the BPDU guard feature is enabled. The STP BPDU guard allows a network administrator to enforce the STP domain borders and keep the active topology be consistent and predictable. The switches behind the edge ports that have STP BPDU guard enabled will not be able to influence the overall STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that is configured with this option and transitions the port into disable state. This would lead to administrative disable of the port.
7. Use **BPDU Filter** to specify whether the BPDU Filter feature is enabled. STP BPDU filtering applies to all operational edge ports. Edge Port in an operational state is supposed to be connected to hosts that typically drop BPDUs. If an operational edge port receives a BPDU, it immediately loses its operational status. In that case, if BPDU filtering is enabled on this port then it drops the BPDUs received on this port.

Table 3-54.

Field	Description
Configuration digest key	Identifier used to identify the configuration currently being used.
MST ID	Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID ID	Table consisting of the VLAN IDs and the corresponding FID associated with each of them.
FID ID	Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.



## 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 ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual interface. The top navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Switching tab is selected, and the sub-menu shows VLAN, STP, Multicast, Address Table, Ports, and LAG. The STP tab is selected, and the sub-menu shows Basic, Advanced, STP Configuration, CST Configuration, CST Port Configuration, CST Port Status, MST Configuration, MST Port Status, and STP Statistics. The CST Configuration page is displayed, showing the following configuration fields:

Field	Value	Range
Bridge Priority	32768	(0 to 61440)
Bridge Max Age (secs)	20	(6 to 40)
Bridge Hello Time (secs)	2	(1 to 10)
Bridge Forward Delay (secs)	15	(4 to 30)
Spanning Tree Maximum Hops	20	(6 to 40)
Spanning Tree Tx Hold Count	6	(1 to 10)

Below the configuration fields is the CST Status section, which displays the following information:

Field	Value
Bridge Identifier	80:00:00:09:08:07:06:05
Time Since Topology Change	2 day 1 hr 38 min 51 sec
Topology Change Count	1
Topology Change	False
Designated Root	00:00:00:01:f4:5f:1b:c0
Root Path Cost	200000
Root Port Identifier	80:25
Max Age (secs)	20
Forward Delay (secs)	15
Hold Time (secs)	6
CST Regional Root	80:00:00:09:08:07:06:05
CST Path Cost	0

At the bottom of the page, there are buttons for REFRESH, CANCEL, and APPLY. The copyright notice at the bottom reads: Copyright © 1996-2013 Netgear, Inc.

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 bridge 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. The value must be less than or equal to  $(\text{Bridge Max Age} / 2) - 1$ . The default hello time value is 2.

- **Bridge Forward Delay (secs)** - Specifies the bridge 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.
- **Spanning Tree Tx Hold Count** - Configures the maximum number of bpdus the bridge is allowed to send within the hello time window. The default value is 6.

**Table 3-55.**

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	Number of times 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. It takes a value if 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 Identifier	Port to access the Designated Root for the CST.
Max Age(secs)	Path Cost to the Designated Root for the CST.
Forward Delay(secs)	Derived value of the Root Port Bridge Forward Delay parameter.
Hold Time(secs)	Minimum time between transmission of Configuration BPDUs.
CST Regional Root	Priority and base MAC address of the CST Regional Root.
CST Path Cost	Path Cost to the CST tree Regional Root.

## 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**.

Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Timer	External Port Path Cost	Auto Calculated External Port Path Cost	BPDU Filter	BPDU Flood	BPDU Guard Effect	Auto Edge	Root Guard	Loop Guard	TCN Guard	Port Mode	Port Force State
1/0/1	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/2	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/3	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/4	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/5	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/6	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/7	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/8	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/9	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/10	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/11	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/12	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/13	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/14	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/15	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/16	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/17	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/18	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/19	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/20	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/21	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/22	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/23	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/24	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/25	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/26	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/27	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/28	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/29	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/30	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/31	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/32	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/33	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/34	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/35	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/36	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/37	128	Enable	200000	Disabled	0	200000	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Force
1/0/38	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/39	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/40	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/41	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/42	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/43	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/44	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/45	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/46	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/47	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/48	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/49	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/50	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/51	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/52	128	Enable	0	Disabled	0	0	Disabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled

To configure CST port settings:

1. **Interface** - One of the physical or port channel interfaces associated with VLANs associated with the CST.
2. Use **Port Priority** to specify the priority for a particular port within the CST. The port priority is set in multiples of 16. For example if the priority is attempted to be set to any value between 0 and 15, it will be set to 0. If it is tried to be set to any value between 16 and  $(2*16-1)$  it will be set to 16 and so on.

3. Use **Admin Edge Port** to specify if the specified port is an Edge Port within the CIST. It takes a value of TRUE or FALSE, where the default value is FALSE.
4. Use **Port Path Cost** to set the Path Cost to a new value for the specified port in the common and internal spanning tree. It takes a value in the range of 1 to 200000000.
5. Use **External Port Path Cost** to set the External Path Cost to a new value for the specified port in the spanning tree. It takes a value in the range of 1 to 200000000.
6. Use **BPDU Filter** to configure the BPDU Filter, which filters the BPDU traffic on this port when STP is enabled on this port. The possible values are Enable or Disable.
7. Use **BPDU Flood** to configure the BPDU Flood, which floods the BPDU traffic arriving on this port when STP is disabled on this port. The possible values are Enable or Disable.
8. Use **Auto Edge** to configure the auto edge mode of a port, which allows the port to become an edge port if it does not see BPDUs for some duration. The possible values are Enable or Disable.
9. Use **Root Guard** to configure the root guard mode, which sets a port to discard any superior information received by the port and thus protect against root of the device from changing. The port gets put into discarding state and does not forward any packets. The possible values are Enable or Disable.
10. Use **Loop Guard** to configure the loop guard on the port to protect layer 2 forwarding loops. If loop guard is enabled, the port moves into the STP loop inconsistent blocking state instead of the listening/learning/forwarding state.
11. Use **TCN Guard** to configure the TCN guard for a port restricting the port from propagating any topology change information received through that port. The possible values are Enable or Disable.
12. Use **Port Mode** to enable/disable Spanning Tree Protocol Administrative Mode associated with the port or port channel. The possible values are Enable or Disable.

Table 3-56.

Field	Description
Auto Calculated Port Path Cost	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost will be calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
Hello Timer	Displays the value of the parameter for the CST.
Auto Calculated External Port Path Cost	Displays whether the external path cost is automatically calculated (Enabled) or not (Disabled). External Path cost will be calculated based on the link speed of the port if the configured value for External Port Path Cost is zero.
BPDU Guard Effect	Display the BPDU Guard Effect, it disables the edge ports that receive BPDU packets. The possible values are Enable or Disable.
Port Forwarding State	The Forwarding State of this port.

## 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 screenshot shows the 'CST Port Status' page for switch GSM73525. The page has a navigation menu on the left with options like System, Switching, Routing, QoS, Security, Monitoring, Maintenance, and Help. The main content area displays a table of port status information. The table has 12 columns: Interface, Port ID, Port Forwarding Mode, Port Role, Designated Root, Designated Cost, Designated Bridge, Designated Port, Topology Change Advertisement, Edge Port, Forward as Root MAC, CST Regional Root, CST Path Cost, and Port Up Time (seconds). The table lists 24 ports, all of which are in the 'Forwarding' state. The 'Port Up Time' column shows values ranging from 0 to 2,000,000 seconds.

Interface	Port ID	Port Forwarding Mode	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port	Topology Change Advertisement	Edge Port	Forward as Root MAC	CST Regional Root	CST Path Cost	Port Up Time (seconds)
1/5/1	80-01	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/2	80-02	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/3	80-03	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/4	80-04	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/5	80-05	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/6	80-06	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/7	80-07	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/8	80-08	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/9	80-09	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/10	80-10	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/11	80-11	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/12	80-12	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/13	80-13	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/14	80-14	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/15	80-15	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/16	80-16	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/17	80-17	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/18	80-18	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/19	80-19	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/20	80-20	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/21	80-21	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/22	80-22	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/23	80-23	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec
1/5/24	80-24	Forwarding	Forwarding	80-00-00-00-00-00-00-00	0	80-00-00-00-00-00-00-00	80-00	True	Enabled	True	80-00-00-00-00-00-00-00	0	2 day 2 hr 8 min 28 sec

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

**Table 3-57.**

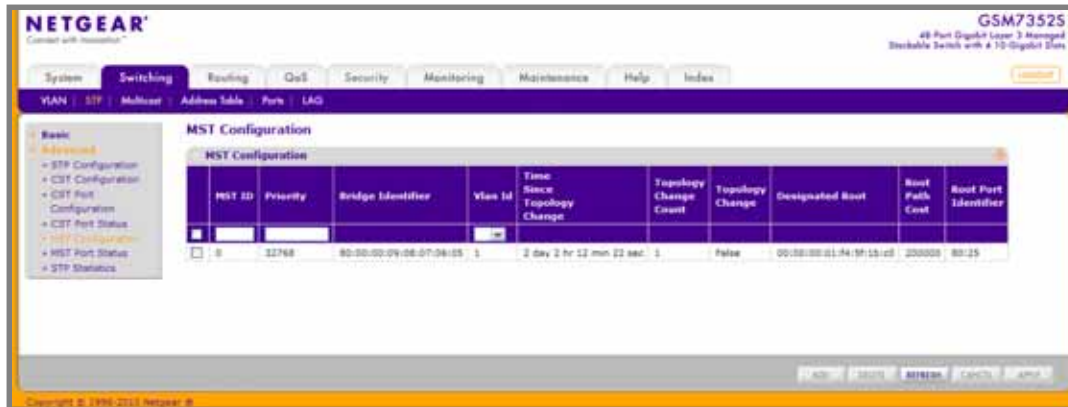
Field	Description
Interface	Identify the physical or port channel interfaces associated with VLANs associated with the CST.
Port ID	The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
Port Forwarding State	The Forwarding State of this port.
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	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Topology Change Acknowledge	Identifies whether the next BPDU to be transmitted for this port would have the topology change acknowledgement flag set. It is either "True" or "False".
Edge port	Indicates whether the port is enabled as an edge port. It takes the value "Enabled" or "Disabled".
Point-to-point MAC	Derived value of the point-to-point status.
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
CST Path Cost	Path Cost to the CST Regional Root.
Port Up Time Since Counters Last Cleared	Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.



## 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**.



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. This is only visible when the select option of the MST ID select box is selected.
  - Priority** - Specifies the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. The default priority is 32768. The valid range is 0–61440.
  - VLAN ID** - This gives a combo box of each VLAN on the switch. These can be selected or unselected for re-configuring the association of VLANs to MST instances.
- 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.

**Table 3-58.**

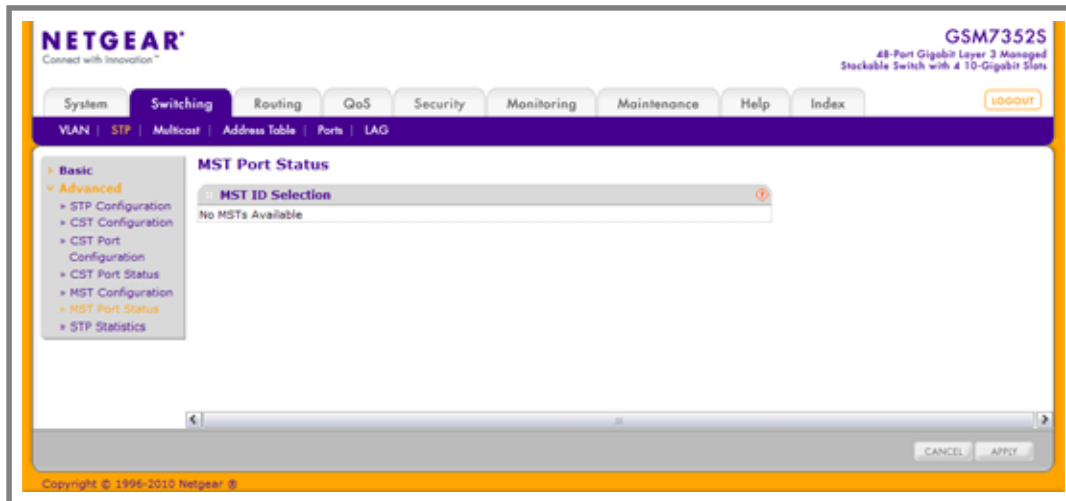
Field	Description
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time in seconds since the topology of the selected MST instance last changed.
Topology Change Count	Number of times topology has changed for the selected MST instance.
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 selected MST instance. It takes a value of 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 this MST instance.
Root PortIdentifier	Port to access the Designated Root for this MST instance.



## MST Port Status

Use the Spanning Tree MST Port Status 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**.




---

**Note:** If no MST instances have been configured on the switch, the page displays a “No MSTs Available” message and does not display the fields shown in the field description table that follows.

---

To configure MST port settings:

1. Use **MST ID** to select one MST instance from existing MST instances.
2. Use **Interface** to select one of the physical or port channel interfaces associated with VLANs associated with the selected MST instance.
3. Use **Port Priority** to specify the priority for a particular port within the selected MST instance. The port priority is set in multiples of 16. For example if the priority is attempted to be set to any value between 0 and 15, it will be set to 0. If it is tried to be set to any value between 16 and  $(2 \times 16 - 1)$  it will be set to 16 and so on.
4. Use **Port Path Cost** to set the Path Cost to a new value for the specified port in the selected MST instance. It takes a value in the range of 1 to 200000000.

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

**Table 3-59.**

Field	Description
Auto Calculated Port Path Cost	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost will be 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 Uptime Since Last Clear Counters	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. The possible values are Enable or Disable.
Port Forwarding State	The Forwarding State of this port.
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	Path Cost offered to the LAN by the Designated Port.
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.

## 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**.

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

VLAN | **STP** | Multicast | Address Table | Ports | LAG

> Basic  
 > **Advanced**  
   > STP Configuration  
   > CST Configuration  
   > CST Port Configuration  
   > CST Port Status  
   > MST Configuration  
   > MST Port Status  
   > **STP Statistics**

### STP Statistics

1 LAGS All

Interface	STP BPDUs Received	STP BPDUs Transmitted	RSTP BPDUs Received	RSTP BPDUs Transmitted	MSTP BPDUs Received	MSTP BPDUs Transmitted
1/0/1	0	0	0	0	0	0
1/0/2	0	0	0	0	0	0
1/0/3	0	0	0	0	0	0
1/0/4	0	0	0	0	0	0
1/0/5	0	0	0	0	0	0
1/0/6	0	0	0	0	0	0
1/0/7	0	0	0	0	0	0
1/0/8	0	0	0	0	0	0
1/0/9	0	0	0	0	0	0
1/0/10	0	0	0	0	0	0
1/0/11	0	0	0	0	0	0
1/0/12	0	0	0	0	0	0
1/0/13	0	0	0	0	0	0
1/0/14	0	0	0	0	0	0
1/0/15	0	0	0	0	0	0
1/0/16	0	0	0	0	0	0
1/0/17	0	0	0	0	0	0
1/0/18	0	0	0	0	0	0

REFRESH

Copyright © 1996-2010 Netgear, Inc.

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

**Table 3-60.**

Field	Description
Interface	Selects one of the physical or port channel interfaces of the switch.
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.

## 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 168
- [IGMP Snooping](#) on page 172
- [MLD Snooping](#) on page 184

## MFDB

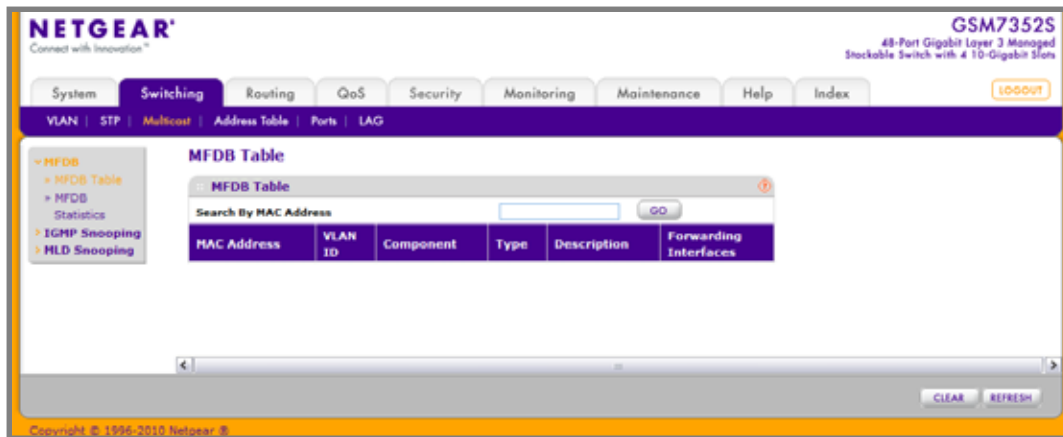
From the MFDB link, you can access the following pages:

- [MFDB Table](#) on page 169
- [MFDB Statistics](#) on page 171

## MFDB Table

The Multicast Forwarding Database holds the port membership information for all active multicast address entries. The key for an entry consists of a VLAN ID and MAC address pair. Entries may contain data for more than one protocol.

To display the MFDB Table page, click **Switching > Multicast > MFDB > MFDB Table**.



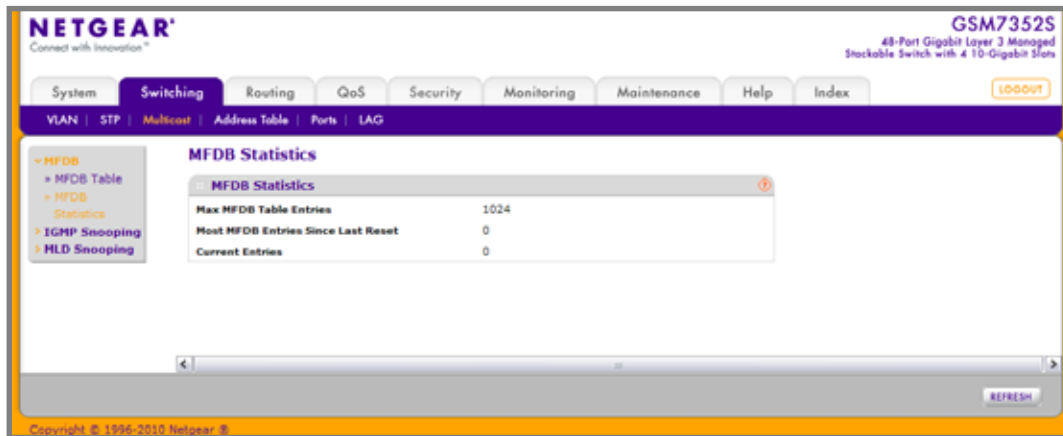
1. Use **Search by MAC Address** to enter a MAC Address whose MFDB table entry you want displayed. Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67. Then click on the “GO” button. If the address exists, that entry will be displayed. An exact match is required.

**Table 3-61.**

Field	Description
MAC Address	The multicast MAC address for which you requested data.
VLAN ID	The VLAN ID to which the multicast MAC address is related.
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.
Component	This is the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, Static Filtering and MLD Snooping.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
ForwardingInterfaces	The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

## MFDB Statistics

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



**Table 3-62.**

Field	Description
Max MFDB Table Entries	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 last reset. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the Multicast Forwarding Database table.

## 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.

From the IGMP Snooping link, you can access the following pages:

- [IGMP Snooping Configuration](#) on page 173
- [IGMP Snooping Interface Configuration](#) on page 174
- [IGMP VLAN Configuration](#) on page 176
- [Multicast Router Configuration](#) on page 178
- [Multicast Router VLAN Configuration](#) on page 179
- [IGMP Snooping Querier](#) on page 180
  - [IGMP Snooping Querier Configuration](#) on page 180
  - [IGMP Snooping Querier VLAN Configuration](#) on page 182

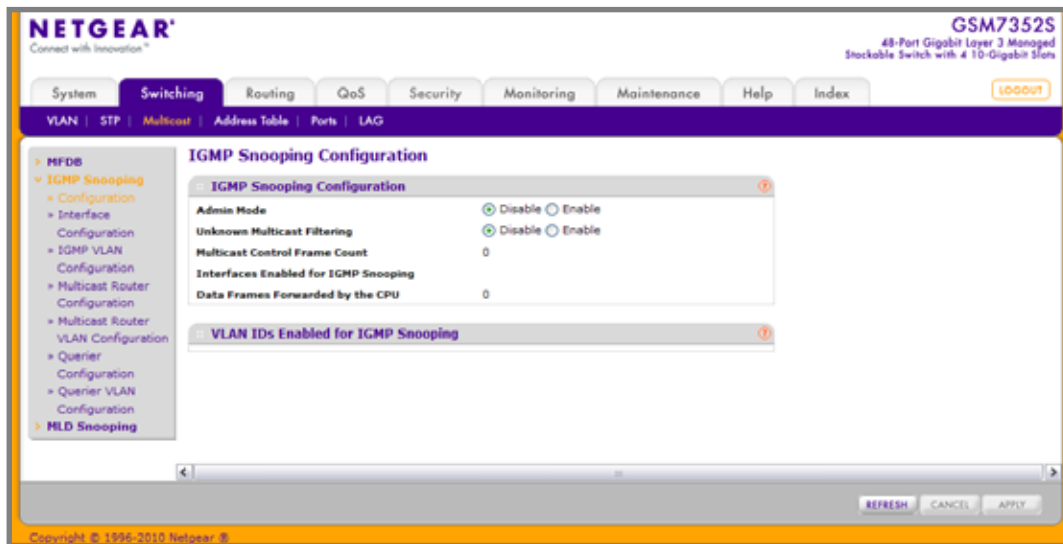


## IGMP Snooping Configuration

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

Note that only a user with Read/Write access privileges may change the data on this screen.

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



To configure IGMP Snooping:

1. Use the **Admin Mode** Enable/Disable radio button to select the administrative mode for IGMP Snooping for the switch. The default is disable.
2. Use the **Unknown Multicast Filtering** Enable/Disable radio button to select the unknown multicast filtering mode for the switch. The default is disable.

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

**Table 3-63.**

Field	Description
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interfaces Enabled for IGMP Snooping	A list of all the interfaces currently enabled for IGMP Snooping.
Data Frames Forwarded by the CPU	The number of data frames forwarded by the CPU.
VLAN Ids Enabled For IGMP Snooping	Displays VLAN Ids enabled for IGMP snooping.

## 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** > **Interface Configuration**.

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

System Switching Routing QoS Security Monitoring Maintenance Help Index

VLAN STP Multicast Address Table Ports LAG

**IGMP Snooping Interface Configuration**

1 LAGS All Go To Interface  GO

Interface	Admin Mode	Group Membership Interval(secs)	Max Response Time(secs)	Present Expiration Time(secs)	Fast Leave Admin Mode
<input type="checkbox"/> 1/0/1	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/2	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/3	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/4	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/5	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/6	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/7	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/8	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/9	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/10	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/11	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/12	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/13	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/14	Disable	260	10	0	Disable
<input type="checkbox"/> 1/0/15	Disable	260	10	0	Disable

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

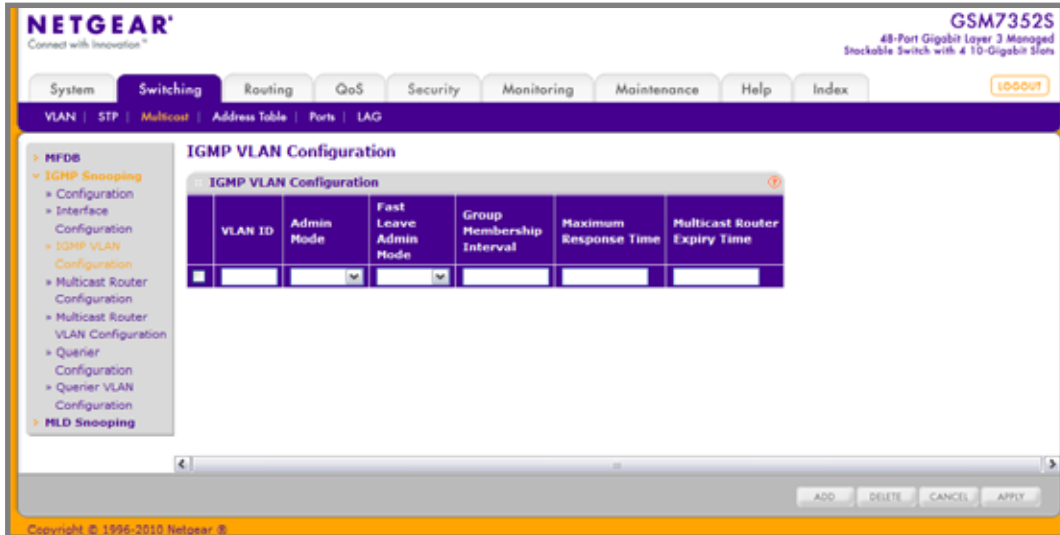
To configure IGMP Snooping interface settings:

1. **Interface:** Lists all physical, VLAN, and LAG interfaces. Select the interface you want to configure.
2. Use **Admin Mode** to select the interface mode for the selected interface for IGMP Snooping for the switch from the pull-down menu. The default is disable.
3. Use **Group Membership Interval** 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. Enter a value between 1 and 3600 seconds. The default is 260 seconds.
4. Use **Max Response Time** 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.
5. Use **Present Expiration Time** 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 time-out, i.e. no expiration.
6. Use **Fast Leave Admin** mode to select the Fast Leave mode for the a particular interface from the pull-down menu. The default is disable.
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 configuration changes, click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

## IGMP 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 VLAN Configuration**.



**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

System Switching Routing QoS Security Monitoring Maintenance Help Index

VLAN STP Multicast Address Table Ports LAG

**IGMP VLAN Configuration**

VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

ADD DELETE CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

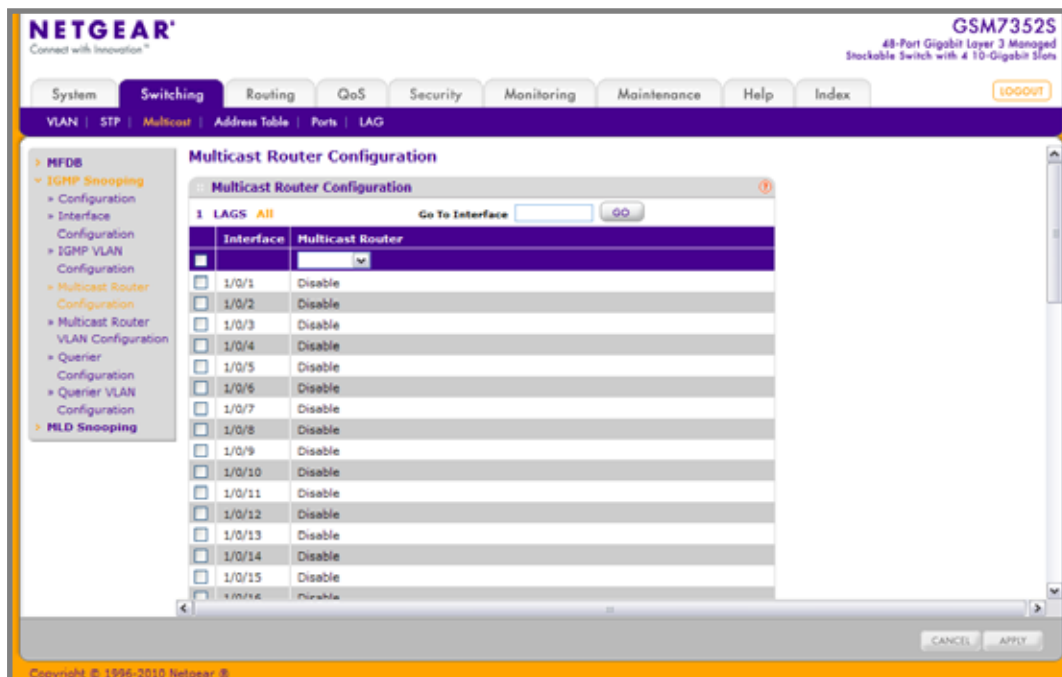
To configure IGMP snooping settings for VLANs:

1. To enable IGMP snooping on a VLAN, enter the VLAN ID in the appropriate field and configure the IGMP Snooping values:
  - Use **Admin Mode** to enable or disable IGMP Snooping for the specified VLAN ID.
  - Use **Fast Leave Admin Mode** to enable or disable the IGMP Snooping Fast Leave Mode for the specified VLAN ID.
  - Use **Group Membership Interval** to set the value for group membership interval of IGMP Snooping for the specified VLAN ID. Valid range is (Maximum Response Time + 1) to 3600 seconds.
  - Use **Maximum Response Time** to set the value for maximum response time of IGMP Snooping for the specified VLAN ID. Valid range is 1 to (Group Membership Interval - 1). Its value should be greater than group membership interval value.
  - Use **Multicast Router Expiry Time** to set the value for multicast router expiry time of IGMP Snooping for the specified VLAN ID. Valid range is 0 to 3600 seconds.
2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. To 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**.
5. 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 Configuration

This page configures the interface as the one the multicast router is attached to. All IGMP packets snooped by the switch will be forwarded to the multicast router reachable from this interface. The configuration is not needed most of the time since the switch will automatically detect the presence of multicast router and forward IGMP packet accordingly. It is only needed when you want to make sure the multicast router always receives IGMP packets from the switch in a complex network.

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

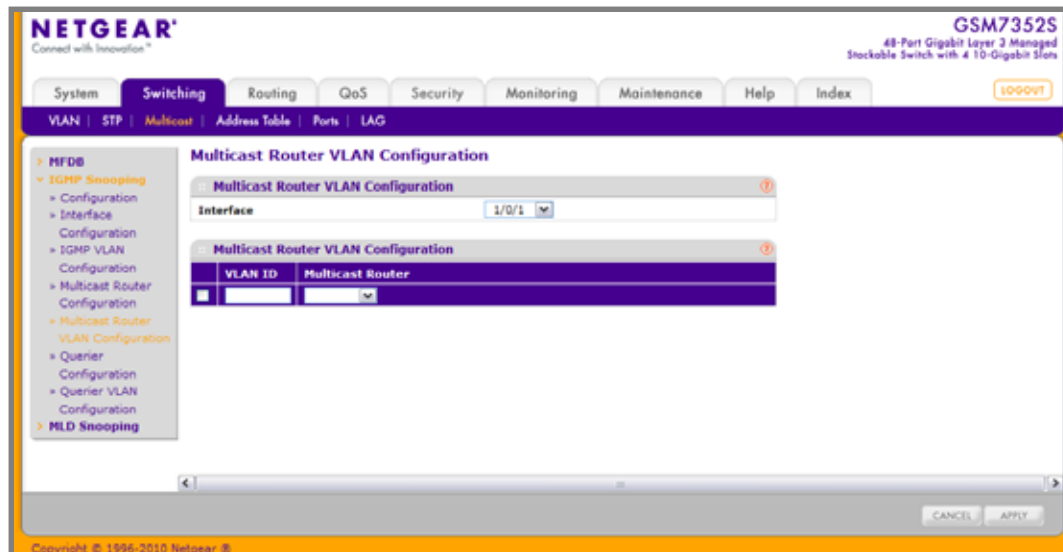


1. Use **Interface** to select the physical interface for which you want Multicast Router to be enabled.
2. Use **Multicast Router** to enable or disable Multicast Router on the selected interfaces.

## Multicast Router VLAN Configuration

This page configures the interface to only forward the snooped IGMP packets that come from VLAN ID (<vlanId>) to the multicast router attached to this interface. The configuration is not needed most of the time since the switch will automatically detect the presence of a multicast router and forward IGMP packets accordingly. It is only needed when you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

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



1. Use **Interface** to select the interface for which you want Multicast Router to be enabled or to be displayed.
2. Use **VLAN ID** to select the VLAN ID for which the Multicast Router Mode is to be Enabled or Disabled.
3. Use **Multicast Router** to enable or disable multicast router for the Vlan ID.

## 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.

### IGMP Snooping Querier Configuration

Use this menu to configure the parameters for IGMP Snooping Querier. Note that only a user with Read/Write access privileges may change the data on this screen.

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

The screenshot displays the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual interface. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar shows a tree view with categories like MFD, IGMP Snooping, and MLD Snooping. The main content area is titled "IGMP Snooping Querier Configuration" and contains the following fields:

- Querier Admin Mode:** Radio buttons for Disable (selected) and Enable.
- Querier IP Address:** Text field with value 0.0.0.0.
- IGMP Version:** Text field with value 2.
- Query Interval(secs):** Text field with value 60, with a range of (1 to 1800).
- Querier Expiry Interval(secs):** Text field with value 60, with a range of (60 to 300).

Below the configuration fields, there is a section titled "VLAN Ids Enabled for IGMP Snooping Querier" with a red information icon. At the bottom of the page, there are "CANCEL" and "APPLY" buttons.



To configure IGMP Snooping Querier settings:

1. Use **Querier Admin Mode** to select the administrative mode for IGMP Snooping for the switch. The default is disable.
2. Use **Querier IP Address** to specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.
3. Use **IGMP Version** to specify the IGMP protocol version used in periodic IGMP queries. IGMP queries.
4. Use **Query Interval(secs)** to specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
5. Use **Querier Expiry Interval(secs)** to specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

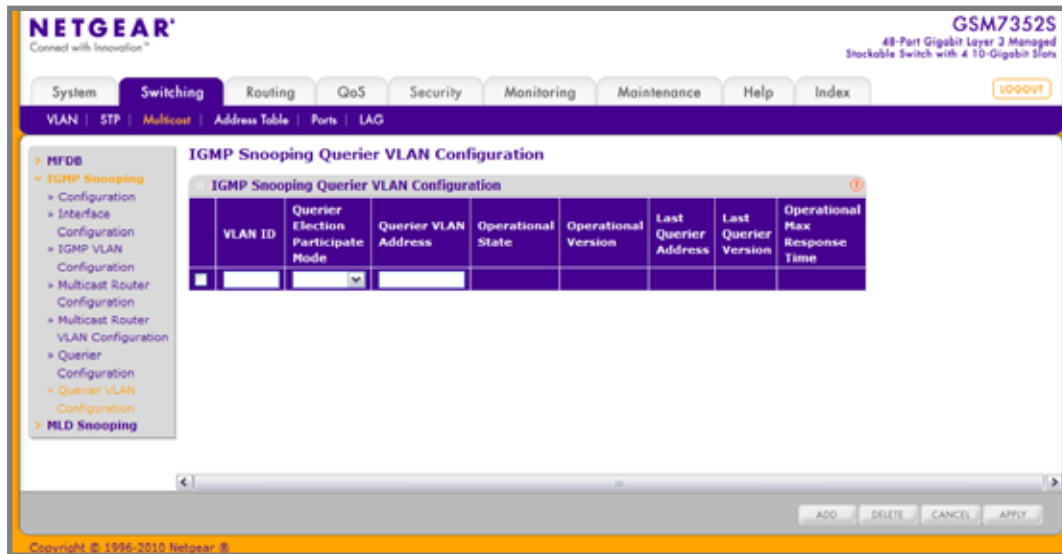
**Table 3-64.**

Field	Description
VLAN Ids Enabled For IGMP Snooping Querier	Displays VLAN Ids enabled for IGMP snooping querier.

## 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 VLAN Configuration**.



To configure Querier VLAN settings:

- To create a new VLAN ID for IGMP Snooping, select New Entry from the VLAN ID field and complete the following fields. User can also set pre-configurable Snooping Querier parameters.
  - 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.
- Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.
- To disable Snooping Querier on a VLAN, select the VLAN ID 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.
- Click **Refresh** to update the page with the latest information from the switch.

Table 3-65.

Field	Description
Operational State	<p>Displays the operational state of the IGMP Snooping Querier on a VLAN. It can be in any of the following states:</p> <ul style="list-style-type: none"> <li>• Querier: 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 in the VLAN, it moves to non-querier mode.</li> <li>• Non-Querier: Snooping switch is in Non-Querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch will move into querier mode.</li> <li>• Disabled: Snooping Querier is not operational on the VLAN. The Snooping Querier moves to disabled mode when IGMP Snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.</li> </ul>
Operational Version	Displays the operational IGMP protocol version of the 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 maximum response time to be used in the queries that are sent by the Snooping Querier.

## MLD Snooping

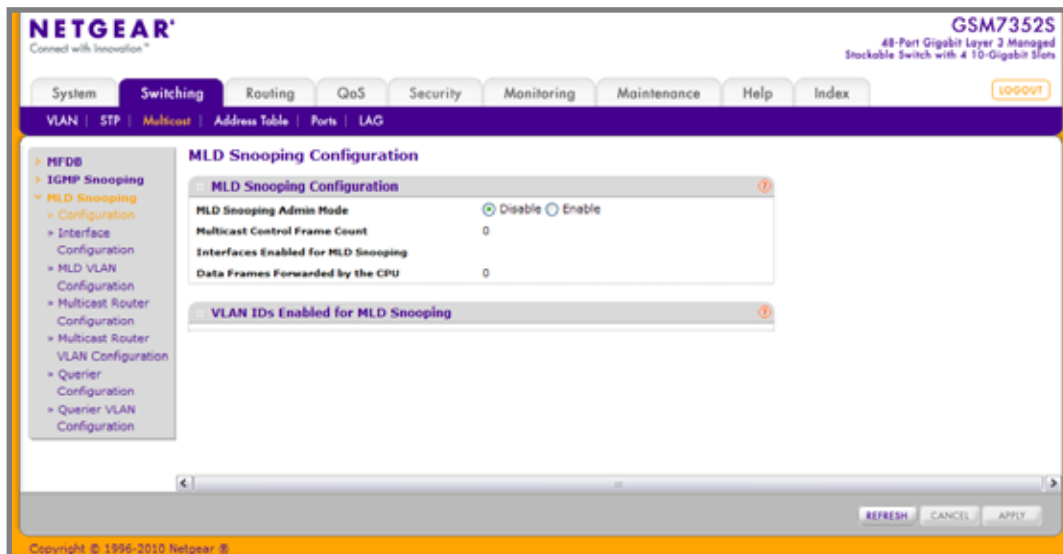
From the MLD Snooping link, you can access the following pages:

- [\*MLD Snooping Configuration\*](#) on page 185
- [\*MLD Snooping Interface Configuration\*](#) on page 186
- [\*MLD VLAN Configuration\*](#) on page 187
- [\*Multicast Router Configuration\*](#) on page 188
- [\*Multicast Router VLAN Configuration\*](#) on page 189
- [\*MLD Snooping Querier Configuration\*](#) on page 190
- [\*MLD Snooping Querier VLAN Configuration\*](#) on page 191

## MLD Snooping Configuration

Use this menu to configure the parameters for MLD Snooping, which is used to build forwarding lists for multicast traffic. Note that only a user with Read/Write access privileges may change the data on this screen.

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



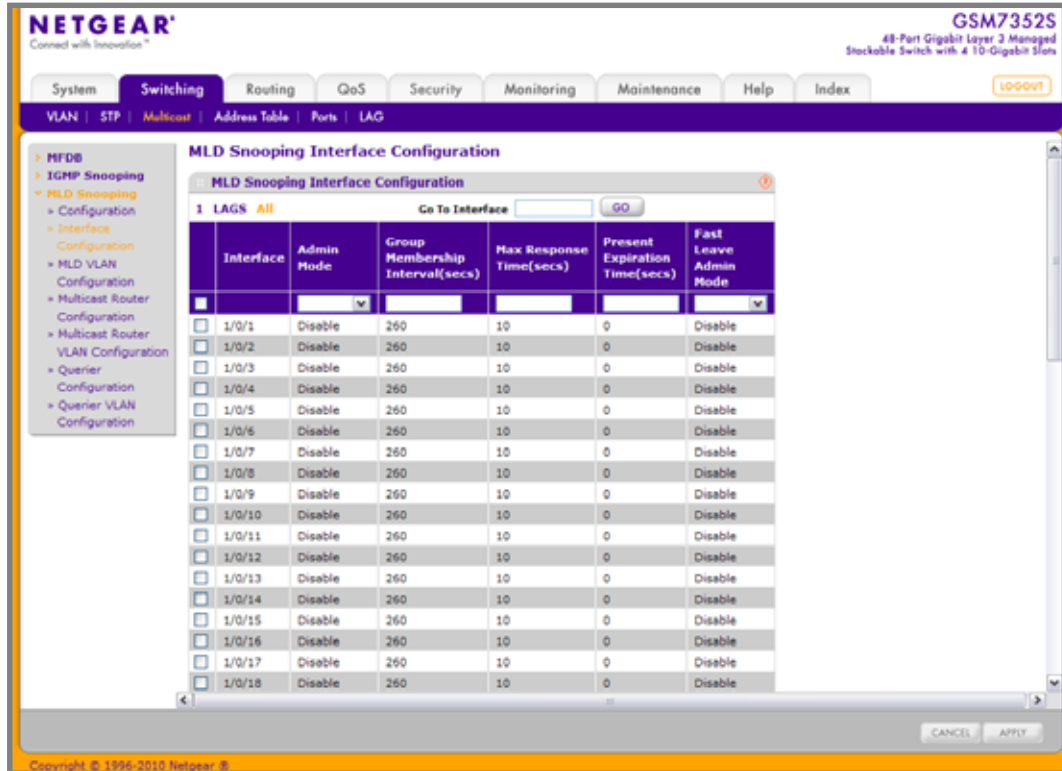
1. Use **MLD Snooping Admin Mode** to select the administrative mode for MLD Snooping for the switch. The default is disable.

**Table 3-66.**

Field	Definition
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interfaces Enabled for MLD Snooping	A list of all the interfaces currently enabled for MLD Snooping.
Data Frames Forwarded by the CPU	The number of data frames forwarded by the CPU.
VLAN Ids Enabled For MLD Snooping	Displays VLAN Ids enabled for MLD snooping.

## MLD Snooping Interface Configuration

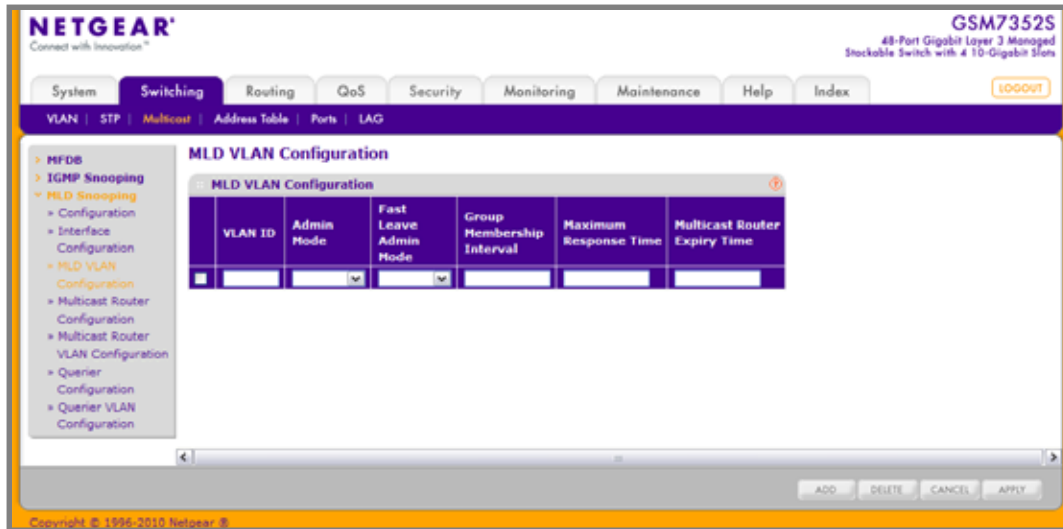
To access the MLD Snooping Interface Configuration page, click **Switching > Multicast > MLD Snooping > Interface Configuration**.



1. **Interface** - Displays all physical, VLAN, and LAG interfaces. Select the interface you want to configure.
2. Use **Admin Mode** to select the interface mode for the selected interface for MLD Snooping for the switch. The default is disable.
3. Use **Group Membership Interval(secs)** 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.
4. Use **Max Response Time(secs)** 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.
5. Use **Present Expiration Time** 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 time-out, i.e. no expiration.
6. Use **Fast Leave Admin mode** to select the Fast Leave mode for the a particular interface from the pull-down menu. The default is disable.

## MLD VLAN Configuration

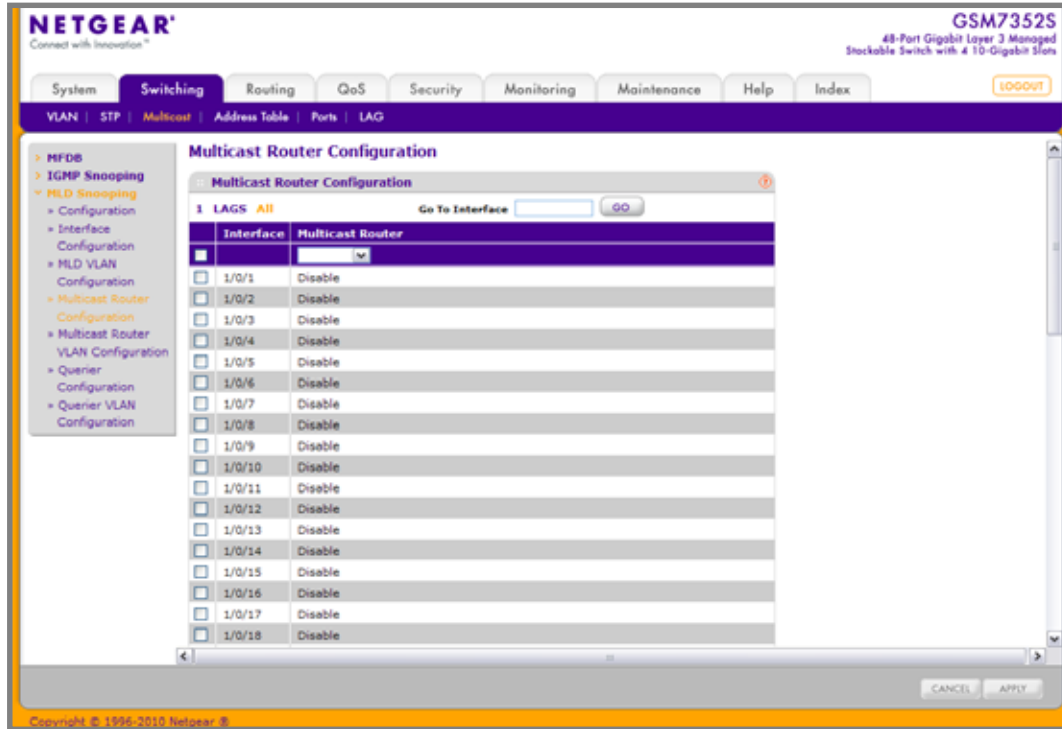
To access the MLD VLAN Configuration page, click **Switching** > **Multicast** > **MLD Snooping** > **MLD VLAN Configuration**.



1. Use **VLAN ID** to set the VLAN IDs for which MLD Snooping is enabled.
2. Use **Admin Mode** to enable MLD Snooping for the specified VLAN ID.
3. Use **Fast Leave Admin Mode** to enable or disable the MLD Snooping Fast Leave Mode for the specified VLAN ID.
4. Use **Group Membership Interval** 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 **Maximum Response Time** to set the value for maximum response time of MLD Snooping for the specified VLAN ID. Valid range is 1 to (Group Membership Interval - 1). Its value should be less than group membership interval value.
6. Use **Multicast Router Expiry Time** to set the value for multicast router expiry time of MLD Snooping for the specified VLAN ID. Valid range is 0 to 3600.

## Multicast Router Configuration

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

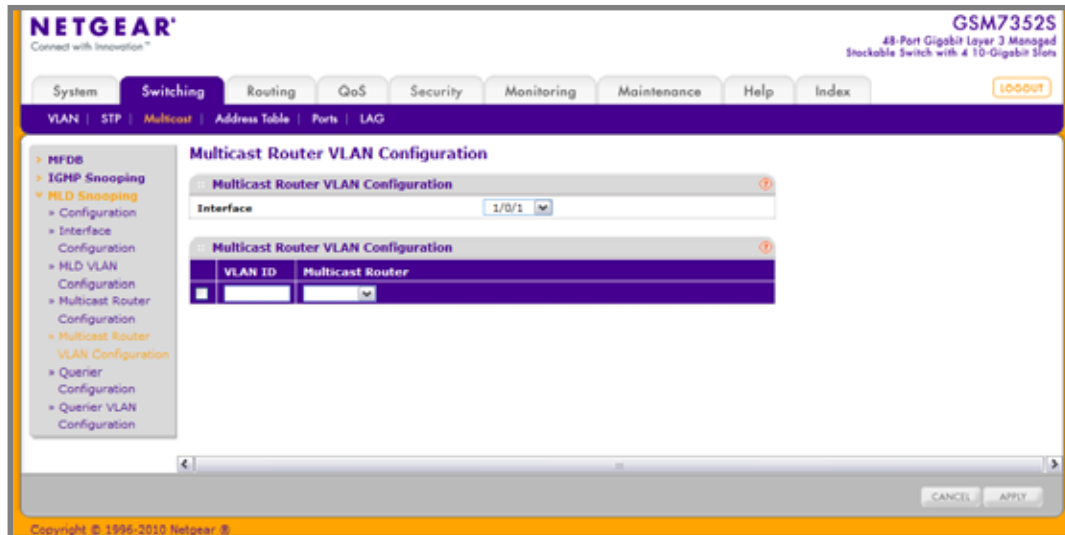


1. Interface: Select the interface for which you want Multicast Router to be enabled.
2. Use **Multicast Router** to enable or disable Multicast Router on the selected interface.



## Multicast Router VLAN Configuration

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

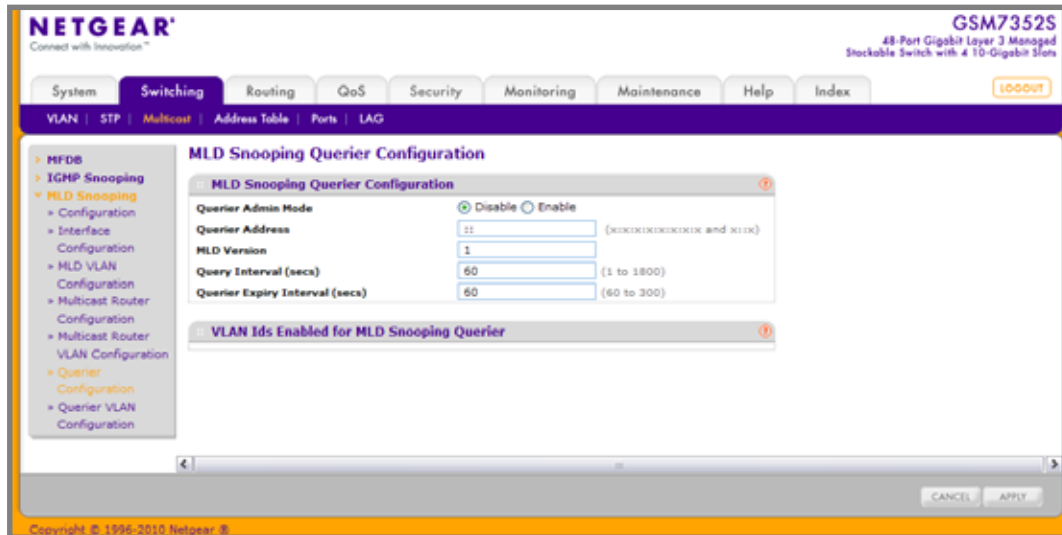


1. Use **Interface** to select the interface for which you want Multicast Router to be enabled.
2. Use **VLAN ID** to select the VLAN ID for which the Multicast Router Mode is to be Enabled or Disabled.
3. Use **Multicast Router** to enable or disable the multicast router for the Vlan ID.

## MLD Snooping Querier Configuration

Use this menu to configure the parameters for MLD Snooping Querier. Note that only a user with Read/Write access privileges may change the data on this screen.

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



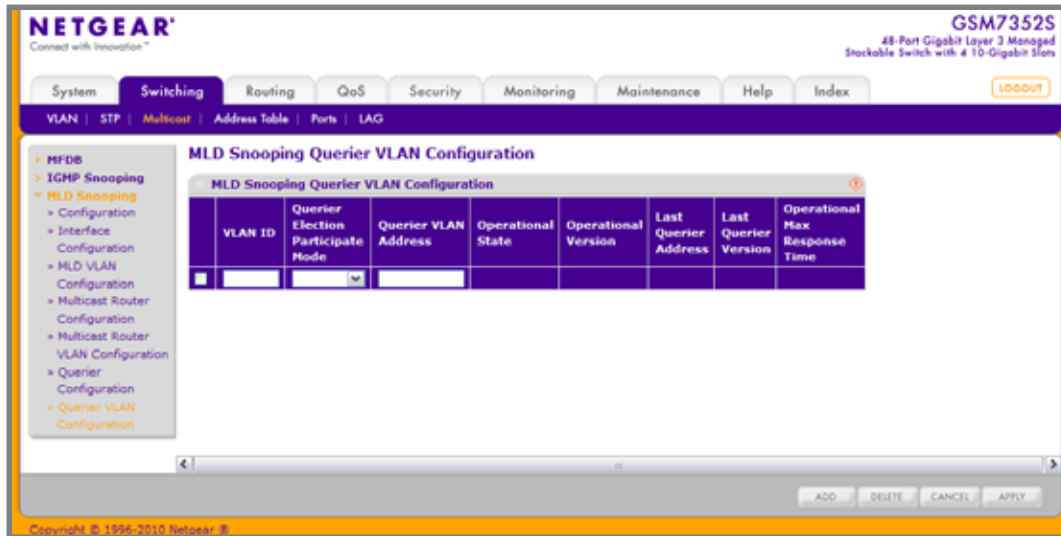
1. Use **Querier Admin Mode** to select the administrative mode for MLD Snooping for the switch. The default is disable.
2. Use **Querier Address** to specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent. The supported IPv6 formats are x:x:x:x:x:x:x and x::x.
3. Use **MLD Version** to specify the MLD protocol version used in periodic MLD queries.
4. Use **Query Interval(secs)** to specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
5. Use **Querier Expiry Interval(secs)** to specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

Table 3-67.

Field	Description
VLAN Ids Enabled For MLD Snooping Querier	Displays VLAN Ids enabled for MLD snooping querier.

## MLD Snooping Querier VLAN Configuration

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



1. **VLAN ID** - Specifies the VLAN ID on which MLD Snooping Querier is administratively enabled and VLAN exists in the VLAN database.
2. Use **Querier Election Participate Mode** to enable or disable the MLD Snooping Querier participate in election mode. When this mode is disabled, upon seeing other querier of same version in the vlan, the snooping querier moves to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where the lowest ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
3. Use **Querier VLAN Address** to specify the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.

Table 3-68.

Field	Description
Operational State	<p>Specifies the operational state of the MLD Snooping Querier on a VLAN. It can be in any of the following states:</p> <ul style="list-style-type: none"> <li>• Querier: 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 in the VLAN, it moves to non-querier mode.</li> <li>• Non-Querier: Snooping switch is in Non-Querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch will move into querier mode.</li> <li>• Disabled: 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.</li> </ul>
Operational Version	Displays the operational MLD protocol version of the 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 maximum response time to be used in the queries that are sent by the Snooping Querier.

## Address Table

From the Address Table link, you can access the following pages:

- [Basic](#) on page 192
- [Advanced](#) on page 195

## Basic

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

- [Address Table](#) on page 193

## Address Table

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

To display the Address Table page, click **Switching > Address Table > Basic > Address Table**.

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

System Switching Routing QoS Security Monitoring Maintenance Help Index

VLAN STP Multicast Address Table Ports LAG

Basic  
Address Table  
Advanced

### Address Table

MAC Address Table

Search By: VLAN ID  GO

Total MAC Addresses: 47

VLAN ID	MAC Address	Port	Status
1	00:00:EB:9A:59:6C	1/0/37	Learned
1	00:01:02:03:04:00	1/0/37	Learned
1	00:01:03:05:07:0B	1/0/37	Learned
1	00:01:F4:32:81:40	1/0/37	Learned
1	00:01:F4:32:81:90	1/0/37	Learned
1	00:01:F4:5F:1B:C0	1/0/37	Learned
1	00:01:F4:5F:1B:D1	1/0/37	Learned
1	00:01:F4:5F:1F:20	1/0/37	Learned
1	00:01:F4:5F:1F:3B	1/0/37	Learned
1	00:02:BC:00:7F:2B	1/0/37	Learned
1	00:02:BC:00:96:C0	1/0/37	Learned
1	00:02:E3:4B:F3:6F	1/0/37	Learned
1	00:04:5A:6D:E0:14	1/0/37	Learned
1	00:06:29:56:94:80	1/0/37	Learned
1	00:09:08:07:06:05	0/5/1	Management
1	00:0B:C0:67:C1:54	1/0/37	Learned
1	00:0F:FE:00:91:99	1/0/37	Learned

CLEAR REFRESH CANCEL

Copyright © 1996-2010 Netgear, Inc.

1. Use **Search By** to search for MAC Addresses by MAC Address, VLAN ID, and port:
  - **Searched by MAC Address** - Select MAC Address from pull-down menu, enter the 6 byte hexadecimal MAC Address in two-digit groups separated by colons, for example 01:23:45:67:89:AB. Then click on the “Go” button. If the address exists, that entry will be displayed as the first entry followed by the remaining (greater) mac addresses. An exact match is required.
  - **Searched by VLAN ID** - Select VLAN ID from pull-down menu, enter the VLAN ID, for example 100. Then click on the “Go” button. If the address exists, the entry will be displayed as the first entry followed by the remaining (greater) mac addresses.
  - **Searched by Port** - Select Port from pull-down menu, enter the port ID in Unit/Slot/Port, for example 2/1/1. Then click on the “Go” button. If the address exists, the entry will be displayed as the first entry followed by the remaining (greater) mac addresses.

Table 3-69.

Field	Description
Total MAC Address	Displaying the number of total MAC addresses learned or configured.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a 6 byte MAC Address that is separated by colons, for example 01:23:45:67:89:AB.
VLAN ID	The VLAN ID associated with the MAC Address.
Port	The port upon which this address was learned.
Status	<p>The status of this entry. The meanings of the values are:</p> <ul style="list-style-type: none"> <li>• Static: the value of the corresponding instance was added by the system or a user and cannot be relearned.</li> <li>• Learned: the value of the corresponding instance was learned, and is being used.</li> <li>• Management: the value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress.</li> </ul>

## Advanced

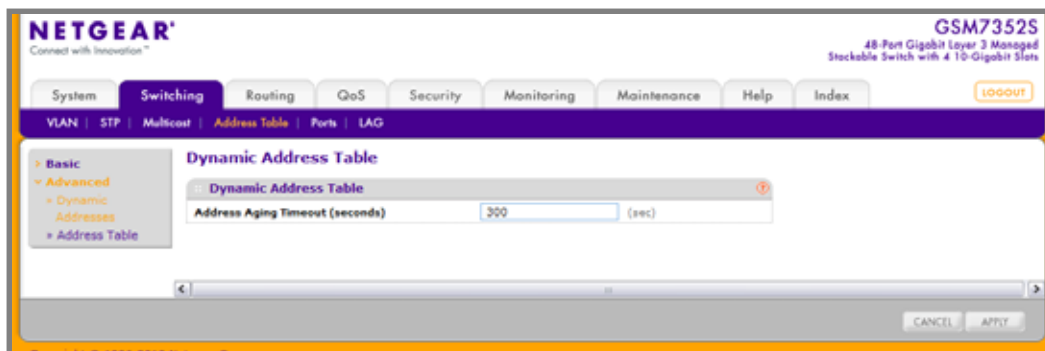
From the Advanced link, you can access the following pages:

- [Dynamic Addresses](#) on page 195
- [Address Table](#) on page 196

### Dynamic Addresses

This page allows the user to set the Address Aging Interval for the specified forwarding database.

To display the Address Table page, click **Switching > Address Table> Advanced > Dynamic Addresses**.

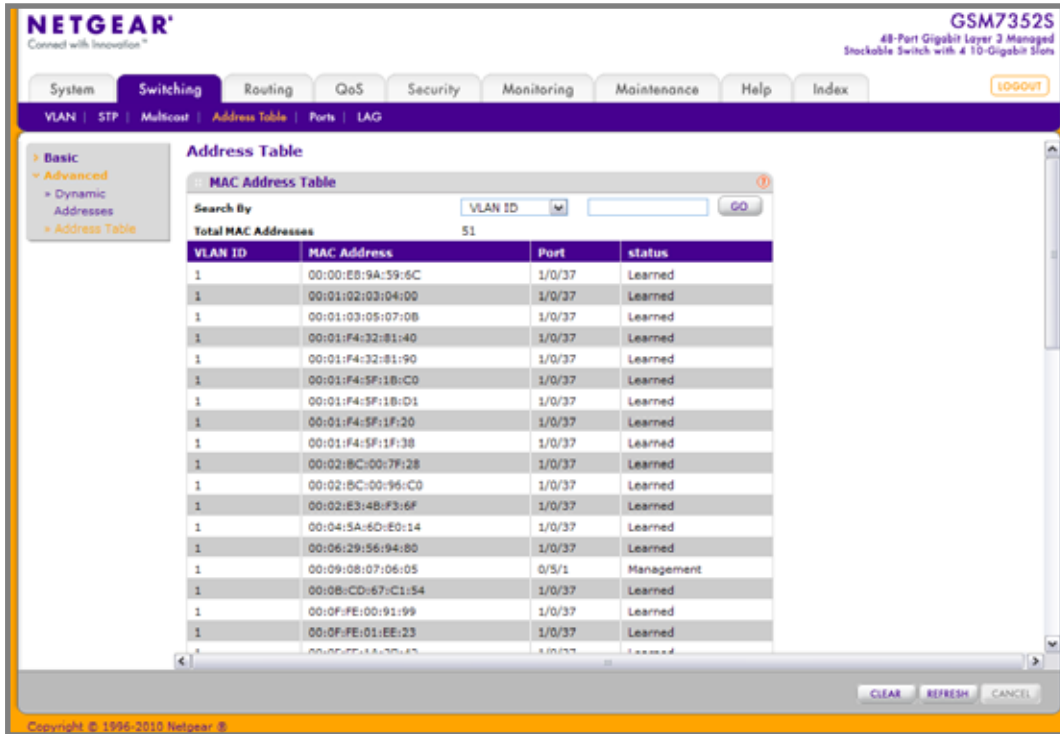


1. Use **Address Aging Timeout (seconds)** to specify the time-out period in seconds for aging out dynamically learned forwarding information. 802.1D-1990 recommends a default of 300 seconds. The value may be specified as any number between 10 and 1000000 seconds. The factory default is 300.

## Address Table

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

To display the Address Table page, click **Switching > Address Table > Advanced > Address Table**.



The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual interface. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The left sidebar shows a tree view with Basic, Advanced, Dynamic Addresses, and Address Table. The main content area displays the Address Table page, which includes a search bar and a table of MAC addresses.

**Address Table**

MAC Address Table

Search By: VLAN ID  GO

Total MAC Addresses: 51

VLAN ID	MAC Address	Port	Status
1	00:00:EB:9A:39:6C	1/0/37	Learned
1	00:01:02:03:04:00	1/0/37	Learned
1	00:01:03:05:07:0B	1/0/37	Learned
1	00:01:F4:32:81:40	1/0/37	Learned
1	00:01:F4:32:81:90	1/0/37	Learned
1	00:01:F4:5F:1B:C0	1/0/37	Learned
1	00:01:F4:5F:1B:D1	1/0/37	Learned
1	00:01:F4:5F:1F:20	1/0/37	Learned
1	00:01:F4:5F:1F:38	1/0/37	Learned
1	00:02:BC:00:7F:28	1/0/37	Learned
1	00:02:BC:00:96:C0	1/0/37	Learned
1	00:02:E3:4B:F3:6F	1/0/37	Learned
1	00:04:5A:6D:E0:14	1/0/37	Learned
1	00:06:29:56:94:80	1/0/37	Learned
1	00:09:08:07:06:05	0/5/1	Management
1	00:0B:CD:67:C1:54	1/0/37	Learned
1	00:0F:FE:00:91:99	1/0/37	Learned
1	00:0F:FE:01:EE:23	1/0/37	Learned
1	00:0F:FE:01:EE:23	1/0/37	Learned

CLEAR REFRESH CANCEL

Copyright © 1996-2010 Netgear, Inc.



1. Use **Search By** to search for MAC Addresses by MAC Address, VLAN ID, and port.
  - **Searched by MAC Address** - Select MAC Address from pull-down menu, enter the 6 byte hexadecimal MAC Address in two-digit groups separated by colons, for example 01:23:45:67:89:AB. Then click on the “Go” button. If the address exists, that entry will be displayed as the first entry followed by the remaining (greater) mac addresses. An exact match is required.
  - **Searched by VLAN ID** - Select VLAN ID from pull-down menu, enter the VLAN ID, for example 100. Then click on the “Go” button. If the address exists, the entry will be displayed as the first entry followed by the remaining (greater) mac addresses.
  - **Searched by Port** - Select Port from pull-down menu, enter the port ID in Unit/Slot/Port, for example 2/1/1. Then click on the “Go” button. If the address exists, the entry will be displayed as the first entry followed by the remaining (greater) mac addresses.

Table 3-70.

Field	Description
Total MAC Address	Displaying the number of total MAC addresses learned or configured.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a 6 byte MAC Address that is separated by colons, for example 01:23:45:67:89:AB.
VLAN ID	The VLAN ID associated with the MAC Address.
Port	The port upon which this address was learned.
Status	<p>The status of this entry. The meanings of the values are:</p> <ul style="list-style-type: none"> <li>• Static: the value of the corresponding instance was added by the system or a user and cannot be relearned.</li> <li>• Learned: the value of the corresponding instance was learned, and is being used.</li> <li>• Management: the value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress.</li> </ul>

## Ports

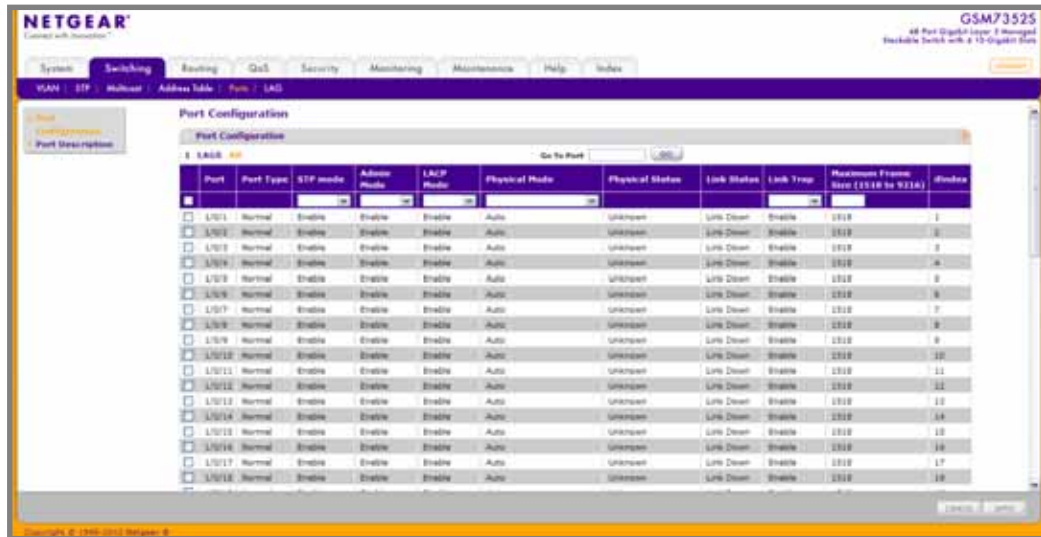
The pages on the Ports tab allow you to view and monitor the physical port information for the ports available on the switch. From the Ports link, you can access the following pages:

- [Port Configuration](#) on page 198
- [Port Description](#) on page 200

## 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. Use **Port** to select the interface for which data is to be displayed or configured.
2. Use **STP Mode** to select the Spanning Tree Protocol Administrative Mode for the port or LAG. The possible values are:
  - **Enable** -Select this to enable the Spanning Tree Protocol for this port.
  - **Disable** -Select this to disable the Spanning Tree Protocol for this port.
3. Use the **Admin Mode** pull-down menu to select the Port control administration state. You must select enable if you want the port to participate in the network. The factory default is enabled.
4. Use **LACP Mode** to select the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation. May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
5. Use the **Physical Mode** pull-down menu to select the port's speed and duplex mode. If you select auto the duplex mode and speed will be set by the auto-negotiation process. Note that the port's maximum capability (full duplex and speed) will be advertised. Otherwise, your selection will determine the port's duplex mode and transmission rate. The factory default is auto.
6. Use the **Link Trap object** to determine whether to send a trap when link status changes. The factory default is enabled.
7. Use **Maximum Frame Size** to specify the maximum Ethernet frame size the interface supports or is configured, including ethernet header, CRC, and payload (1518 to 9216). The default maximum frame size is 1518.

8. Click **CANCEL** to update the switch with the values you entered. If you want the switch to retain the new values across a power cycle you must perform a save.
9. Click **APPLY** to update the switch with the values you entered. If you want the switch to retain the new values across a power cycle you must perform a save.

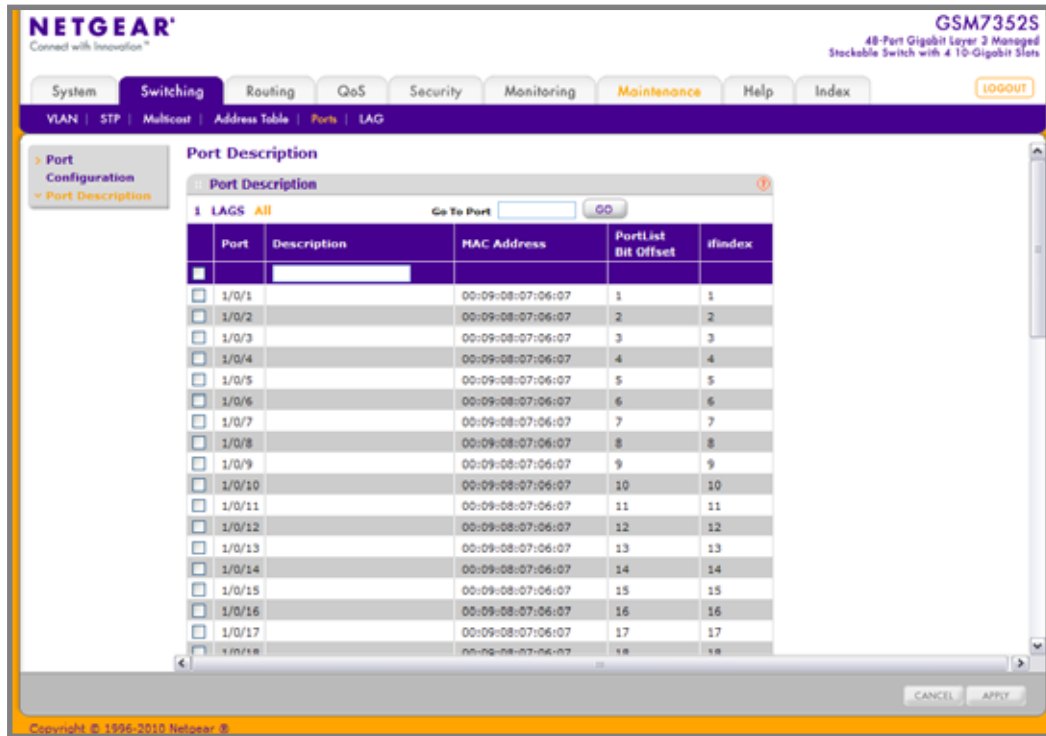
**Table 3-71.**

Field	Description
Port Type	For normal ports this field will be “normal.” Otherwise the possible values are: <ul style="list-style-type: none"><li>• Mirrored - The port is a mirrored port on which all the traffic will be copied to the probe port.</li><li>• Probe - Use this port to monitor mirrored port.</li><li>• Trunk Number - The port is a member of a Link Aggregation trunk. Look at the LAG screens for more information.</li></ul>
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the Link is up or down.
ifIndex	The ifIndex of the interface table entry associated with this port.

## Port Description

This screen configures and displays the description for all ports in the box.

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



1. Use **Port Description** to enter the description string to be attached to a port. It can be up to 64 characters in length.

**Table 3-72.**

Field	Description
Port	Selects the interface for which data is to be displayed or configured.
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	Displays the interface index associated with the port.

## 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. The LAG by default becomes a member of the management VLAN.

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

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LACPDUs. ProSafe® Managed Switches support up to 64 LAGs.

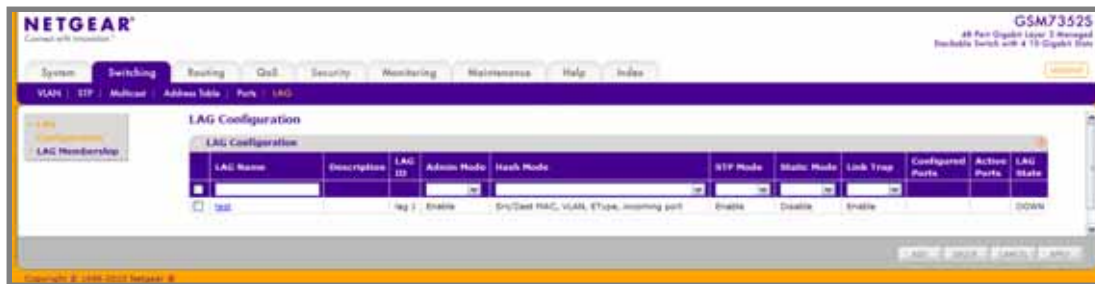
From the LAGs link, you can access the following pages:

- [LAG Configuration](#) on page 201
- [LAG Membership](#) on page 203

## 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 > LAG Configuration**.



To configure LAG settings:

1. Use **LAG Name** to enter the name you want assigned to the LAG. You may enter any string of up to 15 alphanumeric characters. A valid name has to be specified in order to create the LAG.
2. Use **Hash Mode** to select the load-balancing mode used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link:
  - **Src MAC,VLAN,EType,incoming port** - Source MAC, VLAN, EtherType, and incoming port associated with the packet.

- **Dest MAC,VLAN,EType,incoming port** -Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
  - **Src/Dest MAC,VLAN,EType,incoming port** - Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
  - **Src IP** and **Src TCP/UDP Port** fields - Source IP and Source TCP/UDP fields of the packet.
  - **Dest IP** and **Dest TCP/UDP Port** fields - Destination IP and Destination TCP/UDP Port fields of the packet.
  - **Src/Dest IP** and **TCP/UDP Port Fields** - Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
3. Use **Link Trap** to specify whether you want to have a trap sent when link status changes. The factory default is enable, which will cause the trap to be sent.
  4. Use **Admin Mode** to select enable or disable from the pull-down menu. When the LAG is disabled no traffic will flow and LACPDUs will be dropped, but the links that form the LAG will not be released. The factory default is enable.
  5. Use **STP Mode** to enable or disable the Spanning Tree Protocol Administrative Mode associated with the LAG. The possible values are:
    - **Disable** - Spanning tree is disabled for this LAG.
    - **Enable** - Spanning tree is enabled for this LAG.
  6. Use **Static Mode** to select enable or disable from the pull-down menu. When the LAG is enabled it does not transmit or process received LACPDUs i.e. the member ports do not transmit LACPDUs and all the LACPDUs it may receive are dropped. The factory default is disable.
  7. Click **DELETE** to remove the currently selected configured LAG. All ports that were members of this LAG are removed from the LAG and included in the default VLAN.

Table 3-73.

Field	Description
LAG Description	Enter the Description string to be attached to a LAG. It can be up to 64 characters in length.
LAG ID	Identification of the LAG.
LAG State	Indicates whether the Link is up or down.
Configured Ports	Indicate the ports that are members of this port-channel
Active Ports	Indicates the ports that are actively participating in the port-channel.

## 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** > **LAG Membership**.

1. Use **LAG ID** to select the identification of the LAG.
2. Use **LAG Name** to enter the name you want assigned to the LAG. You may enter any string of up to 15 alphanumeric characters. A valid name has to be specified in order to create the LAG.
3. Use **LAG Description** to enter the Description string to be attached to a LAG. It can be up to 64 characters in length.
4. Use **Admin Mode** to select enable or disable from the pull-down menu. When the LAG is disabled no traffic will flow and LACPDUs will be dropped, but the links that form the LAG will not be released. The factory default is enable.
5. Use **Link Trap** to specify whether you want to have a trap sent when link status changes. The factory default is enable, which will cause the trap to be sent.
6. Use **STP Mode** to enable or disable the Spanning Tree Protocol Administrative Mode associated with the LAG. The possible values are:
  - **Disable** - Spanning tree is disabled for this LAG.
  - **Enable** - Spanning tree is enabled for this LAG.
7. Use **Static Mode** to select enable or disable from the pull-down menu. When the LAG is enabled it does not transmit or process received LACPDUs i.e. the member ports do not transmit LACPDUs and all the LACPDUs it may receive are dropped. The factory default is disable.
8. Use **Hash Mode** to select the load-balancing mode used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link:

- **Src MAC,VLAN,EType,incoming port** - Source MAC, VLAN, EtherType, and incoming port associated with the packet.
- **Dest MAC,VLAN,EType,incoming port** - Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
- **Src/Dest MAC,VLAN,EType,incoming port** - Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
- **Src IP** and **Src TCP/UDP Port** fields - Source IP and Source TCP/UDP fields of the packet.
- **Dest IP** and **Dest TCP/UDP Port** fields - Destination IP and Destination TCP/UDP Port fields of the packet.
- **Src/Dest IP** and **TCP/UDP Port** fields - Source/Destination IP and source/destination TCP/UDP Port fields of the packet.

9. Use the **Port Selection Table** to select the ports as members of the LAG.

### LAG Membership

LAG ID

None

LAG Name

LAG Description

Admin Mode

Enable

Link Trap

Enable

STP Mode

Enable

Static Mode

Disable

Hash Mode

Src/Dest MAC, VLAN, EType, incoming port

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																				



The **Routing** tab contains links to the following features:

- [Routing Table](#) on page 205
- [IP](#) on page 213
- [IPv6](#) on page 229
- [VLAN](#) on page 250
- [ARP](#) on page 252
- [RIP](#) on page 258
- [OSPF](#) on page 266
- [OSPFv3](#) on page 296
- [Router Discovery](#) on page 323
- [VRRP](#) on page 325
- [Multicast](#) on page 334
- [IPv6 Multicast](#) on page 371

## Routing Table

The Routing Table collects routes from multiple sources: static routes, RIP routes, OSPF routes, and local routes. The Routing Table may learn multiple routes to the same destination from multiple sources. The Routing Table lists all routes.

From the Routing Table link, you can access the following pages:

- [Basic](#) on page 205
- [Advanced](#) on page 209

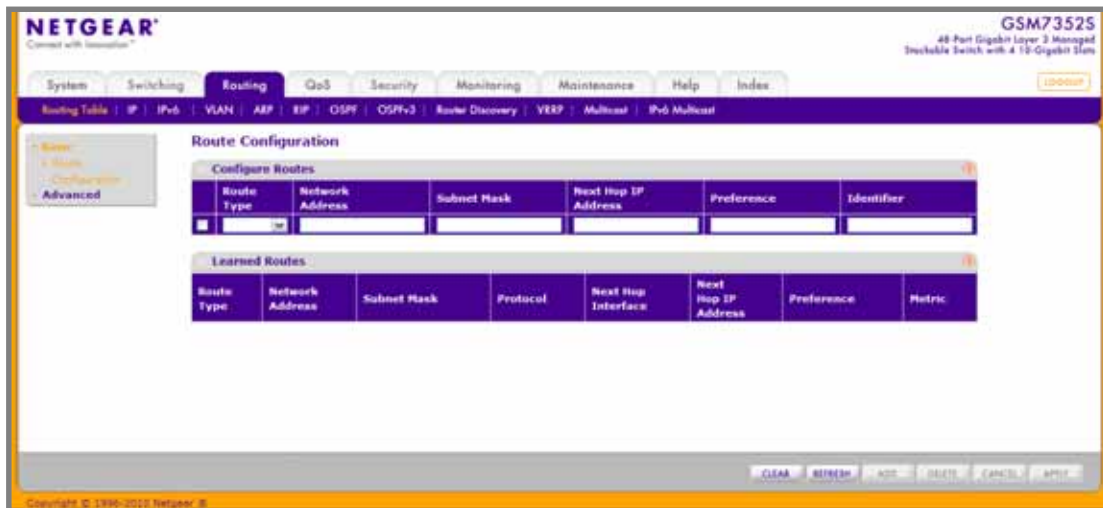
### Basic

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

- [Route Configuration](#) on page 206

## Route Configuration

To display the Route Configuration page, click **Routing** > **Routing Table** > **Basic** > **Route Configuration**.



**NETGEAR**  
Connect with Innovation™

GSM73525  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Routing Table IP IPv6 VLAN AMP RIP OSPF OSPFv3 Router Discovery VRRP Multicast IPv6 Multicast

Basic  
Advanced

### Route Configuration

Configure Routes

Route Type	Network Address	Subnet Mask	Next Hop IP Address	Preference	Identifier
<input type="checkbox"/> Static	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Learned Routes

Route Type	Network Address	Subnet Mask	Protocol	Next Hop Interface	Next Hop IP Address	Preference	Metric
------------	-----------------	-------------	----------	--------------------	---------------------	------------	--------

CLEAR REFRESH ADD DELETE CANCEL APPLY

Copyright © 1996-2015 Netgear, Inc.

## Route Configuration

1. Use the **Route Type** field to specify default or static. If creating a default route, all that needs to be specified is the next hop IP address, otherwise each field needs to be specified.
2. **Network Address** displays the IP route prefix for the destination.
3. **Subnet Mask** indicates the portion of the IP interface address that identifies the attached network. This is also referred to as the subnet/network mask.
4. **Next Hop IP Address** displays 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 will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
5. **Preference** displays an integer value from (1 to 255). The user 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 than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.
6. Use **Identifier** to specify the description of this route that identifies the route.
7. Click **ADD** to add a new static route entry to the switch.
8. Click **DELETE** to delete a existing static route entry from the switch.

## Learned Routes

**Table 4.**

Field	Description
Route Type	This field can be either default or static. If creating a default route, all that needs to be specified is the next hop IP address, otherwise each field needs to be specified.
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"> <li>• Local</li> <li>• Static</li> <li>• OSPF</li> <li>• RIP</li> </ul>
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 will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Metric	Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 - 255.
Preference	The preference is an integer value from (0 to 255). The user 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 than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

Click **REFRESH** to refresh the web page to show the latest learned routes.

## Advanced

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

- [Route Configuration](#) on page 209
- [Route Preferences](#) on page 212

### Route Configuration

To display the Route Configuration page, click **Routing** > **Routing Table** > **Advanced** > **Route Configuration**.

The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switch web interface. The top navigation bar includes links for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The 'Routing' section is expanded, showing sub-links for Routing Table, IP, IPv6, VLAN, ARP, RIP, OSPF, OSPFv3, Router Discovery, VRRP, Multicast, and IPv6 Multicast. The 'Route Configuration' page is displayed, featuring a 'Configure Routes' table with columns for Route Type, Network Address, Subnet Mask, Next Hop IP Address, Preference, and Identifier. Below this is a 'Learned Routes' table with columns for Route Type, Network Address, Subnet Mask, Protocol, Next Hop Interface, Next Hop IP Address, Preference, and Metric. The bottom of the page includes a footer with 'CLEAR', 'REFRESH', and other buttons.

## Route Configuration

1. Use the **Route Type** field to specify default or static. If creating a default route, all that needs to be specified is the next hop IP address, otherwise each field needs to be specified.
2. **Network Address** displays the IP route prefix for the destination.
3. **Subnet Mask** indicates the portion of the IP interface address that identifies the attached network. This is also referred to as the subnet/network mask.
4. **Next Hop IP Address** displays 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 will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
5. **Preference** displays an integer value from (1 to 255). The user 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 than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.
6. Use **Identifier** to specify the description of this route that identifies the route.
7. Click **ADD** to add a new static route entry to the switch.
8. Click **DELETE** to delete a existing static route entry from the switch.

## Learned Routes

**Table 5.**

Field	Description
Route Type	This field can be either default or static. If creating a default route, all that needs to be specified is the next hop IP address, otherwise each field needs to be specified.
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"> <li>• Local</li> <li>• Static</li> <li>• OSPF</li> <li>• RIP</li> </ul>
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 will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Metric	Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 - 255.
Preference	The preference is an integer value from (0 to 255). The user 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 than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

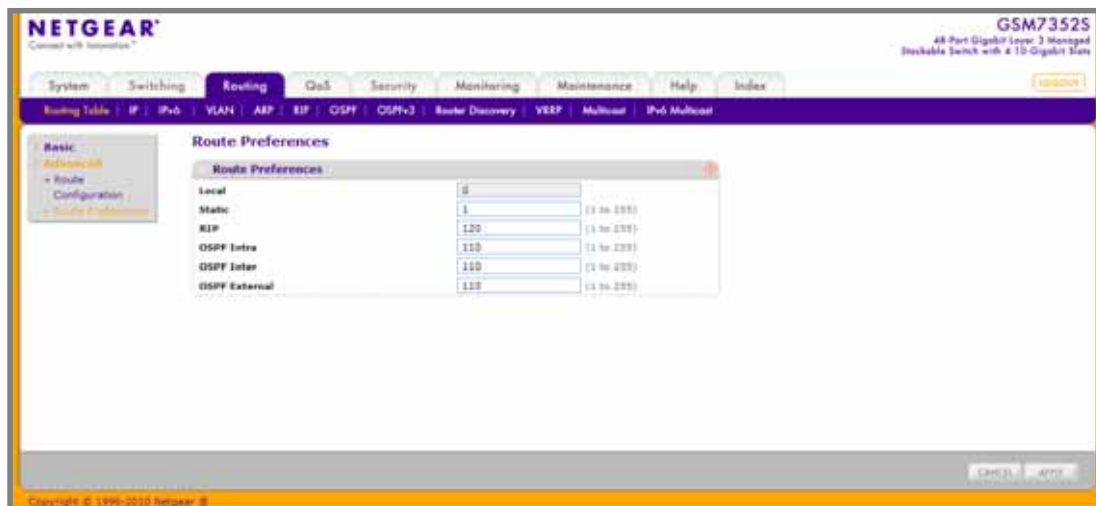
Click **REFRESH** to refresh the web page to show the latest learned routes.

## Route Preferences

Use this panel to configure the default preference for each protocol, e.g., 60 for static routes, 120 for RIP. These values are arbitrary values in the range of 1 to 255 and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol.

The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multiple routes to a destination, the preference values are used to determine the preferred route. If there is still a tie, the route with the best route metric will be chosen. To avoid problems with mismatched metrics (i.e., RIP and OSPF metrics are not directly comparable) you must configure different preference values for each of the protocols.

To display the Route Preferences page, click **Routing** > **Routing Table** > **Advanced** > **Route Preferences**.



1. Use **Static** to specify the static route preference value in the router. The default value is 1. The range is 1 to 255.
2. Use **RIP** to specify the RIP route preference value in the router. The default value is 120. The range is 1 to 255.
3. Use **OSPF Intra** to specify the OSPF intra route preference value in the router. The default value is 110. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2.
4. Use **OSPF Inter** to specify the OSPF inter route preference value in the router. The default value is 110. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2.
5. Use **OSPF External** to specify the OSPF external route preference value in the router. The default value is 110. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preference value must be the same for all the OSPF external route types like type1/type2/nssa1/nssa2.



Table 6.

Field	Description
Local	This field displays the local route preference value.

## IP

The IP folder contains links to the following web pages that configure and display IP routing data:

- [Basic](#) on page 213
- [Advanced](#) on page 220

## Basic

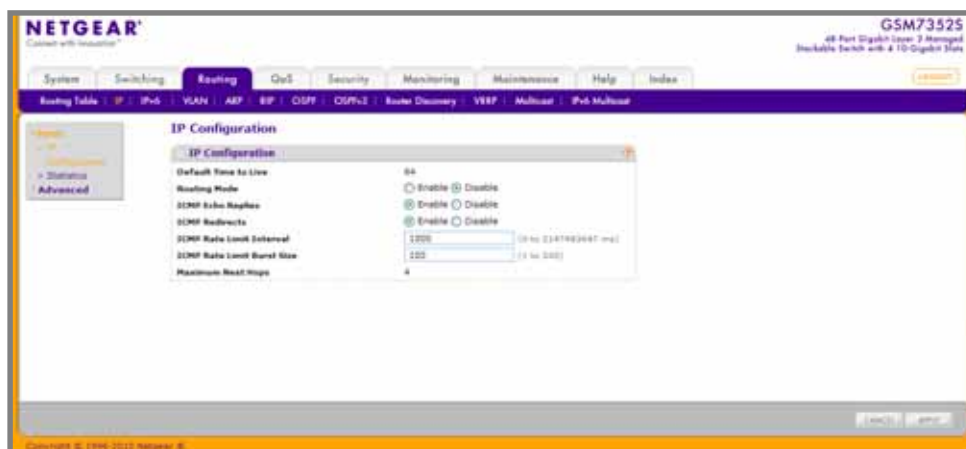
From the Basic link, you can access the following pages:

- [IP Configuration](#) on page 213
- [Statistics](#) on page 215

### IP Configuration

Use this menu to configure routing parameters for the switch, as opposed to an interface.

To display the IP Configuration page, click **Routing > IP > Basic > IP Configuration**.



1. Use **Routing Mode** to select enable or disable. You must enable routing for the switch before you can route through any of the interfaces. The default value is disable.
2. Use **ICMP Echo Replies** to select enable or disable. If it is enable then only the router can send ECHO replies. By default ICMP Echo Replies are sent for echo requests.
3. Use **ICMP Redirects** to select enable or disable. If it is enabled globally and on interface level then only the router can send ICMP Redirects.
4. Use **ICMP Rate Limit Interval** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval. By default, Rate limit is 100 packets/sec i.e., burst interval is 1000 msec. To disable ICMP Rate limiting, set this field to '0'. Valid Rate Interval must be in the range 0 to 2147483647.
5. Use **ICMP Rate Limit Burst Size** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval. By default, burst size is 100 packets. When burst interval is 0 then configuring this field is not a valid operation. Valid Burst Size must be in the range 1 to 200.

**Table 7.**

Field	Description
Default Time to Live	The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a compile-time constant.

## Statistics

The statistics reported on this screen are as specified in RFC 1213.

To display the Statistics page, click **Routing > IP > Basic > Statistics**.

IP Statistics	
IpInReceives	544721
IpInHdrErrors	0
IpInAddrErrors	4473
IpForwDatagrams	0
IpInUnknownProtes	0
IpInDiscards	0
IpInDelivers	530150
IpOutRequests	27163
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	0
IcmpInErrors	0
IcmpInDestUnreachs	0
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSrcQuenches	0
IcmpInRedirects	0
IcmpInEchos	0
IcmpInEchoReps	0
IcmpInTimestamps	0
IcmpInTimestampReps	0
IcmpInAddrMasks	0
IcmpInAddrMaskReps	0
IcmpOutMsgs	0
IcmpOutErrors	0
IcmpOutDestUnreachs	0
IcmpOutTimeExcds	0
IcmpOutParmProbs	0
IcmpOutSrcQuenches	0
IcmpOutRedirects	0
IcmpOutEchos	0
IcmpOutEchoReps	0
IcmpOutTimestamps	0
IcmpOutTimestampReps	0
IcmpOutAddrMasks	0
IcmpOutAddrMaskReps	0

**Table 8.**

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 will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.

Table 8.

Field	Description
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.
IcmlnMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmlnErrors.

Table 8.

Field	Description
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.

**Table 8.**

Field	Description
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 will always be zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
IcmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

## Advanced

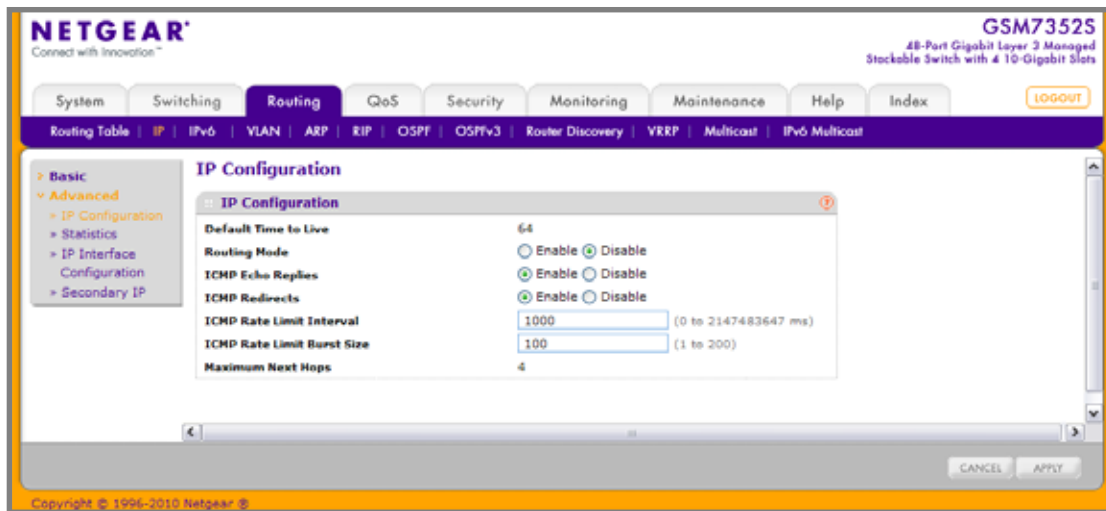
From the Advanced link, you can access the following pages:

- [IP Configuration](#) on page 220
- [IP Statistics](#) on page 222
- [IP Interface Configuration](#) on page 227
- [Secondary IP Address](#) on page 229

### IP Configuration

Use this menu to configure routing parameters for the switch as opposed to an interface.

To display the IP Configuration page, click **Routing > IP > Advanced > IP Configuration**.





1. Use **Routing Mode** to select enable or disable. You must enable routing for the switch before you can route through any of the interfaces. The default value is disable.
2. Use **ICMP Echo Replies** to select enable or disable. If it is enable, then only the router can send ECHO replies. By default ICMP Echo Replies are sent for echo requests.
3. Use **ICMP Redirects** to select enable or disable. If it is enabled globally and on interface level then only the router can send ICMP Redirects.
4. Use **ICMP Rate Limit Interval** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval. By Default Rate limit is 100 packets/sec, i.e., burst interval is 1000 msec. To disable ICMP Rate limiting set this field to '0'. Valid Rate Interval must be in the range 0 to 2147483647.
5. Use **ICMP Rate Limit Burst Size** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval. By Default burst size is 100 packets. When burst interval is 0 then configuring this field is not a valid operation. Valid Burst Size must be in the range 1 to 200.

Table 9.

Field	Description
Default Time to Live	The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a compile-time constant.

## IP Statistics

The statistics reported on this screen are as specified in RFC 1213.

To display the IP Statistics page, click **Routing** > **IP** > **Advanced** > **IP Statistics**.

IP Statistics	
IP Statistics	
IpInReceives	544999
IpInHdrErrors	0
IpInAddrErrors	4473
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	530422
IpOutRequests	27212
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	0
IcmpInErrors	0
IcmpInDestUnreachs	0
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSecQuenches	0
IcmpInRedirects	0
IcmpInEchos	0
IcmpInEchoReps	0
IcmpInTimestamps	0
IcmpInTimestampReps	0
IcmpInAddrMasks	0
IcmpInAddrMaskReps	0
IcmpOutMsgs	0
IcmpOutErrors	0
IcmpOutDestUnreachs	0
IcmpOutTimeExcds	0
IcmpOutParmProbs	0
IcmpOutSecQuenches	0
IcmpOutRedirects	0
IcmpOutEchos	0
IcmpOutEchoReps	0
IcmpOutTimestamps	0
IcmpOutTimestampReps	0
IcmpOutAddrMasks	0
IcmpOutAddrMaskReps	0

**Table 10.**

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 will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.

Table 10.

Field	Description
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.
IcmlnMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmlnErrors.

**Table 10.**

Field	Description
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.

**Table 10.**

Field	Description
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 will always be zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
IcmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

## IP Interface Configuration

Use the IP Interface Configuration page to update IP interface data for this switch.

To display the IP Interface Configuration page, click **Routing > IP > Advanced > IP Interface Configuration**.

IP Interface Configuration

Go To Interface:

Port	Description	VLAN ID	IP Address	Subnet Mask	Routing Mode	Administrative Mode	OSPF Admin Mode	Forward Net Directed Broadcasts	Encapsulation Type	Proxy Arp	Local Proxy Arp	Bandwidth	ICMP Destination Unreachable	ICMP Echo Reply
<input type="checkbox"/> 1/0/1			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/2			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/3			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/4			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/5			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/6			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/7			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/8			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/9			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/10			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/11			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/12			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/13			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/14			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/15			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/16			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/17			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/18			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/19			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/20			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/21			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/22			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/23			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/24			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/25			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/26			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/27			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/28			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/29			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/30			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/31			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/32			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/33			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/34			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/35			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/36			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/37			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/38			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/39			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/40			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/41			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/42			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/43			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/44			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/45			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/46			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/47			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/48			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/49			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/50			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/51			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable
<input type="checkbox"/> 1/0/52			0.0.0.0	0.0.0.0	Disable	Enable	Disable	Disable	Ethernet	Enable	Disable	100000	Enable	Enable

Go To Interface:

1. Use **Port** to select the interface for which data is to be displayed or configured.
2. Use **Description** to enter the Description for the interface.
3. Use **IP Address** to enter the IP address for the interface.
4. Use **Subnet Mask** to enter the subnet mask for the interface. This is also referred to as the subnet/network mask, and defines the portion of the interface's IP address that is used to identify the attached network.
5. Use **Routing Mode** to enable or disable routing for an interface. The default value is enable.
6. Use **Administrative Mode** to enable/disable the Administrative Mode of the interface. The default value is enable. This mode is not supported for Logical VLAN Interfaces.
7. Use **Forward Net Directed Broadcasts** to select how network directed broadcast packets should be handled. If you select enable from the pull-down menu, network directed

broadcasts will be forwarded. If you select disable they will be dropped. The default value is disable.

8. Use **Encapsulation Type** to select the link layer encapsulation type for packets transmitted from the specified interface from the pull-down menu. The possible values are Ethernet and SNAP. The default is Ethernet.
9. Use **Proxy Arp** to disable or enable proxy Arp for the specified interface from the pull-down menu.
10. Use **Local Proxy Arp** to disable or enable Local Proxy ARP for the specified interface from the pull-down menu.
11. Use **Bandwidth** to specify the configured bandwidth on this interface. This parameter communicates the speed of the interface to higher level protocols. OSPF uses bandwidth to compute link cost. Valid range is (1 to 10000000).
12. Use **ICMP Destination Unreachables** to specify the Mode of Sending ICMP Destination Unreachables on this interface. If this is Disabled then this interface will not send ICMP Destination Unreachables. By default Destination Unreachables mode is enable.
13. Use **ICMP Redirects** to enable/disable ICMP Redirects Mode. The router sends an ICMP Redirect on an interface only if Redirects are enabled both globally and on the interface. By default ICMP Redirects Mode is enable.
14. Use **IP MTU** to specify the maximum size of IP packets sent on an interface. Valid range is 68 bytes to the link MTU. Default value is 0. 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.

**Table 11.**

Field	Description
VLAN ID	Displays the VLAN ID for the interface.
Link State	The state of the specified interface is either Active or Inactive. An interface is considered active if it the link is up and it is in forwarding state.
OSPF Admin Mode	Displays OSPF admin mode of the interface. The default value is disable.

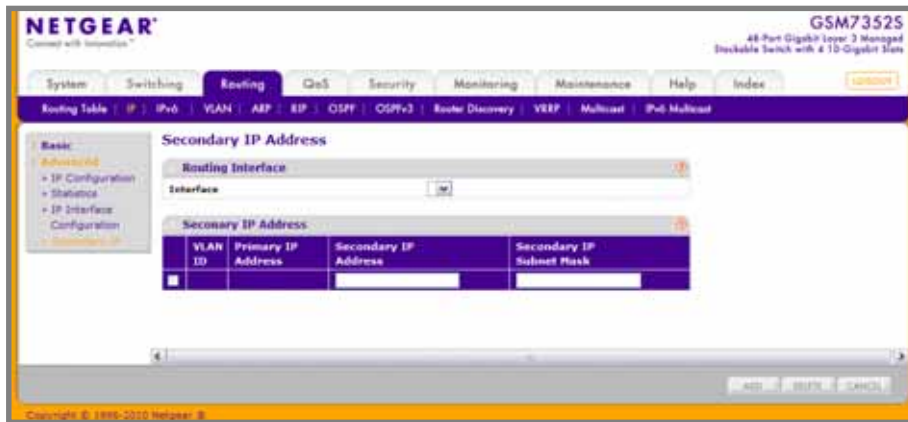
Click **DELETE** to delete the IP Address from the selected interface.

Click **REFRESH** to refresh the web page to show the latest IP information.



## Secondary IP Address

To display the Secondary IP Address page, click **Routing** > **IP** > **Advanced** > **Secondary IP**.



1. Use **Interface** to select the interface for which data is to be displayed or configured.
2. Use **Secondary IP Address** to add a secondary IP address to the selected interface.
3. Use **Secondary IP Subnet Mask** to enter the subnet mask for the interface. This is also referred to as the subnet/network mask, and defines the portion of the interface's IP Address that is used to identify the attached network. This value is read only once configured.
4. Click **ADD** to add a Secondary IP Address for the selected interface.
5. Click **DELETE** to delete the Secondary IP Address from the selected interface.

**Table 12.**

Field	Description
VLAN ID	The VLAN ID associated with the displayed or configured interface.
Primary IP Address	The Primary IP Address for the Interface.

## IPv6

IPv6 is the next generation of the Internet Protocol. With 128-bit addresses, versus 32-bit addresses for IPv4, IPv6 solves the address depletion issues seen with IPv4 and removes the requirement for Network Address Translation (NAT), which is used in IPv4 networks to reduce the number of globally unique IP addresses required for a given network. Its aggregate addresses can dramatically reduce the size of the global routing table through well known address combinations. Security is more integrated and network configuration is simplified yet more flexible.

IPv6 can coexist with IPv4. As with IPv4, IPv6 routing can be enabled on physical and VLAN interfaces. Each L3 routing interface can be used for IPv4, IPv6, or both. IP protocols running over L3 (for example, UDP and TCP) do not change with IPv6. For this reason, a single CPU stack is used for transport of both IPv4 and IPv6, and a single sockets interface provides

access to both. Routing protocols are capable of computing routes for one or both IP versions.

From the IPv6 link, you can access the following pages:

- [Basic](#) on page 230
- [Advanced](#) on page 233

## Basic

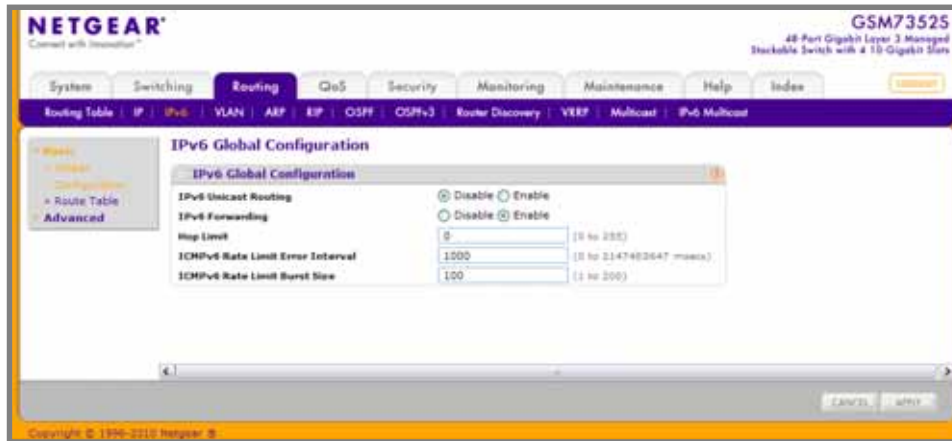
From the Basic link, you can access the following pages:

- [IPv6 Global Configuration](#) on page 231
- [IPv6 Route Table](#) on page 232

## IPv6 Global Configuration

Use the Global Configuration page to enable IPv6 forwarding on the router and to enable the forwarding of IPv6 unicast datagrams.

To display the IPv6 Global Configuration page, click **Routing > IPv6 > Basic > Global Configuration**.

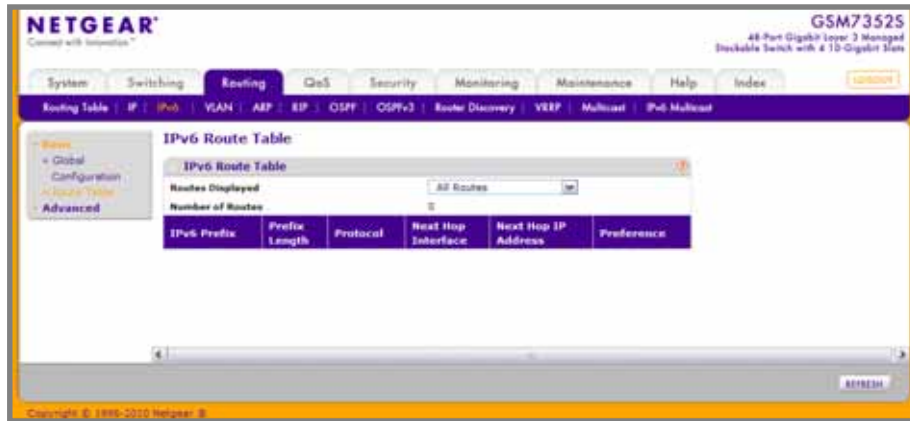


1. Use **IPv6 Unicast Routing** to globally enable or disable IPv6 unicast routing on the entity.
2. Use **IPv6 Forwarding** to enable or disable forwarding of IPv6 frames on the router.
3. Use the **Hop Limit** option to define the unicast hop count used in IPv6 packets originated by the node. The value is also included in router advertisements. Valid values for <hops> are 1-64 inclusive. The default “not configured” means that a value of zero is sent in router advertisements and a value of 64 is sent in packets originated by the node. Note that this is not the same as configuring a value of 64.
4. Use **ICMPv6 Rate Limit Error Interval** to control the ICMPv6 error packets by specifying the number of ICMP error packets that are allowed per burst interval. By Default Rate limit is 100 packets/sec i.e., burst interval is 1000 msec. To disable ICMP Ratelimiting set this field to '0'. Valid Rate Interval must be in the range 0 to 2147483647.
5. Use **ICMPv6 Rate Limit Burst Size** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval. Default burst size is 100 packets. When burst interval is 0 then configuring this field is not a valid operation. Valid Burst Size must be in the range 1 to 200.

## IPv6 Route Table

Use the IPv6 Route Table page to display all active IPv6 routes and their settings.

To display the IPv6 Route Table page, click **Routing** > **IPv6** > **Basic** > **Route Table**.



1. Use **Routes Displayed** to choose from:

- **Configured Routes** - Shows the routes configured by the user.
- **Best Routes** - Shows only the best active routes.
- **All Routes** - Shows all active IPv6 routes.

**Table 13.**

Field	Description
Number of Routes	Displays the total number of active routes in the route table.
IPv6 Prefix	Displays the Network Prefix for the Active Route.
Prefix Length	Displays the Prefix Length for the Active Route.
Protocol	Displays the Type of Protocol for the Active Route.
Next Hop Interface	Displays the Interface over which the Route is Active. For a Reject Route the next hop would be a "Null0" interface.
Next Hop IP Address	Displays the Next Hop IPv6 Address for the Active Route.
Preference	Displays the Route Preference of the Configured Route.

Click **REFRESH** to refresh the web page to show the latest IP information.

## Advanced

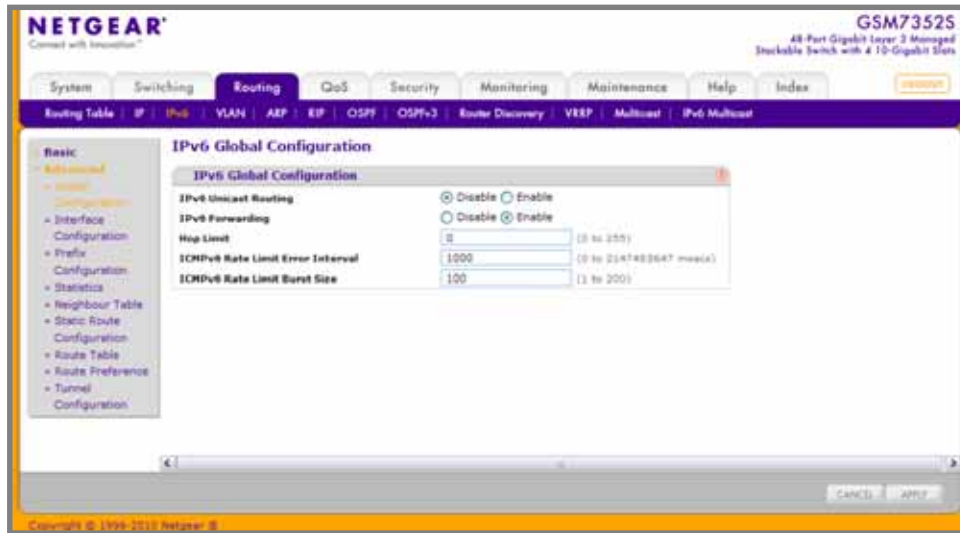
From the Basic link, you can access the following pages:

- [\*IPv6 Global Configuration\*](#) on page 234
- [\*IPv6 Interface Configuration\*](#) on page 235
- [\*IPv6 Prefix Configuration\*](#) on page 237
- [\*IPv6 Statistics\*](#) on page 238
- [\*IPv6 Neighbor Table\*](#) on page 244
- [\*IPv6 Route Configuration\*](#) on page 246
- [\*IPv6 Route Table\*](#) on page 247
- [\*IPv6 Route Preferences\*](#) on page 248
- [\*Tunnel Configuration\*](#) on page 249

## IPv6 Global Configuration

Use the Global Configuration page to enable IPv6 forwarding on the router and to enable the forwarding of IPv6 unicast datagrams.

To display the IPv6 Global Configuration page, click **Routing** > **IPv6** > **Advanced** > **Global Configuration**.

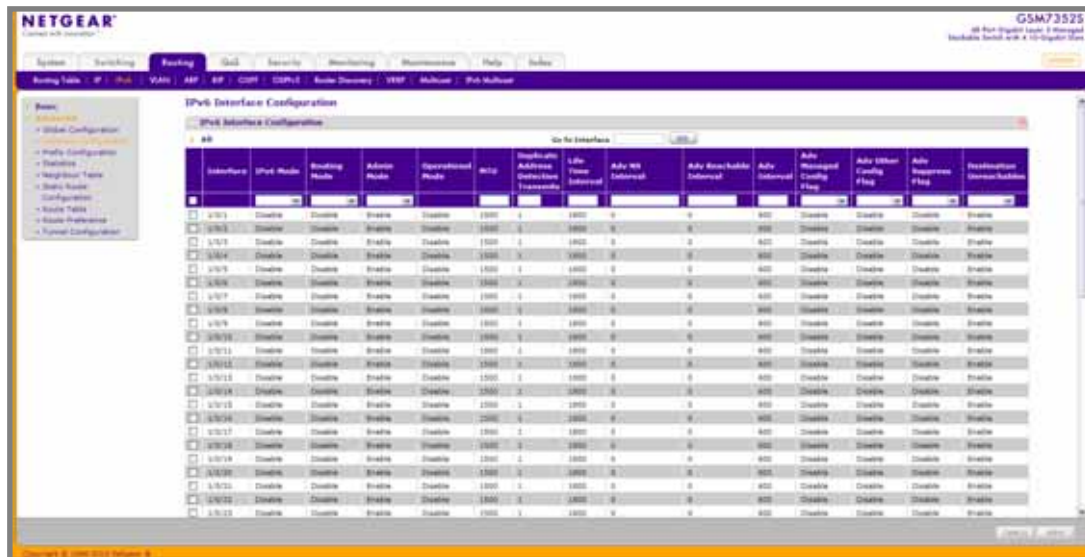


1. Use **IPv6 Unicast Routing** to globally enable or disable IPv6 unicast routing on the entity.
2. Use **IPv6 Forwarding** to enable or disable forwarding of IPv6 frames on the router.
3. Use the **Hop Limit** option to define the unicast hop count used in IPv6 packets originated by the node. The value is also included in router advertisements. Valid values for <hops> are 1-64 inclusive. The default "not configured" means that a value of zero is sent in router advertisements and a value of 64 is sent in packets originated by the node. Note that this is not the same as configuring a value of 64.
4. Use **ICMPv6 Rate Limit Error Interval** to control the ICMPv6 error packets by specifying the number of ICMP error packets that are allowed per burst interval. By default Rate limit is 100 packets/sec i.e., burst interval is 1000 msec. To disable ICMP Rate limiting, set this field to '0'. Valid Rate Interval must be in the range 0 to 2147483647.
5. Use **ICMPv6 Rate Limit Burst Size** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval. Default burst size is 100 packets. When burst interval is 0 then configuring this field is not a valid operation. Valid Burst Size must be in the range 1 to 200.

## IPv6 Interface Configuration

Use the Interface Configuration page to configure IPv6 interface parameters.

To display the IPv6 Interface Configuration page, click **Routing > IPv6 > Advanced > Interface Configuration**.



1. Use **Interface** to select the interface to be configured or displayed. All physical interfaces are valid.
2. Use **IPv6 Mode** to enable/disable IPv6 mode. When IPv6 mode is enabled, interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used. This selector lists the two options for IPv6 mode: enable and disable. Default value is disable.
3. Use **Routing Mode** to enable/disable routing mode of an interface. Default value is disable.
4. Use **Admin Mode** to enable/disable the Administrative Mode of the interface. The default value is enable. This mode is not supported for Logical VLAN Interfaces.
5. Use **MTU** to specify the maximum transmit unit on an interface. If the value is 0 then this interface is not enabled for routing. It is not valid to set this value to 0 if routing is enabled. Range of MTU is 1280 to 1500.
6. Use **Duplicate Address Detection Transmits** to specify the number of duplicate address detections transmits on an interface. DAD transmits values must be in range 0 to 600.
7. Use **Life Time Interval** to specify the router advertisement lifetime field sent from the interface. This value must be greater than or equal to the maximum advertisement interval. 0 means do not use the router as the default router. The range of router lifetime is 0 to 9000.
8. Use **Adv NS Interval** to specify the retransmission time field of router advertisement sent from the interface. A value of 0 means interval is not specified for router. Range of neighbor solicit interval is 1000 to 4294967295.
9. Use **Adv Reachable Time** to specify the router advertisement time to consider neighbor reachable after ND confirmation. Range of reachable time is 0 to 3600000.

10. Use **Adv Interval** to specify the maximum time allowed between sending router advertisements from the interface. Default value is 600. Range of maximum advertisement interval is 4 to 1800.
11. Use **Adv Managed Config Flag** to specify the router advertisement managed address configuration flag. When true, end nodes use DHCPV6. When false, end nodes auto configure addresses. Default value of managed flag is disable.
12. Use **Adv Other Config Flag** To specify router advertisement for "other" Stateful configuration flag. Default value of other config flag is disable.
13. Use **Adv Suppress Flag** to specify router advertisement suppression on an interface. Default value of suppress flag is disable.
14. Use **Destination Unreachables** to specify the Mode of Sending ICMPv6 Destination Unreachables on this interface. If Disabled then this interface will not send ICMPv6 Destination Unreachables. By default IPv6 Destination Unreachables mode is enable.

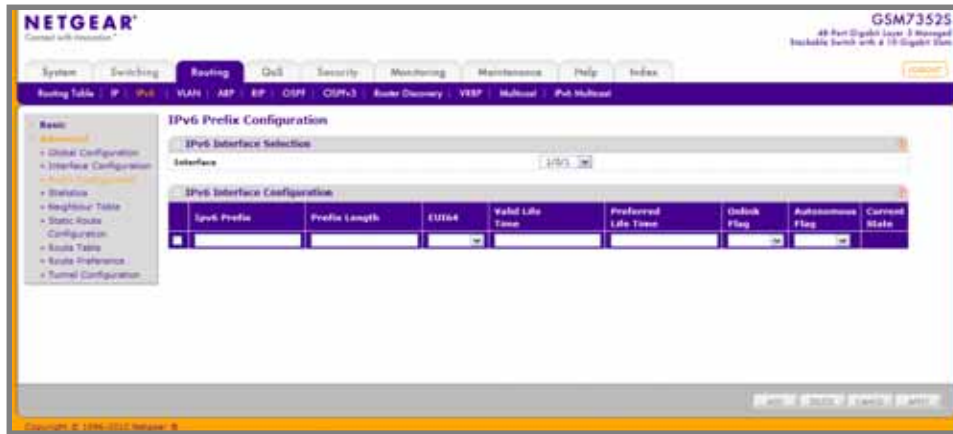
**Table 14.**

Field	Description
Operational Mode	Specifies operational state of an interface. Default value is disable.



## IPv6 Prefix Configuration

To display the IPv6 Prefix Configuration page, click **Routing** > **IPv6** > **Advanced** > **Prefix Configuration**.



1. Use **Interface** to select the interface to be configured. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port. All physical interfaces are valid.
2. Use **IPv6 Prefix/Prefix Length** to specify the IPv6 prefix with prefix length for an interface.
3. Use **EUI-64** to specify 64 bit unicast prefix.
4. Use **Valid Lifetime** to specify router advertisement per prefix time to consider prefix valid for purposes of on link determination. Valid lifetime must be in the range 0 to 4294967295.
5. Use **Preferred Lifetime** to specify router advertisement per prefix time. An auto configured address generated from this prefix is preferred. Preferred lifetime must be in range 0 to 4294967295.
6. Use **OnLink Flag** to specify selected prefix can be used for on-link determination. Default value is enable. This selector lists the two options for on-link flag: enable and disable.
7. Use **Autonomous Flag** to specify selected prefix can be used for autonomous address configuration. Default value is disable. This selector lists the two options for autonomous flag: enable and disable.

**Table 15.**

Field	Description
Current State	Indicates the state of the IPV6 address. The state is TENT if routing is disabled or DAD fails. The state is Active if interface is active and DAD is successful.

- Click **ADD** to add a new IPv6 address to the interface.
- Click **DELETE** to delete a existing IPv6 address entry from the interface.

## IPv6 Statistics

Use the IPv6 Statistics page to display IPv6 traffic statistics for one or all interfaces.

To display the IPv6 Statistics page, click **Routing** > **IPv6** > **Advanced** > **Statistics**.

**IPv6 Statistics**

**IPv6 Interface Selection**

Interface: 1/10/1 ↻

**IPv6 Statistics**

Total Datagrams Received	0
Received Datagrams Locally Delivered	0
Received Datagrams Discarded Due To Header Errors	0
Received Datagrams Discarded Due To MTU	0
Received Datagrams Discarded Due To No Route	0
Received Datagrams With Unknown Protocol	0
Received Datagrams Discarded Due To Invalid Address	0
Received Datagrams Discarded Due To Truncated Data	0
Received Datagrams Discarded Other	0
Received Datagrams Reassembly Required	0
Datagrams Successfully Reassembled	0
Datagrams Failed To Reassemble	0
Datagrams Forwarded	0
Datagrams Locally Transmitted	0
Datagrams Transmit Failed	0
Datagrams Successfully Fragmented	0
Datagrams Failed To Fragment	0
Datagrams Fragments Created	0
Multicast Datagrams Received	0
Multicast Datagrams Transmitted	0

**ICMPv6 Statistics**

Total ICMPv6 Messages Received	0
ICMPv6 Messages With Errors Received	0
ICMPv6 Destination Unreachable Messages Received	0
ICMPv6 Messages Prohibited Administratively Received	0
ICMPv6 Time Exceeded Messages Received	0
ICMPv6 Parameter Problem Messages Received	0
ICMPv6 Packet Too Big Messages Received	0
ICMPv6 Echo Request Messages Received	0
ICMPv6 Echo Reply Messages Received	0
ICMPv6 Router Solicit Messages Received	0
ICMPv6 Router Advertisement Messages Received	0
ICMPv6 Neighbor Solicit Messages Received	0
ICMPv6 Neighbor Advertisement Messages Received	0
ICMPv6 Redirect Messages Received	0
ICMPv6 Group Membership Query Messages Received	0
ICMPv6 Group Membership Response Messages Received	0
ICMPv6 Group Membership Reduction Messages Received	0
Total ICMPv6 Messages Transmitted	0
ICMPv6 Messages Not Transmitted Due To Error	0
ICMPv6 Destination Unreachable Messages Transmitted	0
ICMPv6 Messages Prohibited Administratively Transmitted	0
ICMPv6 Time Exceeded Messages Transmitted	0
ICMPv6 Parameter Problem Messages Transmitted	0
ICMPv6 Packet Too Big Messages Transmitted	0
ICMPv6 Echo Request Messages Transmitted	0
ICMPv6 Echo Reply Messages Transmitted	0
ICMPv6 Router Solicit Messages Transmitted	0
ICMPv6 Router Advertisement Messages Transmitted	0
ICMPv6 Neighbor Solicit Messages Transmitted	0
ICMPv6 Neighbor Advertisement Messages Transmitted	0
ICMPv6 Redirect Messages Transmitted	0
ICMPv6 Group Membership Query Messages Transmitted	0
ICMPv6 Group Membership Response Messages Transmitted	0
ICMPv6 Group Membership Reduction Messages Transmitted	0
ICMPv6 Duplicate Address Detects	0

1. Use **Interface** to select the interface to be configured. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port.

## IPv6 Statistics

**Table 16.**

Field	Description
Total Datagrams Received	The total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Header Errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.
Received Datagrams Discarded Due To MTU	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	The number of input datagrams discarded because no route could be found to transmit them to their destination.
Received Datagrams With Unknown Protocol	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses, e.g., ::0, and unsupported addresses, e.g., addresses with unallocated prefixes. For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received Datagrams Discarded Due To Truncated Data	The number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	The number of input IPv6 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.

Table 16.

Field	Description
Received Datagrams Reassembly Required	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Datagrams Successfully Reassembled	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
Datagrams Failed To Reassemble	The number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Datagrams Forwarded	The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.
Datagrams Locally Transmitted	The number of datagrams which this entity has successfully transmitted from this output interface.
Datagrams Transmit Failed	The number of datagrams which this entity failed to transmit successfully.
Datagrams Successfully Fragmented	The number of IPv6 datagrams that have been successfully fragmented at this output interface.
Datagrams Failed To Fragment	The number of output datagrams that could not be fragmented at this interface.
Datagrams Fragments Created	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.

**Table 16.**

Field	Description
Multicast Datagrams Received	The number of multicast packets received by the interface.
Multicast Datagrams Transmitted	The number of multicast packets transmitted by the interface.

## ICMPv6 Statistics

**Table 17.**

Field	Description
Total ICMPv6 Messages Received	The total number of ICMP messages received by the interface which includes all those counted by <code>ipv6IfIcmpInErrors</code> . Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
ICMPv6 Messages With Errors Received	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.)
ICMPv6 Destination Unreachable Messages Received	The number of ICMP Destination Unreachable messages received by the interface.
ICMPv6 Messages Prohibited Administratively Received	The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages Received	The number of ICMP Time Exceeded messages received by the interface.
ICMPv6 Parameter Problem Messages Received	The number of ICMP Parameter Problem messages received by the interface.
ICMPv6 Packet Too Big Messages Received	The number of ICMP Packet Too Big messages received by the interface.
ICMPv6 Echo Request Messages Received	The number of ICMP Echo (request) messages received by the interface.
ICMPv6 Echo Reply Messages Received	The number of ICMP Echo Reply messages received by the interface.
ICMPv6 Router Solicit Messages Received	The number of ICMP Router Solicit messages received by the interface.
ICMPv6 Router Advertisement Messages Received	The number of ICMP Router Advertisement messages received by the interface.
ICMPv6 Neighbor Solicit Messages Received	The number of ICMP Neighbor Solicit messages received by the interface.

Table 17.

Field	Description
ICMPv6 Neighbor Advertisement Messages Received	The number of ICMP Neighbor Advertisement messages received by the interface.
ICMPv6 Redirect Messages Received	The number of ICMPv6 Redirect messages received by the interface.
ICMPv6 Group Membership Query Messages Received	The number of ICMPv6 Group Membership Query messages received by the interface.
ICMPv6 Group Membership Response Messages Received	The number of ICMPv6 Group Membership Response messages received by the interface.
ICMPv6 Group Membership Reduction Messages Received	The number of ICMPv6 Group Membership Reduction messages received by the interface.
Total ICMPv6 Messages Transmitted	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
ICMPv6 Messages Not Transmitted Due To Error	The number of ICMP messages which this interface 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 IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
ICMPv6 Destination Unreachable Messages Transmitted	The number of ICMP Destination Unreachable Messages sent by the interface.
ICMPv6 Messages Prohibited Administratively Transmitted	Number of ICMP destination unreachable/communication administratively prohibited messages sent.
ICMPv6 Time Exceeded Messages Transmitted	The number of ICMP Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	The number of ICMP Parameter Problem messages sent by the interface.
ICMPv6 Packet Too Big Messages Transmitted	The number of ICMP Packet Too Big messages sent by the interface.
ICMPv6 Echo Request Messages Transmitted	The number of ICMP Echo (request) messages sent by the interface.
ICMPv6 Echo Reply Messages Transmitted	The number of ICMP Echo Reply messages sent by the interface.
ICMPv6 Router Solicit Messages Transmitted	The number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	The number of ICMP Router Advertisement messages sent by the interface.

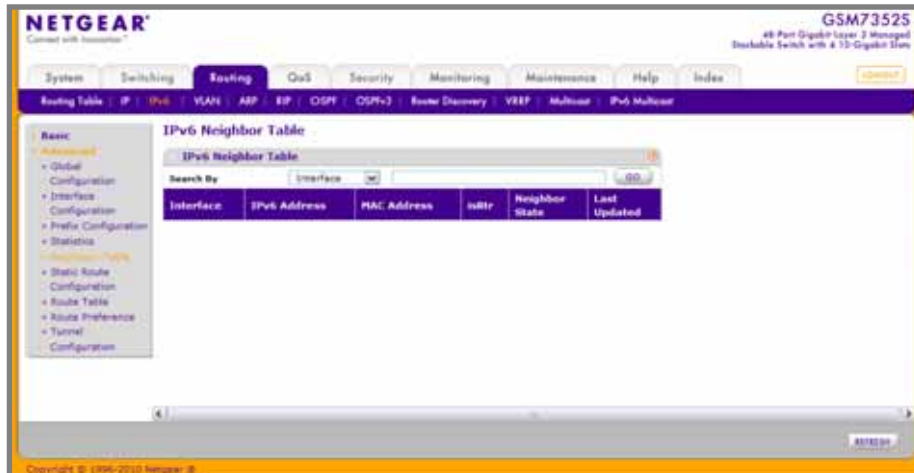
**Table 17.**

Field	Description
ICMPv6 Neighbor Solicit Messages Transmitted	The number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Neighbor Advertisement Messages Transmitted	The number of ICMP Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Transmitted	The number of Redirect messages sent.
ICMPv6 Group Membership Query Messages Transmitted	The number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Transmitted	The number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Transmitted	The number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	The number of duplicate Addresses detected by the interface.

## IPv6 Neighbor Table

Use the IPv6 Neighbor Table page to display IPv6 neighbor details for a specified interface.

To display the IPv6 Neighbor Table page, click **Routing > IPv6 > Advanced > Neighbor Table**.



1. Use **Search By** to search for IPv6 routes by IPv6 address or interface:

- Searched by IPv6 Address - Select **IPv6 Address** from pull-down menu, enter the 128 byte hexadecimal IPv6 Address in four-digit groups separated by colons, for example 2001:231F:::1. Then click **Go**. If the address exists, that entry will be displayed. An exact match is required.
- Searched by Interface - Select **Interface** from pull-down menu, enter the interface ID in Unit/Slot/Port, for example 2/1/1. Then click **Go**. If the IPv6 route exists, the entry will be displayed.

**Table 18.**

Field	Description
Interface	Specifies the interface whose settings are displayed in the current table row.
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.



Table 18.

Field	Description
Neighbor State	<p>Specifies the state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> <li>• Incmp - Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.</li> <li>• Reach - 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• Probe - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.</li> </ul>
Last Updated	Time since the address was confirmed to be reachable.

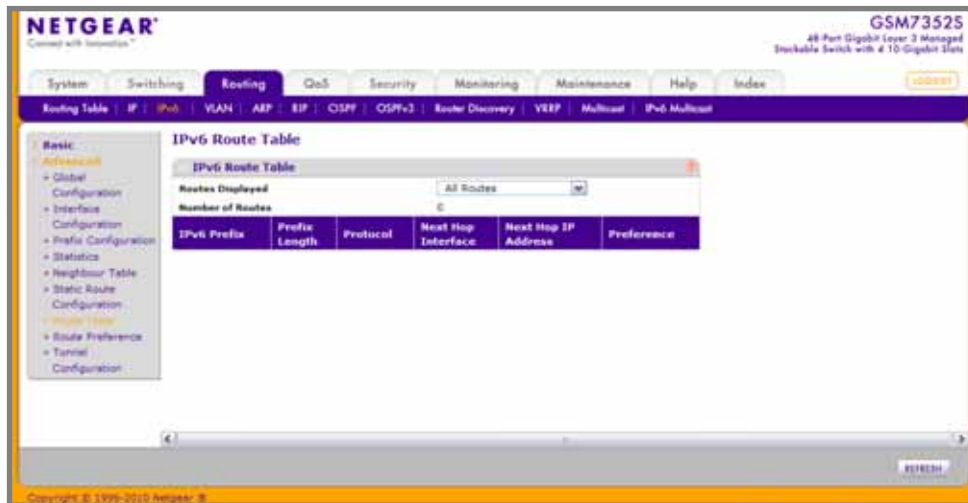
## IPv6 Route Configuration

To display the IPv6 Route Configuration page, click **Routing** > **IPv6** > **Advanced** > **Static Route Configuration**.

1. Use **IPv6 Prefix/Prefix Length** to enter the Network Prefix and Prefix Length for the Configured Route.
2. Use **Next Hop IPv6 Address Type** to specify if the Next Hop IPv6 Address is a Global IPv6 Address or a Link-local IPv6 Address or a Static-Reject IPv6 Address. If the Next Hop IPv6 address specified is a Link-Local IPv6 Address, specify the Interface for the Link-local IPv6 Next Hop Address. Select Static-Reject from this menu to create a static reject route for a destination prefix. No next hop address is specified in that case.
3. Use **Next Hop IPv6 Address** to enter the Next Hop IPv6 Address for the Configured Route.
4. Use **Interface** to specify the unit, slot, and port number for the Link-local IPv6 Next Hop Address. This field is enabled only if the Link-local is selected.
5. Use **Preference** to specify the Route Preference of the Configured Route.
6. Click **ADD** to configure a new route.
7. Click **DELETE** to delete the corresponding route.

## IPv6 Route Table

To display the IPv6 Route Table page, click **Routing** > **IPv6** > **Advanced** > **Route Table**.



1. Use **Routes Displayed** to display:
  - **Configured Routes** - Shows the routes configured by the user.
  - **Best Routes** - Shows only the best active routes.
  - **All Routes** - Shows all active IPv6 routes.
2. Click **REFRESH** to show the latest IP information.

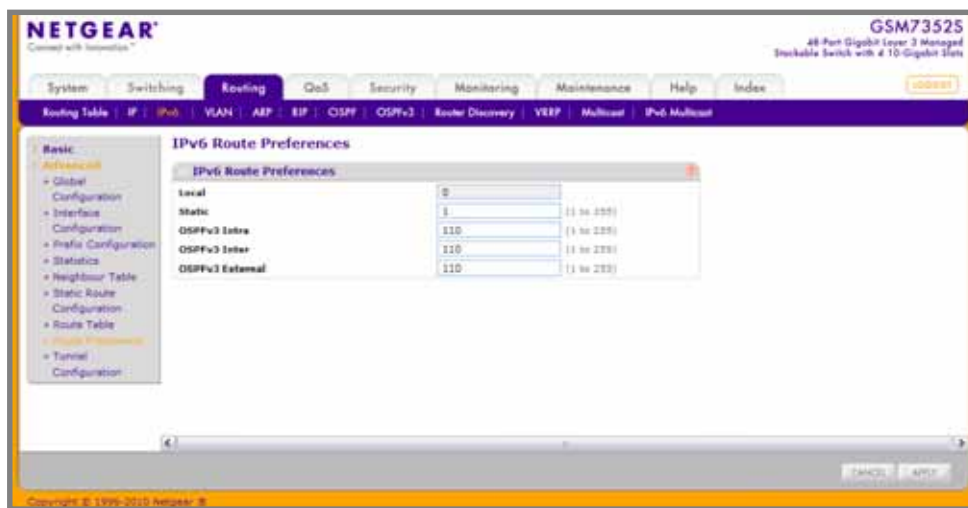
**Table 19.**

Field	Description
Number of Routes	Displays the total number of active routes in the route table.
IPv6 Prefix	Displays the Network Prefix for the Active Route.
Prefix Length	Displays the Prefix Length for the Active Route.
Protocol	Displays the Type of Protocol for the Active Route.
Next Hop Interface	Displays the Interface over which the Route is Active. For a Reject Route the next hop would be a "Null0" interface.
Next Hop IP Address	Displays the Next Hop IPv6 Address for the Active Route.
Preference	Displays the Route Preference of the Configured Route.

## IPv6 Route Preferences

Use this panel to configure the default preference for each protocol. These values are arbitrary values in the range of 1 to 255 and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol. The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multiple routes to a destination, the preference values are used to determine the preferred route. If there is still a tie, the route with the best route metric will be chosen. To avoid problems with mismatched metrics you must configure different preference values for each of the protocols.

To display the IPv6 Route Preferences page, click **Routing > IPv6 > Advanced > Route Preferences**.



1. Use **Static** to specify the Static Route preference value for the router. The default value is 1. The range is 1 to 255.
2. Use **OSPFv3 Intra** to specify the OSPFv3 intra route preference value in the router. The default value is 110. The range is 1 to 255.
3. Use **OSPFv3 Inter** to specify the OSPFv3 inter route preference value in the router. The default value is 110. The range is 1 to 255.
4. Use **OSPFv3 External** to specify the OSPFv3 External route preference value in the router. The default value is 110. The range is 1 to 255.

**Table 20.**

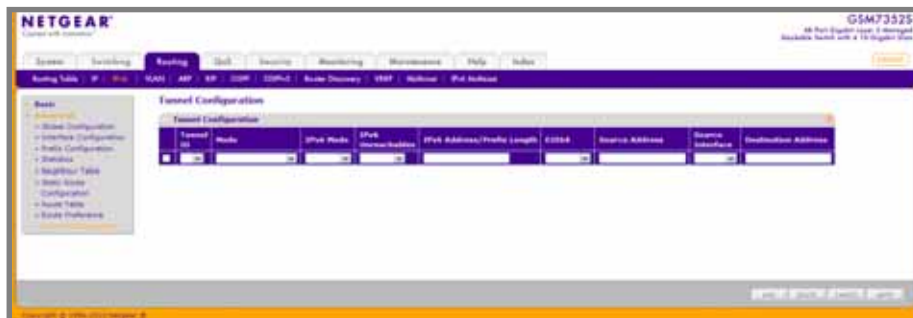
Field	Description
Local	Local preference.

## Tunnel Configuration

ProSafe® Managed Switches software provides for the creation, deletion, and management of tunnel interfaces. These are dynamic interfaces that are created and deleted via user-configuration. ProSafe® Managed Switches support configured IPv6 over IPv4 tunnels to facilitate the transition of IPv4 networks to IPv6 networks. With configured tunnels, the user specifies the endpoints of the tunnel. Tunnels operate as point-to-point links.

Tunnels can be created, configured, and deleted from this page.

To display the Tunnel Configuration page, click **Routing > IPv6 > Advanced > Tunnel Configuration**.



1. Use **Tunnel ID** to select from a list of all of available tunnel IDs.
2. Use **Mode** to select the Tunnel mode. The supported modes are 6-in-4-configured and 6-to-4.
3. Use **IPv6 Mode** to enable IPv6 on this interface using the IPv6 address. This option is only configurable prior to specifying an explicit IPv6 address.
4. Use **IPv6 Unreachables** to specify the Mode of Sending ICMPv6 Destination Unreachables on this interface. If Disabled then this interface will not send ICMPv6 Destination Unreachables. By default IPv6 Destination Unreachables mode is enable.
5. Use **IPv6 Address** to select a list of configured IPv6 addresses for the selected interface. Address must be entered in the format prefix/length.
6. Use **EUI64** to specify the 64-bit extended unique identifier (EUI-64). For 6to4 tunnels, configure the ipv6 address with first 48-bits in the format 2002:tunnel-source-ipv4-address::/48.
7. Use **Source Address** to specify the desired source address. The source address for this tunnel must be entered in dotted decimal notation.
8. Use **Source Interface** to specify the source interface for this tunnel. The address associated with the selected interface will be used as the source address.
9. Use **Destination Address** to specify the destination address for this tunnel in dotted decimal notation.
10. Click **ADD** to allow the user to configure a new tunnel.
11. Click **DELETE** to delete the corresponding tunnel.
12. Click **CANCEL** to discard the changes made on the page and navigate back to the referring page.

## VLAN

You can configure ProSafe® Managed 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 the NETGEAR switch 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:

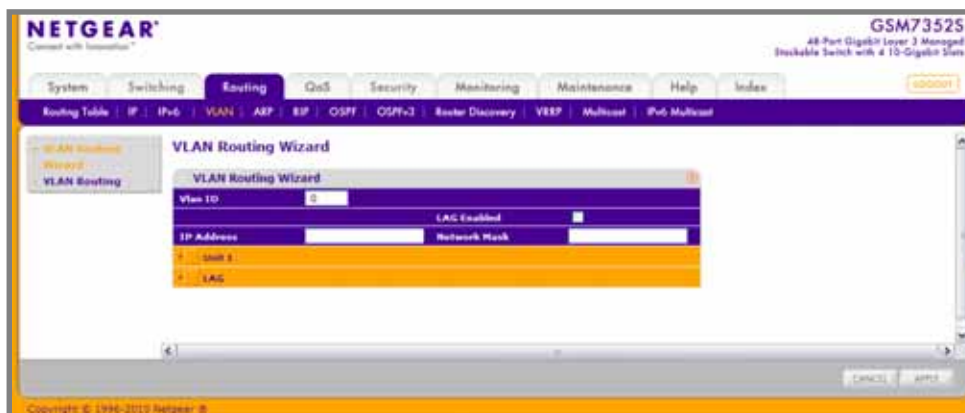
- [VLAN Routing Wizard](#) on page 251
- [VLAN Routing Configuration](#) on page 252

## VLAN Routing Wizard

The VLAN Routing Wizard creates a VLAN, adds selected ports to the VLAN. The VLAN Wizard gives the user the option to add the selected ports as a Link Aggregation (LAG). The Wizard will:

- Create a VLAN and generate a unique name for VLAN.
- Add selected ports to the newly created VLAN and remove selected ports from the default VLAN.
- Create a LAG, add selected ports to a LAG, then add LAG 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 VLAN Routing Wizard page, click **Routing > VLAN > VLAN Routing Wizard**.

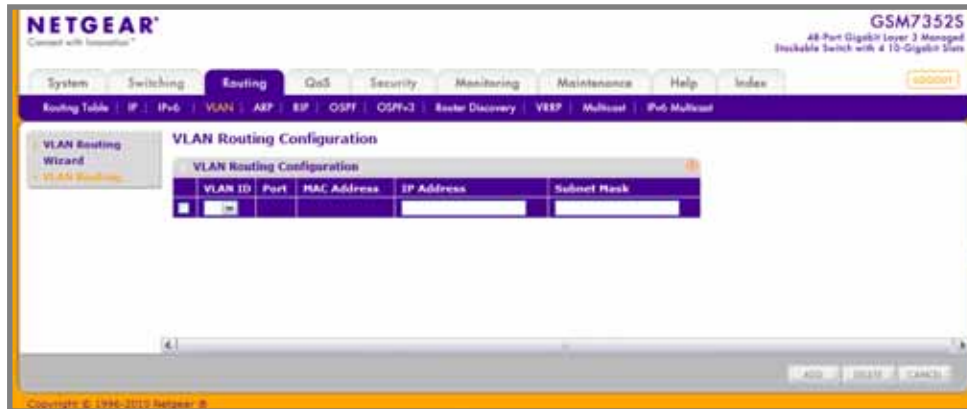


1. Use **VLAN ID** to specify the VLAN Identifier (VID) associated with this VLAN. The range of the VLAN ID is 1 to 4093.
2. Use **Ports** to display selectable physical ports and LAGs (if any). Selected ports will be added to the Routing VLAN. Each port has three modes:
  - **T(Tagged)** - Select the ports on which all frames transmitted for this VLAN will be tagged. The ports that are selected will be included in the VLAN.
  - **U(Untagged)** - Select the ports on which all frames transmitted for this VLAN will be untagged. The ports that are selected will be included in the VLAN.
  - **BLANK(Autodetect)** - Select the ports that may be dynamically registered in this VLAN via GVRP. This selection has the effect of excluding a port from the selected VLAN.
3. Use the **LAG Enabled** option to add selected ports to VLAN as a LAG. The default is No.
4. Use **IP Address** to define the IP address of the VLAN interface.
5. Use **Network Mask** to define the subnet mask of the VLAN interface.

## VLAN Routing Configuration

Use the VLAN Routing Configuration page to configure VLAN Routing interfaces on the system.

To display the VLAN Routing Configuration page, click **Routing > VLAN > VLAN Routing**.



1. Use **VLAN ID** to enter the ID of a VLAN you want to configure for VLAN Routing. The field will display the all IDs of the VLAN configured on this switch.
2. Use **IP Address** to enter the IP Address to be configured for the VLAN Routing Interface.
3. Use **Subnet Mask** to enter the Subnet Mask to be configured for the VLAN Routing Interface.
4. Click **ADD** to add the VLAN Routing Interface specified in the VLAN ID field to the switch configuration.
5. Click **DELETE** to remove the VLAN Routing Interface specified in the VLAN ID field from the switch configuration.

**Table 21.**

Field	Description
Port	The interface assigned to the VLAN for routing.
MAC Address	The MAC Address assigned to the VLAN Routing Interface

## ARP

The ARP protocol associates a layer 2 MAC address with a layer 3 IPv4 address. ProSafe® Managed 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 number of supported ARP entries is platform-dependent.

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.

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

- [Basic](#) on page 253
- [Advanced](#) on page 255

## Basic

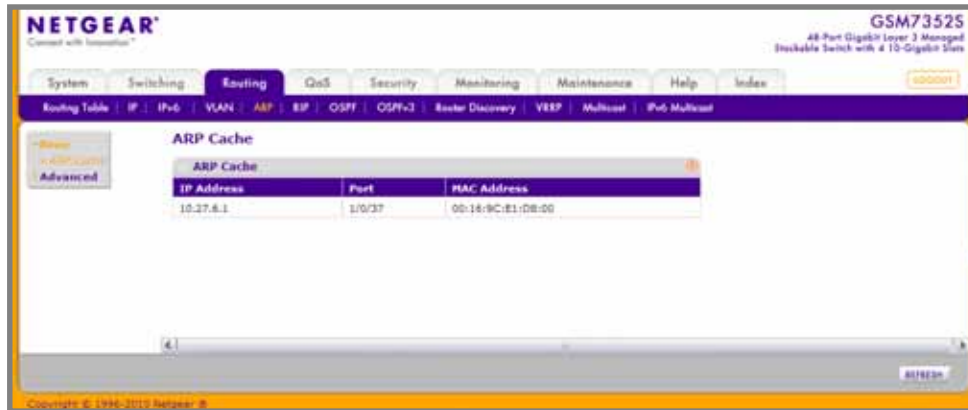
From the Basic link, you can access the following pages:

- [ARP Cache](#) on page 254

## ARP Cache

Use this screen to show ARP entries in the ARP Cache.

To display the ARP Cache page, click **Routing** > **ARP** > **Basic** > **ARP Cache**.



1. Use **Port** to select the associated Unit/Slot/Port of the connection
2. **IP Address** displays the IP address. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
3. **MAC Address** displays the unicast MAC address of the device. The address is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
4. Click **REFRESH** to show the latest IP information.

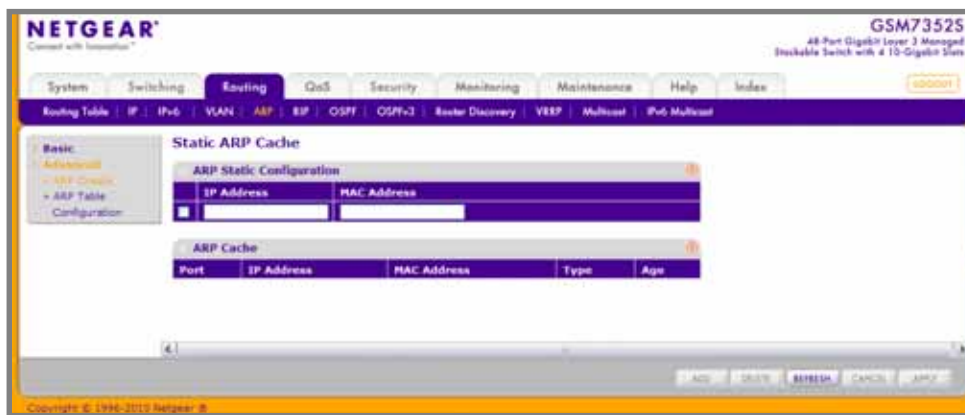
## Advanced

.From the Advanced link, you can access the following pages:

- [Static ARP Cache](#) on page 255
- [ARP Table Configuration](#) on page 257

### Static ARP Cache

To display the Static ARP Cache page, click **Routing > ARP > Advanced > ARP Create**.



### ARP Static Configuration

Use this screen to add an entry to the Address Resolution Protocol table.

1. Use **IP Address** to enter the IP address 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. Use **MAC Address** to specify the unicast MAC address of the device. Enter the address as six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
3. Click **ADD** to add a new static ARP entry to the switch.
4. Click **DELETE** to delete an existing static ARP entry from the switch.
5. Click **APPLY** to change the MAC Address mapping to the IP. Configuration changes take effect immediately.

## ARP Cache

Use this screen to show ARP entries in the ARP Cache.

**Table 22.**

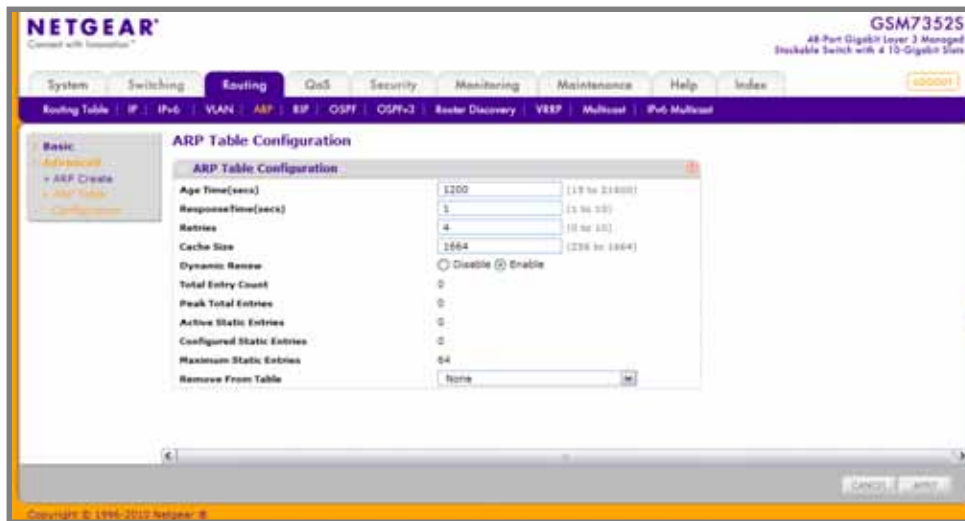
Field	Description
Port	The associated Unit/Slot/Port of the connection
IP Address	Displays the IP address. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
MAC Address	The unicast MAC address of the device. The address is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

Click **REFRESH** to show the latest IP information.

## ARP Table Configuration

You can use this screen to change the configuration parameters for the Address Resolution Protocol Table. You can also use this screen to display the contents of the table.

To display the ARP Table Configuration page, click **Routing > ARP > Advanced > ARP Table Configuration**.



1. Use **Age Time** to enter the value for 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 for this field is 15 to 21600 seconds. The default value for Age Time is 1200 seconds.
2. Use **Response Time** to enter the value for the switch to use for the ARP response time-out. 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 for this field is 1 to 10 seconds. The default value for Response Time is 1 second.
3. Use **Retries** to enter an integer that specifies the maximum number of times an ARP request will be retried. The range for this field is 0 to 10. The default value for Retries is 4.
4. Use **Cache Size** to enter an integer that specifies the maximum number of entries for the ARP cache. The range for this field is 256 to 1664. The default value for Cache Size is 1664.
5. Use **Dynamic Renew** to control whether the ARP component automatically attempts to renew ARP Entries of type Dynamic when they age out. The default setting is Enable.
6. Use **Remove from Table** to remove certain entries from the ARP Table. The choices listed specify the type of ARP Entry to be deleted:
  - **All Dynamic Entries**
  - **All Dynamic and Gateway Entries**
  - **Specific Dynamic/Gateway Entry** - Selecting this allows the user to specify the required IP Address.
  - **Specific Static Entry** - Selecting this allows the user to specify the required IP Address.

- **None** - Selected if the user does not want to delete any entry from the ARP Table.
7. Use **Remove IP Address** to enter the IP Address against the entry that is to be removed from the ARP Table. This appears only if the user selects Specific Dynamic/Gateway Entry or Specific Static Entry in the Remove from Table Drop Down List.

**Table 23.**

Field	Description
Total Entry Count	Total number of Entries in the ARP table.
Peak Total Entries	Highest value reached by Total Entry Count. This counter value is restarted whenever the ARP table Cache Size value is changed.
Active Static Entries	Total number of Active Static Entries in the ARP table.
Configured Static Entries	Total number of Configured Static Entries in the ARP table.
Maximum Static Entries	Maximum number of Static Entries that can be defined.

## RIP

RIP is an Interior Gateway Protocol (IGP) based on the Bellman-Ford algorithm and targeted at smaller networks (network diameter no greater than 15 hops). The routing information is propagated in RIP update packets that are sent out both periodically and in the event of a network topology change. On receipt of a RIP update, depending on whether the specified route exists or does not exist in the route table, the router may modify, delete, or add the route to its route table.

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

- [Basic](#) on page 258
- [Advanced](#) on page 260

### Basic

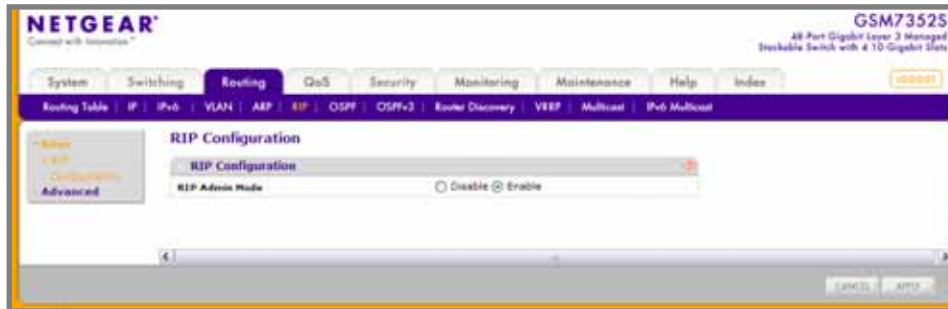
From the Basic link, you can access the following pages:

- [RIP Configuration](#) on page 259

## RIP Configuration

Use the RIP Configuration page to enable and configure or disable RIP in Global mode.

To display the RIP Configuration page, click **Routing > RIP > Basic > RIP Configuration**.



1. Use **RIP Admin Mode** to enable or disable RIP for the switch. The default is enable.
2. Use **Split Horizon Mode** to select none, simple, or poison reverse from the radio buttons. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are:
  - **None** - No special processing for this case.
  - **Simple** - A route will not be included in updates sent to the router from which it was learned.
  - **Poison reverse** - A route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

The default is simple.

3. Use **Auto Summary Mode** to select enable or disable. If you select enable, groups of adjacent routes will be summarized into single entries in order to reduce the total number of entries. The default is disable.
4. Use **Host Routes Accept Mode** to select enable or disable. If you select enable, the router will be accept host routes. The default is enable.
5. Use **Default Information Originate** to enable or disable Default Route Advertise.
6. Use **Default Metric** to set a default for the metric of redistributed routes. This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are 1 to 15.

**Table 24.**

Field	Description
Global Route Changes	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
Global queries	The number of responses sent to RIP queries from other systems.

## Advanced

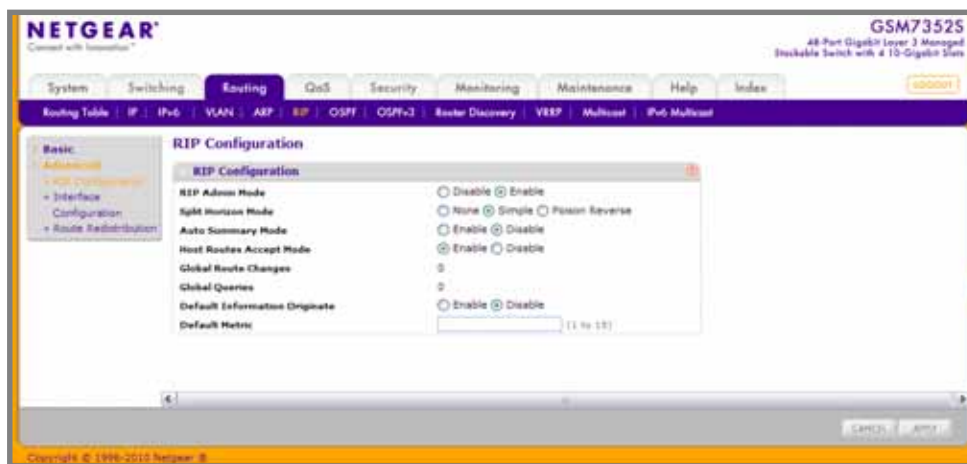
From the Advanced link, you can access the following pages:

- [RIP Configuration](#) on page 260
- [Interface Configuration](#) on page 262
- [Route Redistribution](#) on page 265

### RIP Configuration

Use the RIP Configuration page to enable and configure or disable RIP in Global mode.

To display the RIP Configuration page, click **Routing** > **RIP** > **Advanced** > **RIP Configuration**.





1. Use **RIP Admin Mode** to enable or disable RIP for the switch. The default is enable.
2. Use **Split Horizon Mode** to select none, simple, or poison reverse from the radio buttons. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are:
  - **None** - No special processing for this case.
  - **Simple** - A route will not be included in updates sent to the router from which it was learned.
  - **Poison reverse** - A route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

The default is simple.

3. Use **Auto Summary Mode** to select enable or disable. If you select enable, groups of adjacent routes will be summarized into single entries in order to reduce the total number of entries. The default is disable.
4. Use **Host Routes Accept Mode** to select enable or disable. If you select enable, the router will accept host routes. The default is enable.
5. Use **Default Information Originate** to enable or disable Default Route Advertise.
6. Use **Default Metric** to set a default for the metric of redistributed routes. This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are 1 to 15.

**Table 25.**

Field	Description
Global Route Changes	The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
Global queries	The number of responses sent to RIP queries from other systems.

## Interface Configuration

Use the RIP Interface Configuration page to enable and configure or to disable RIP on a specific interface.

To display the Interface Configuration page, click **Routing > RIP > Advanced > Interface Configuration**.

### Interface Configuration

Interface:

Send Version:

Receive Version:

RIP Admin Mode: ☒ Disable ☐ Enable

Authentication Type:

Interface	IP Address	Send Version	Receive Version	Admin Mode	Link State	Bad Packets Received	Bad Routes Received	Updates Sent
1/0/1	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/2	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/3	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/4	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/5	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/6	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/7	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/8	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/9	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/10	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/11	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/12	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/13	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/14	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/15	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/16	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/17	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/18	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/19	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/20	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/21	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/22	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/23	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/24	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/25	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/26	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/27	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/28	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/29	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/30	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/31	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/32	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/33	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/34	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/35	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/36	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/37	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/38	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/39	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/40	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/41	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/42	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/43	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/44	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/45	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/46	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/47	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/48	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/49	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/50	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/51	0.0.0.0	RIP-2	RIP-2	Disable				
1/0/52	0.0.0.0	RIP-2	RIP-2	Disable				

## RIP Interface Configuration

1. Use **Interface** to select the interface for which data is to be configured.
2. Use **Send Version** to select the version of RIP control packets the interface should send from the pull-down menu. The value is one of the following:
  - **RIP-1** - Send RIP version 1 formatted packets via broadcast.
  - **RIP-1c** - RIP version 1 compatibility mode. Send RIP version 2 formatted packets via broadcast.
  - **RIP-2** - Send RIP version 2 packets using multicast. The default is RIP-2.
  - **None** - No RIP control packets will be sent.
3. Use **Receive Version** to select what RIP control packets the interface will accept from the pull-down menu. The value is one of the following:
  - **RIP-1** - Accept only RIP version 1 formatted packets.
  - **RIP-2** - Accept only RIP version 2 formatted packets. The default is RIP-2.
  - **Both** - Accept packets in either format.
  - **None** - No RIP control packets will be accepted.
4. Use **RIP admin mode** to enable RIP for an interface. The default is Disable.
5. Use **Authentication Type** to select an authentication type other than none by clicking on the 'Configure Authentication' button. You will then see a new screen, where you can select the authentication type from the pull-down menu. The choices are:
  - **None** - This is the initial interface state. If you select this option from the pull-down menu on the second screen you will be returned to the first screen and no authentication protocols will be run.
  - **Simple** - If you select 'Simple' you will be prompted to enter an authentication key. This key will be included, in the clear, in the RIP header of all packets sent on the network. All routers on the network must be configured with the same key.
  - **Encrypt** - If you select 'Encrypt' you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.
6. Use **Authentication Key** to enter the RIP Authentication Key for the specified interface. If you do not choose to use authentication you will not be prompted to enter a key. If you choose 'simple' or 'encrypt' the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges.
7. Use **Authentication Key ID** to enter the RIP Authentication Key ID for the specified interface. If you choose not to use authentication or to use 'simple' you will not be prompted to enter the key ID. If you choose 'encrypt' the key ID may be in range from 0 to 255. The key ID value will be displayed only if you are logged on with Read/Write privileges.
8. Click **CANCEL** to display a new screen where you can select the authentication method for the virtual link.

## RIP Status

**Table 26.**

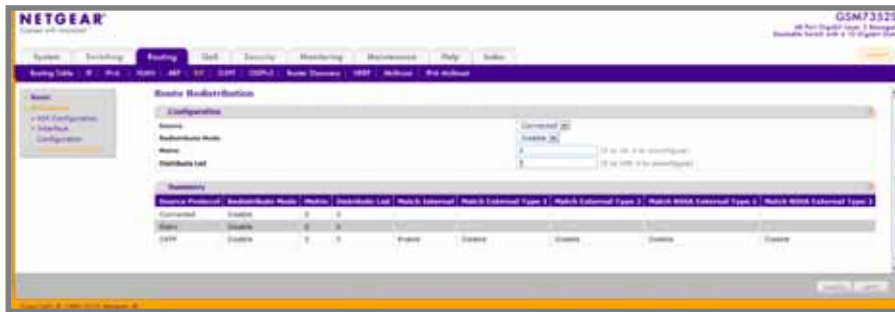
Field	Description
Interface	Displays the interface for which data is configured.
IP Address	Displays the IP Address of the router interface.
Send Version	Displays the version of RIP control packets the interface should send from the pull-down menu. The value is one of the following: <ul style="list-style-type: none"> <li>• RIP-1 - send RIP version 1 formatted packets via broadcast.</li> <li>• RIP-1c - RIP version 1 compatibility mode. Send RIP version 2 formatted packets via broadcast.</li> <li>• RIP-2 - send RIP version 2 packets using multicast. The default is RIP-2.</li> <li>• None: no RIP control packets will be sent.</li> </ul>
Receive Version	Displays what RIP control packets the interface will accept from the pull-down menu. The value is one of the following: <ul style="list-style-type: none"> <li>• RIP-1 - accept only RIP version 1 formatted packets.</li> <li>• RIP-2 - accept only RIP version 2 formatted packets. The default is RIP-2.</li> <li>• Both - accept packets in either format.</li> <li>• None - no RIP control packets will be accepted.</li> </ul>
Admin Mode	Enables RIP for an interface. The default is Disable.
Link State	Indicates whether the RIP interface is up or down.
Bad Packets Received	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
Bad Routes Received	The number of routes, in valid RIP packets, which were ignored for any reason (e.g., unknown address family, or invalid metric).
Updates Sent	The number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.

Click **REFRESH** to show the latest RIP information.

## Route Redistribution

Use the RIP Route Redistribution page to configure which routes are redistributed to other routers using RIP. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

To display the Route Redistribution page, click **Routing > RIP > Advanced > Route Redistribution**.



## RIP Route Redistribution Configuration

This screen can be used to configure the RIP Route Redistribution parameters. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message will be displayed with the list of all the valid values.

1. The Source select box is a dynamic selector and is populated by only those Source Routes that have already been configured for redistribute by RIP. Use Source to configure another Source Route from among the Available Source Routes. The valid values are:
  - **Static**
  - **Connected**
  - **OSPF**
2. Use **Redistribute Mode** to enable or disable RIP redistribute mode. The default value is disable.
3. Use **Metric** to specify the Metric of redistributed routes for the given Source Route.
4. Use **Distribute List** to set the Access List that filters the routes to be redistributed by the destination protocol. Only permitted routes are redistributed. If this command refers to a non-existent access list, all routes are permitted. The valid values for Access List IDs are 1 to 199. When used for route filtering, the only fields in an access list that get used are:
  - **Source IP Address and netmask**
  - **Destination IP Address and netmask**
  - **Action (permit or deny)**

All other fields (source and destination port, precedence, tos, etc.) are ignored.

The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route. (Note that a 1 in the mask indicates a “don't care” in the corresponding address bit.)

When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the destination of the route. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route's destination mask are significant for the filtering operation.

## RIP Route Redistribution Summary

This screen displays the RIP Route Redistribution Configurations.

**Table 27.**

Field	Description
Source	The Source Route to be Redistributed by RIP.
Metric	The Metric of redistributed routes for the given Source Route. Displays “Unconfigured” when not configured.
Match	List of Routes redistributed when “OSPF” is selected as Source. The list may include one or more of: <ul style="list-style-type: none"> <li>• Internal: Sets Internal OSPF Routes to be redistributed</li> <li>• External Type 1: Sets External Type 1 OSPF Routes to be redistributed</li> <li>• External Type 2: Sets External Type 2 OSPF Routes to be redistributed</li> <li>• NSSA External Type 1: Sets NSSA External Type 1 OSPF Routes to be redistributed</li> <li>• NSSA External Type 2: Sets NSSA External Type 2 OSPF Routes to be redistributed</li> </ul>
Distribute List	The Access List that filters the routes to be redistributed by the Destination Protocol. Displays 0 when not configured.

## OSPF

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

- [Basic](#) on page 267
- [Advanced](#) on page 268

## Basic

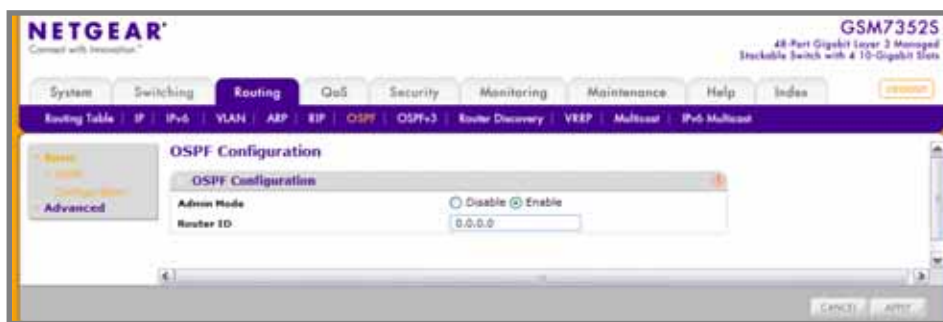
From the Basic link, you can access the following pages:

- [OSPF Configuration](#) on page 267

### OSPF Configuration

Use the OSPF Configuration page to enable OSPF on a router and to configure the related OSPF settings.

To display the OSPF Configuration page, click **Routing** > **OSPF** > **Basic** > **OSPF Configuration**.



1. Use **Router ID** to specify a 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). To change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
2. Use **Admin Mode** to select enable or disable. If you select enable, OSPF will be activated for the switch. The default value is disable. You must configure a Router ID before OSPF can become operational; see step 1 or by issuing the CLI command:  
(Config-router) #router-id.

## Advanced

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

- [\*OSPF Configuration\*](#) on page 269
- [\*Common Area Configuration\*](#) on page 272
- [\*Stub Area Configuration\*](#) on page 274
- [\*NSSA Area Configuration\*](#) on page 276
- [\*Area Range Configuration\*](#) on page 278
- [\*Interface Configuration\*](#) on page 279
- [\*OSPF Interface Statistics\*](#) on page 284
- [\*OSPF Neighbor Table\*](#) on page 288
- [\*Link State Database\*](#) on page 291
- [\*Virtual Link Configuration\*](#) on page 293
- [\*Route Redistribution\*](#) on page 295



## OSPF Configuration

Use the OSPF Configuration page to enable OSPF on a router and to configure the related OSPF settings.

To display the OSPF Configuration page, click **Routing > OSPF > Advanced > OSPF Configuration**.

### Default Route Advertise Configuration

1. When **Default Information Originate** is enabled, OSPF originates an external LSA advertising a default route (0.0.0.0/0.0.0.0).
2. **Always** - If Default Information Originate is enabled, but the Always option is FALSE, OSPF will only originate a default route if the router already has a default route in its routing table. Set Always to TRUE to force OSPF to originate a default route regardless of whether the router has a default route.
3. Use **Metric** to specify the metric of the default route. The range of valid values is 0 to 16777214.
4. Use **Metric Type** to set the OSPF metric type of the default route. Two types are supported:
  - **External Type 1**
  - **External Type 2** - Default is External Type 2.

## OSPF Configuration

1. Use **Router ID** to specify the 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
2. Use **Admin Mode** to select enable or disable. If you select enable, OSPF will be activated for the switch. The default value is disable. You must configure a Router ID before OSPF can become operational; see step 1 or by issuing the CLI command:  
(Config-router)#router-id.
3. Enable or disable **RFC 1583 Compatibility** to specify the preference rules that will be used when choosing among multiple AS-external-LSAs advertising the same destination. If you select enable, the preference rules will be those defined by RFC 1583. If you select disable, the preference rules will be those defined in Section 16.4.1 of the OSPF-2 standard (RFC 2328), which will prevent routing loops when AS-external-LSAs for the same destination have been originated from different areas. The default value is 'enable'. All routers in the OSPF domain must be configured the same. If all OSPF routers are capable of operating according to RFC 2328, RFC 1583 Compatibility should be disabled.
4. Set the **Opaque LSA Status** parameter to enable if OSPF should store and flood opaque LSAs. An opaque LSA is used for flooding user-defined information within an OSPF router domain.
5. Use **Exit Overflow Interval(secs)** to specify how long OSPF must wait before attempting to leave overflow state. When the number of non-default external LSAs exceeds a configured limit, the router enters an overflow state as defined in RFC 1765. In overflow state, OSPF cannot originate non-default external LSAs. If the Exit Overflow Interval is 0, OSPF will not leave overflow state until it is disabled and re-enabled. The range is 0 to 2,147,483,647 seconds.
6. Use **SPF DelayTime(secs)** to specify the number of seconds from when OSPF receives a topology change to the start of the next SPF calculation. Delay Time is an integer from 0 to 65535 seconds. The default time is 5 seconds. A value of 0 means that there is no delay; that is, the SPF calculation is started upon a topology change.
7. Use **SPF HoldTime(secs)** to specify the minimum time in seconds between two consecutive SPF calculations. The range is 0 to 65,535 seconds. The default time is 10 seconds. A value of 0 means that there is no delay; that is, two SPF calculations can be done, one immediately after the other.
8. Use **External LSDB Limit** to set the number of the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit none-default AS-external-LSAs in database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for limit is -1 to 2147483647.
9. Use **Default Metric** to set a default for the metric of redistributed routes. This field is blank if a default metric has not been configured. The range of valid values is 1 to 16777214.
10. Use **Maximum Paths** to set the number of paths that OSPF can report for a given destination. The range of valid values is 1 to 4.
11. Use **AutoCost Reference Bandwidth** to configure the auto-cost reference-bandwidth to control how OSPF calculates link cost. Specify the reference bandwidth in megabits per

second. Unless a link cost is configured, the link cost is computed by dividing the reference bandwidth by the interface bandwidth. The range is 1 to 4294967.

12. Use **Default Passive Setting** to configure the global passive mode setting for all OSPF interfaces. Configuring this field overwrites any present interface level passive mode setting. OSPF does not form adjacencies on passive interfaces, but does advertise attached networks as stub networks.

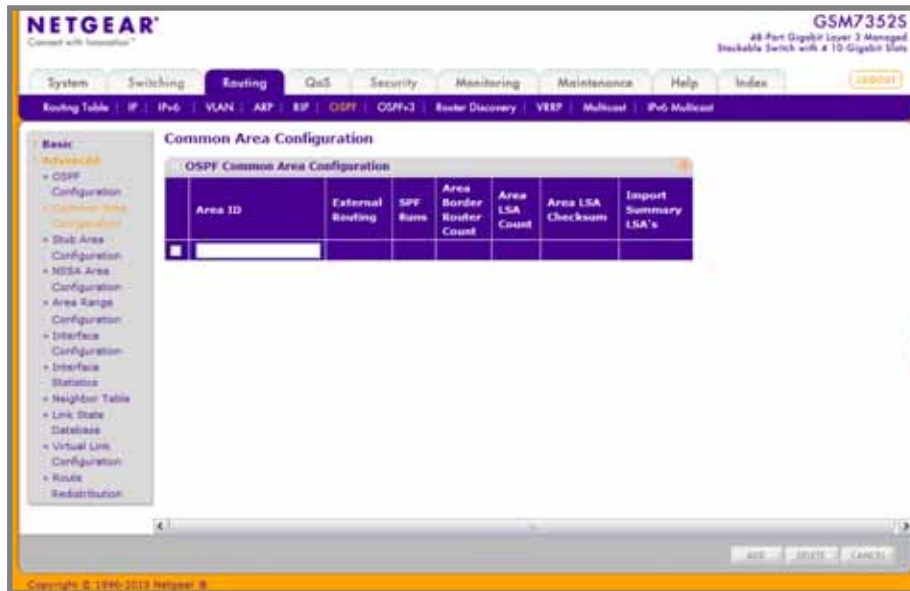
**Table 28.**

Field	Description
ASBR Mode	The router is an Autonomous System Boundary Router if it is configured to redistribute routes from another protocol, or if it is configured to originate an external LSA advertising the default route.
ABR Status	The router is an Area Border Router if it has active non-virtual interfaces in two or more OSPF areas.
External LSA Count	The number of external (LS type 5) LSAs (link state advertisements) in the link state database.
External LSA Checksum	The sum of the LS checksums of the external LSAs (link state advertisements) contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers. This value is in hexadecimal.
AS_OPAQUE LSA Count	The number of opaque LSAs with domain wide flooding scope.
AS_OPAQUE LSA Checksum	The sum of the LS checksums of the opaque LSAs with domain wide flooding scope. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers. This value is in hexadecimal.
New LSAs Originated	In any given OSPF area, a router will originate several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it will originate network-LSAs for those networks. This value represents the number of LSAs originated by this router.
LSAs Received	The number of LSAs (link state advertisements) received that were determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.

## Common Area Configuration

The OSPF Common Area Configuration page lets you create a Common Area Configuration once you have enabled OSPF on an interface. At least one router must have OSPF enabled for this web page to display.

To display the Common Area Configuration page, click **Routing > OSPF > Advanced > Common Area Configuration**.



1. Use **Area ID** to enter the OSPF area ID. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.

**Table 29.**

Field	Description
Aging Interval	The Link State Advertisement (LSA) aging timer interval.
External Routing	A definition of the router's capabilities for the area, including whether or not AS-external-LSAs are flooded into/throughout the area. If the area is a stub area, then these are the possible options for which you may configure the external routing capability, otherwise the only option is "Import External LSAs": <ul style="list-style-type: none"> <li>• Import External LSAs: Import and propagate external LSAs</li> <li>• Import No LSAs: Do not import and propagate external LSAs</li> </ul>
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Import Summary LSAs	The summary LSAs will be enabled/disabled imported into this area.

Click **ADD** to configure the area as a common area.

Click **DELETE** to delete the common area.

## Stub Area Configuration

To display the Stub Area Configuration page, click **Routing** > **OSPF** > **Advanced** > **Stub Area Configuration**.

**NETGEAR**  
GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Routing Table IP IPv6 VLAN ARP RIP **OSPF** OSPFv3 Router Discovery VRRP Multicast IPv6 Multicast

Basic  
Advanced  
OSPF  
Configuration  
Common Area Configuration  
Stub Area Configuration  
NLSA Area Configuration  
Area Range Configuration  
Interface Configuration  
Interface Status  
Neighbor Table  
Link State Database  
Virtual Link Configuration  
Route Redistribution

**Stub Area Configuration**

OSPF Stub Area Configuration

Area ID	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSA's	Default Cost	Type of Service
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

4

ADD DELETE CANCEL APPLY

Copyright © 1999-2013 Netgear, Inc.

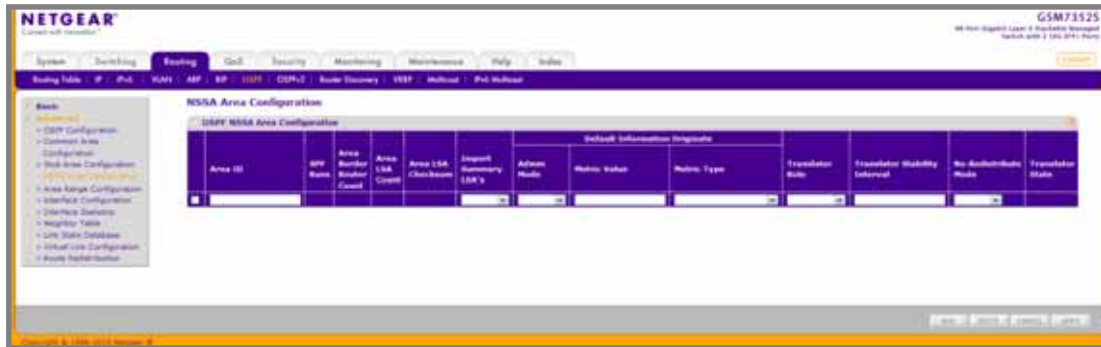
1. Use **Area ID** to enter the OSPF area ID. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Use **Import Summary LSAs** to select enable or disable. If you select enable, summary LSAs will be imported into stub areas.
3. Use **Default Cost** to enter the metric value you want applied for the default route advertised into the stub area. Valid values range from 1 to 16,777,215.
4. Click **ADD** to configure the area as a stub area.
5. Click **DELETE** to delete the stub area designation. The area will be returned to normal state.

**Table 30.**

Field	Description
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Type of Service	This field is the normal TOS associated with the stub metric.

## NSSA Area Configuration

To display the NSSA Area Configuration page, click **Routing** > **OSPF**> **Advanced** > **NSSA Area Configuration**.



1. Use **Area ID** to enter the OSPF area ID. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Use **Import Summary LSAs** to select enable or disable. If you select enable, summary LSAs will be imported into NSSA areas.
3. The **Default Information Originate** area displays the default Route Information. These options will permit a user to advertise a default route into the NSSA when Import Summary LSAs is disabled. They can also be applied by the CLI command `area (area-id) nssa default-info-originate` in the ip router OSPF config mode.
  - Use **Admin Mode** to enable or disable the default information originate. Valid values are True or False.
  - Use **Metric Value** to set the Default Metric value for default information originate. The valid range of values is 1 to 16777214.
  - Use **Metric Type** to select the type of metric specified in the Metric Value field:
    - **Comparable Cost** - External Type 1 metrics that are comparable to the OSPF metric
    - **Non-comparable Cost** - External Type 2 metrics that are assumed to be larger than the cost of the OSPF metric.
4. Use **Translate Role** to select the translator role of the NSSA:
  - **always** - Cause the router to assume the role of the translator the instant it becomes a border router.
  - **candidate** - Cause the router to participate in the translator election process when it attains border router status.
5. Use **Translate Stability Interval** to configure the translator of the NSSA. The value is the period of time that an elected translation continues to perform its duties after it determines that its translator status has been deposed by another router.
6. Use **No-Redistribute Mode** to configure the NSSA ABR so that learned external routes will not be redistributed to the NSSA.
7. Click **ADD** to configure the area as a NSSA area.



8. Click **DELETE** to delete the NSSA area designation. The area will be returned to normal state.

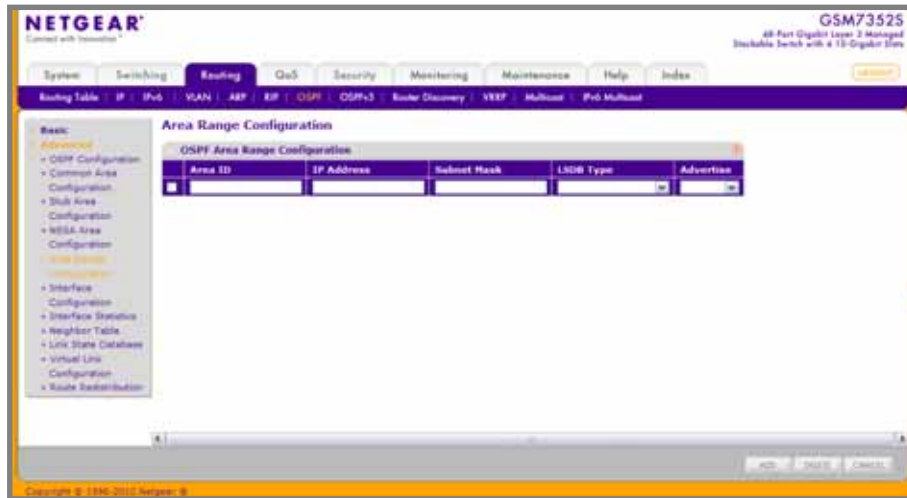
**Table 31.**

Field	Description
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Translator State	The field tells you if and how the NSSA border router translates type-7 into type-5: <ul style="list-style-type: none"> <li>• enabled: The NSSA border router's translator role has been set to always.</li> <li>• elected: The candidate NSSA border router is translating type-7 LSAs into type-5.</li> <li>• disabled: The candidate NSSA border router is NOT translating type-7 LSAs into type-5.</li> </ul>

## Area Range Configuration

Use the OSPF Area Range Configuration page to configure and display an area range for a specified NSSA.

To display the Area Range Configuration page, click **Routing** > **OSPF** > **Advanced** > **Area Range Configuration**.

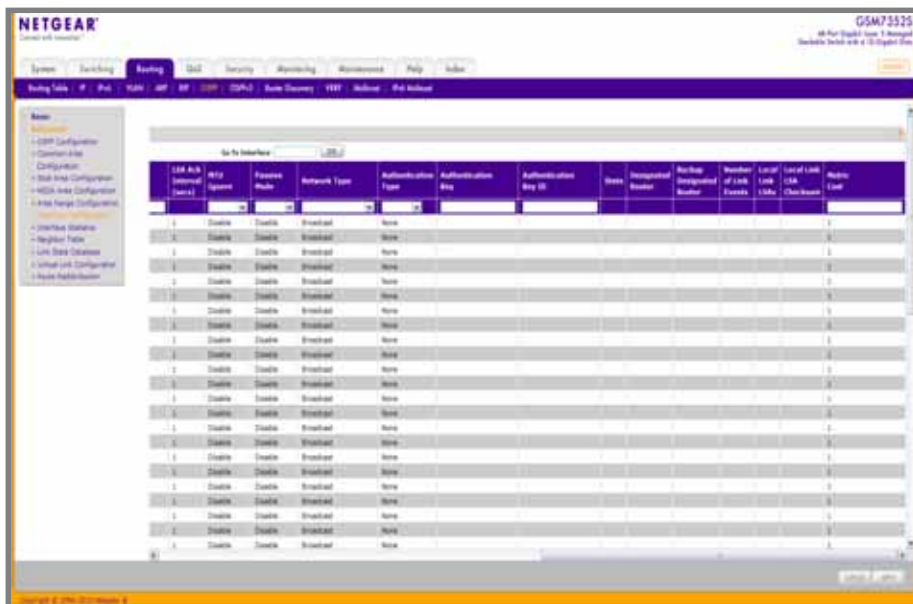
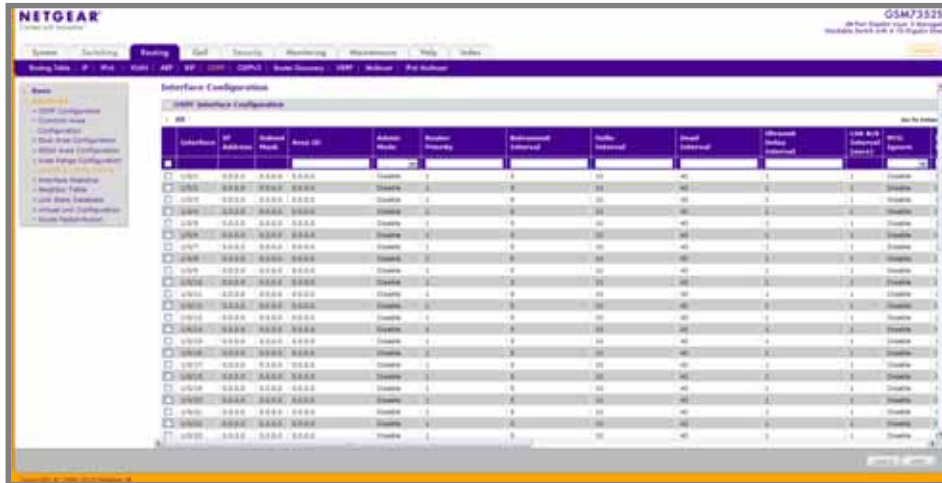


1. Use **Area ID** to specify the area for which data is to be configured.
2. Use **IP address** to enter the IP Address for the address range for the selected area.
3. Use **Subnet Mask** to enter the Subnet Mask for the address range for the selected area.
4. Use **LSDB Type** to select the type of Link Advertisement associated with the specified area and address range. The default type is 'Network Summary'.
5. Use **Advertise** to select Enable or Disable. If you select Enable, the address range will be advertised outside the area via a Network Summary LSA. The default is Enable.
6. Click **ADD** to add the new address range to the switch.
7. Click **DELETE** to remove the specified address range from the area configuration.

## Interface Configuration

Use the OSPF Interface Configuration page to configure an OSPF interface.

To display the Interface Configuration page, click **Routing > OSPF > Advanced > Interface Configuration**.



1. **Interface** - The interface for which data is to be displayed or configured.
2. Use **Area ID** to enter the 32-bit integer in dotted decimal format that uniquely identifies the OSPF area to which the selected router interface connects. If you assign an Area ID which does not exist, the area will be created with default values.
3. Use **Admin Mode\*** to select enable or disable. The default value is 'disable.' You can configure OSPF parameters without enabling OSPF Admin Mode, but they will have no effect until you enable Admin Mode. The following information will be displayed only if the

Admin Mode is enabled: State, Designated Router, Backup Designated Router, Number of Link Events, LSA ACK Interval, and Metric Cost. For OSPF to be fully functional, you must enter a valid IP Address and Subnet Mask via the Interface IP Configuration page or through the CLI command `ip address <ipaddr> <subnet-mask>`.

---

**Note:** \*Once OSPF is initialized on the router, it will remain initialized until the router is reset.

---

4. Use **Router Priority** to enter the OSPF priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. The default is 1, which is the highest router priority. A value of '0' indicates that the router is not eligible to become the designated router on this network.
5. Use **Retransmit Interval** to enter the OSPF retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.
6. Use **Hello Interval** to enter the OSPF hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.
7. Use **Dead Interval** to enter the OSPF dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should be a multiple of the Hello Interval, e.g., 4. Valid values range from 1 to 2147483647. The default is 40.
8. Use **Iftransit Delay Interval** to enter the OSPF Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
9. Use **MTU Ignore** to disable OSPF MTU mismatch detection on received database description packets. Default value is Disable (MTU mismatch detection is enabled).
10. Use **Passive Mode** to make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default.
11. Use **Network Type** to set the OSPF network type on the interface to broadcast or point-to-point. OSPF only selects a designated router and originates network LSAs for broadcast networks. No more than two OSPF routers may be present on a point-to-point link. The default network type for Ethernet interfaces is broadcast.

12. Use **Authentication Type** to select an authentication type other than none. You can select the authentication type from the pull-down menu. The choices are:
- **None**: This is the initial interface state. If you select this option from the pull-down menu, no authentication protocols will be run.
  - **Simple** - If you select 'Simple' you will be prompted to enter an authentication key. This key will be included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
  - **Encrypt** - If you select 'Encrypt' you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.
13. Use **Authentication Key** to enter the OSPF Authentication Key for the specified interface. If you do not choose to use authentication you will not be prompted to enter a key. If you choose 'simple' authentication you cannot use a key of more than eight octets. If you choose 'encrypt' the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges, otherwise it will be displayed as asterisks.
14. Use **Authentication Key ID** to enter the ID to be used for authentication. You will only be prompted to enter an ID when you select 'Encrypt' as the authentication type. The ID is a number between 0 and 255, inclusive.
15. Use **Metric Cost** to enter the link cost. OSPF uses this value in computing shortest paths. The range is from 1 to 65,535.

Table 32.

Field	Description
IP Address	The IP address of the interface.
Subnet Mask	The network mask, indicating the portion of the IP address that identifies the attached network.
LSA Ack Intervlan (secs)	The number of seconds to wait before sending a delayed acknowledgement.

Table 32.

Field	Description
State	<p>The current state of the selected router interface. One of:</p> <ul style="list-style-type: none"> <li>• <b>Down:</b> This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface.</li> <li>• <b>Loopback:</b> In this state, the router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. However, it may still be desirable to gain information on the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets may still be addressed to an interface in Loopback state. To facilitate this, such interfaces are advertised in router-LSAs as single host routes, whose destination is the IP interface address.</li> <li>• <b>Waiting:</b> The router is trying to determine the identity of the (Backup) Designated Router for the network by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.</li> </ul>
Designated Router	<p>This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network-LSA will contain links to all routers (including the Designated Router itself) attached to the network.</p>
Backup Designated Router	<p>This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the LSA flooding, as compared to the Designated Router.</p>
Other Designated Router	<p>The interface is connected to a broadcast on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.</p>

**Table 32.**

Field	Description
Designated Router	The identity of the Designated Router for this network, in the view of the advertising router. The Designated Router is identified here by its router ID. The value 0.0.0.0 means that there is no Designated Router. This field is only displayed if the OSPF admin mode is enabled.
Backup Designated Router	The identity of the Backup Designated Router for this network, in the view of the advertising router. The Backup Designated Router is identified here by its router ID. Set to 0.0.0.0 if there is no Backup Designated Router.
Number of Link Events	This is the number of times the specified OSPF interface has changed its state.
Local Link LSAs	The number of opaque LSAs whose flooding scope is the link on this interface.
Local Link LSA Checksum	The sum of the checksums of local link LSAs for this link.

## OSPF Interface Statistics

This screen displays statistics for the selected interface. The information will be displayed only if OSPF is enabled.

To display the OSPF Interface Statistics page, click **Routing > OSPF > Advanced > OSPF Interface Statistics**.

**OSPF Interface Statistics**

**OSPF Interface Selection**

Interface: 1/0/1

**OSPF Interface Statistics**

- OSPF Area ID
- Area Border Router Count
- AS Border Router Count
- Area LSA Count
- IP Address
- Interface Events
- Virtual Events
- Neighbor Events
- External LSA Count
- Sent Packets
- Received Packets
- Discards
- Bad Version
- Source Not On Local Subnet
- Virtual Link Not Found
- Area Mismatch
- Invalid Destination Address
- Wrong Authentication Type
- Authentication Failure
- No Neighbor at Source Address
- Invalid OSPF Packet Type
- Hellos Ignored
- Hellos Sent
- Hellos Received
- DD Packets Sent
- DD Packets Received
- LS Requests Sent
- LS Requests Received
- LS Updates Sent
- LS Updates Received
- LS Acknowledgements Sent
- LS Acknowledgements Received

**Interface** - Selects the interface for which data is to be displayed.



**Table 33.**

Field	Description
OSPF Area ID	The OSPF area to which the selected router interface belongs. An OSPF Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which the interface connects.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
AS Border Router Count	The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IP Address	The IP address of the interface.
Interface Events	The number of times the specified OSPF interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that have occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
Sent packets	The number of OSPF packets transmitted on the interface.
Received packets	The number of valid OSPF packets received on the interface.
Discards	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
Source Not On Local Subnet	The number of received packets discarded because the source IP address is not within a subnet configured on a local interface.
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.

**Table 33.**

Field	Description
Area Mismatch	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrouters or AllSpfRouters multicast addresses.
Wrong Authentication Type	The number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface.
Authentication Failure	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
Invalid OSPF Packet Type	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.
Hellos Sent	The number of Hello packets sent on this interface by this router.
Hellos Received	The number of Hello packets received on this interface by this router.
DD Packets Sent	The number of Database Description packets sent on this interface by this router.
DD Packets Received	The number of Database Description packets received on this interface by this router.
LS Requests Sent	The number of LS Requests sent on this interface by this router.
LS Requests Received	The number of LS Requests received on this interface by this router.
LS Updates Sent	The number of LS updates sent on this interface by this router.

**Table 33.**

Field	Description
LS Updates Received	The number of LS updates received on this interface by this router.
LS Acknowledgements Sent	The number of LS acknowledgements sent on this interface by this router.
LS Acknowledgements Received	The number of LS acknowledgements received on this interface by this router.

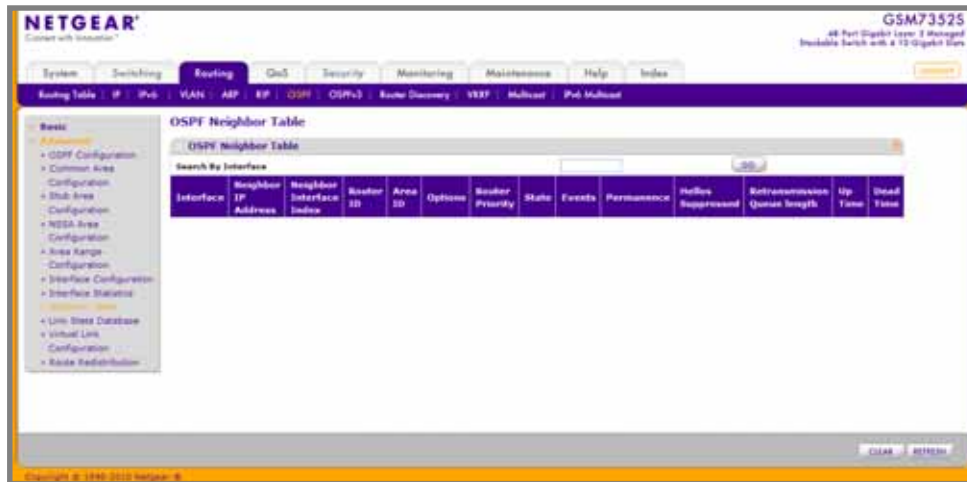
Click **REFRESH** to refresh the data on the screen to show the latest interface statistics.

Click **CLEAR** to clear all the statistics of the OSPF interface.

## OSPF Neighbor Table

This screen displays the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below will only be displayed if OSPF is enabled.

To display the OSPF Neighbor Table page, click **Routing > OSPF > Advanced > OSPF Neighbor Table**.



**Table 34.**

Field	Description
Interface	Displays the interface for which data is to be displayed or configured. Slot 0 is the base unit.
Router ID	A 32-bit integer in dotted decimal format representing the neighbor interface.
Neighbor IP Address	The IP address of the neighboring router's interface to the attached network. It is used as the destination IP address when protocol packets are sent as unicasts along this adjacency. Also used in router-LSAs as the Link ID for the attached network if the neighboring router is selected to be designated router. The Neighbor IP address is learned when Hello packets are received from the neighbor. For virtual links, the Neighbor IP address is learned during the routing table build process.
Area ID	The area ID of the OSPF area associated with the interface.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.

Table 34.

Field	Description
Neighbor Interface Index	A Unit/Slot/Port identifying the neighbor interface index.
State	<p>The state of a neighbor can be the following:</p> <ul style="list-style-type: none"> <li>• Down - This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor. On NBMA networks, Hello packets may still be sent to "Down" neighbors, although at a reduced frequency.</li> <li>• Attempt - This state is only valid for neighbors attached to NBMA networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor. This is done by sending the neighbor Hello packets at intervals of Hello Interval.</li> <li>• Init - In this state, a Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor (i.e., the router itself did not appear in the neighbor's Hello packet). All neighbors in this state (or greater) are listed in the Hello packets sent from the associated interface.</li> <li>• 2-Way - In this state, communication between the two routers is bidirectional. This has been assured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The (Backup) Designated Router is selected from the set of neighbors in state 2-Way or greater.</li> <li>• Exchange Start - This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.</li> <li>• Exchange - In this state the router is describing its entire link state database by sending Database Description packets to the neighbor. In this state, Link State Request Packets may also be sent asking for the neighbor's more recent LSAs. All adjacencies in Exchange state or greater are used by the flooding procedure. These adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.</li> <li>• Loading - In this state, Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.</li> <li>• Full - In this state, the neighboring routers are fully adjacent. These adjacencies will now appear in router-LSAs and network-LSAs.</li> </ul>
Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Permanence	This variable displays the status of the entry. 'dynamic' and 'permanent' refer to how the neighbor became known.
Hellos Suppressed	This indicates whether Hellos are being suppressed to the neighbor.
Retransmission Queue Length	An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.
Up Time	Neighbor uptime; how long since the adjacency last reached the Full state.
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

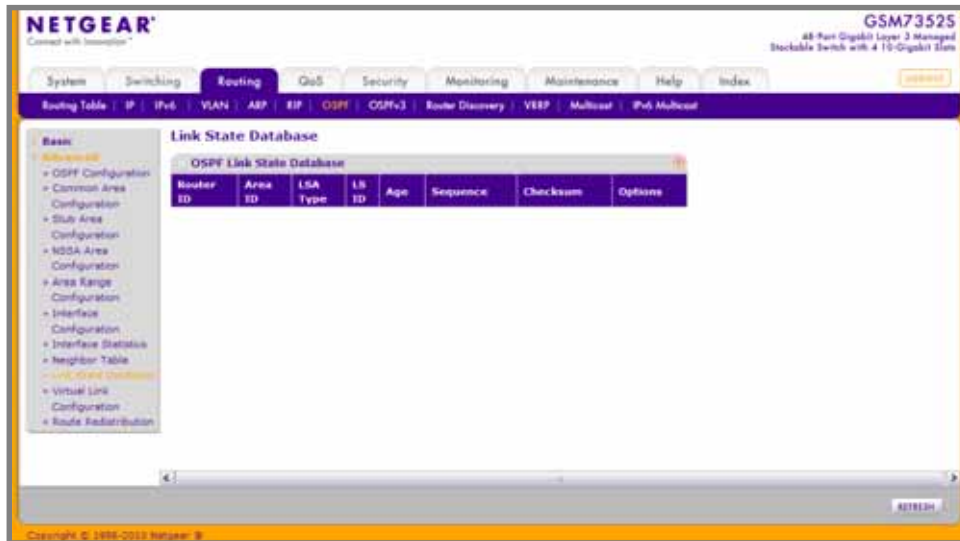
Click **REFRESH** to show the latest DHCP bindings information.

Click **CLEAR** to clear all the neighbors in the table.

## Link State Database

Use the OSPF Link State Database page to display OSPF link state information.

To display the Link State Database page, click **Routing > OSPF > Advanced > Link State Database**.



**Table 35.**

Field	Description
Router ID	The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the IP Configuration page. If you want to change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
Area ID	The ID of an OSPF area to which one of the router interfaces is connected. An Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which an interface is connected.
LSA Type	The format and function of the link state advertisement. One of the following: <ul style="list-style-type: none"> <li>• Router Links</li> <li>• Network Links</li> <li>• Network Summary</li> <li>• ASBR Summary</li> <li>• AS-external</li> </ul>

Table 35.

Field	Description
LS ID	The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.
Options	<p>The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. The options are:</p> <ul style="list-style-type: none"> <li>• Q: This enables support for QoS Traffic Engineering.</li> <li>• E: This describes the way AS-external-LSAs are flooded.</li> <li>• MC: This describes the way IP multicast datagrams are forwarded according to the standard specifications.</li> <li>• O: This describes whether Opaque-LSAs are supported.</li> <li>• V: This describes whether OSPF++ extensions for VPN/COS are supported.</li> </ul>

Click **REFRESH** to show the latest OSPF Link State information.



## Virtual Link Configuration

Use the OSPF Virtual Link Configuration page to create or configure virtual interface information for a specific area and neighbor. A valid OSPF area must be configured before this page can be displayed.

To display the Virtual Link Configuration page, click **Routing > OSPF > Advanced > Virtual Link Configuration**.

Virtual Link Configuration					
:: OSPF Virtual Link Configuration					
	Area ID	Neighbor Router ID	Hello Interval	Dead Interval	Iftransit Delay Interval
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Retransmit Interval	Authentication Type
<input type="text"/>	<input type="text"/>

1. Use **Area ID** to enter the area ID of the OSPF area. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.
2. Use **Neighbor Router ID** to enter the neighbor portion of a Virtual Link specification. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.
3. Use **Hello Interval** to enter the OSPF hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.
4. Use **Dead Interval** to enter the OSPF dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should be a multiple of the Hello Interval, e.g., 4. Valid values range from 1 to 2147483647. The default is 40.
5. Use **Iftransit Delay Interval** to enter the OSPF Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
6. Use **Retransmit Interval** to enter the OSPF retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.
7. Use **Authentication Type** to select an authentication type other than none by clicking on the 'Configure Authentication' button. You will then see a new screen, where you can select the authentication type from the pull-down menu. The choices are:
  - **None** - This is the initial interface state. If you select this option from the pull-down menu on the second screen you will be returned to the first screen.

- **Simple** - If you select 'Simple' you will be prompted to enter an authentication key. This key will be included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
  - **Encrypt** - If you select 'Encrypt' you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.
8. Use **Authentication Key** to enter the OSPF Authentication Key for the specified interface. If you do not choose to use authentication you will not be prompted to enter a key. If you choose 'simple' authentication you cannot use a key of more than eight octets. If you choose 'encrypt' the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges, otherwise it will be displayed as asterisks.
  9. Use **Authentication ID** to enter the ID to be used for authentication. You will only be prompted to enter an ID when you select 'Encrypt' as the authentication type. The ID is a number between 0 and 255, inclusive.
  10. Click **ADD** to add a new virtual link to the switch.
  11. Click **DELETE** to remove the specified virtual link from the switch configuration.

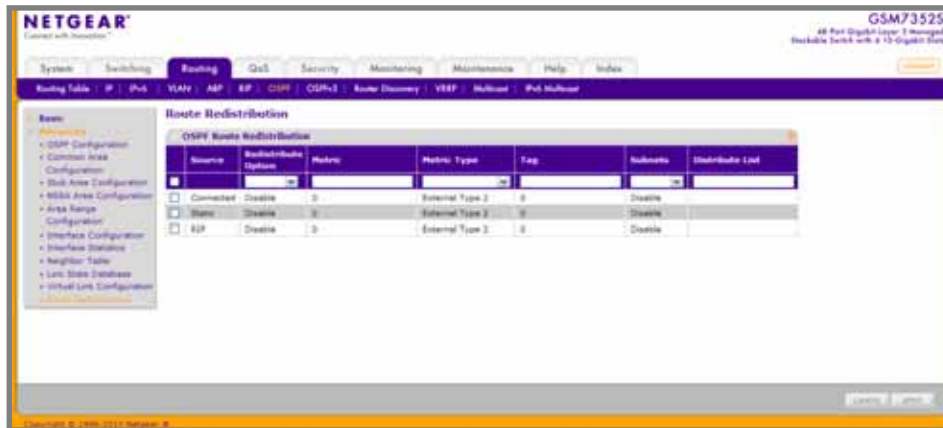
Table 36.

Field	Description
Neighbor State	<p>The OSPF interface state, it can be these values:</p> <ul style="list-style-type: none"> <li>• <b>Down:</b> This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface.</li> <li>• <b>Waiting:</b> The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.</li> <li>• <b>Point-to-Point:</b> The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every HelloInterval seconds.</li> <li>• <b>Designated Router:</b> This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network.</li> <li>• <b>Backup Designated Router:</b> This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.</li> <li>• <b>Other Designated Router:</b> The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.</li> </ul>
Neighbor State	The state of the Virtual Neighbor Relationship.

## Route Redistribution

This screen can be used to configure the OSPF Route Redistribution parameters. The allowable values for each fields are displayed next to the field. If any invalid values are entered, an alert message will be displayed with the list of all the valid values.

To display the Route Redistribution page, click **Routing > OSPF > Advanced > Route Redistribution**.



1. Use **Source** to list available source routes that have not previously been configured for redistribution by OSPF. The valid values are 'Static', 'Connected', and 'RIP'.
2. Use **Redistribute Option** to enable or disable the redistribution for the selected source protocol.
3. Use **Metric** to set the metric value to be used as the metric of redistributed routes. This field displays the metric if the source was pre-configured and can be modified. The valid values are 0 to 16777214.
4. Use **Metric Type** to set the OSPF metric type of redistributed routes.
5. Use **Tag** to set the tag field in routes redistributed. This field displays the tag if the source was pre-configured, otherwise 0 and can be modified. The valid values are 0 to 4294967295.
6. Use **Subnets** to set whether the subnetted routes should be redistributed.
7. Use **Distribute List** to set the Access List that filters the routes to be redistributed by the destination protocol. Only permitted routes are redistributed. If this command refers to a non-existent access list, all routes are permitted. The valid values for Access List IDs are 1 to 199.

When used for route filtering, the only fields in an access list that get used are:

- Source IP Address and netmask
- Destination IP Address and netmask
- Action (permit or deny)

All other fields (source and destination port, precedence, tos, and so on) are ignored.

The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route. (Note that a 1 in the mask indicates a “don't care” in the corresponding address bit.)

When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the destination of the route. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route's destination mask are significant for the filtering operation.

## OSPFv3

OSPFv3 is the Open Shortest Path First routing protocol for IPv6. It is similar to OSPFv2 in its concept of a link state database, intra/inter area, and AS external routes and virtual links. It differs from its IPv4 counterpart in a number of respects, including the following: peering is done via link-local addresses; the protocol is link-based rather than network-based; and addressing semantics have been moved to leaf LSAs, which eventually allow its use for both IPv4 and IPv6. Point-to-point links are also supported in order to enable operation over tunnels.

It is possible to enable OSPF and OSPFv3 at the same time. OSPF works with IPv4 and OSPFv3 works with IPv6.

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

- [Basic](#) on page 296
- [Advanced](#) on page 298

### Basic

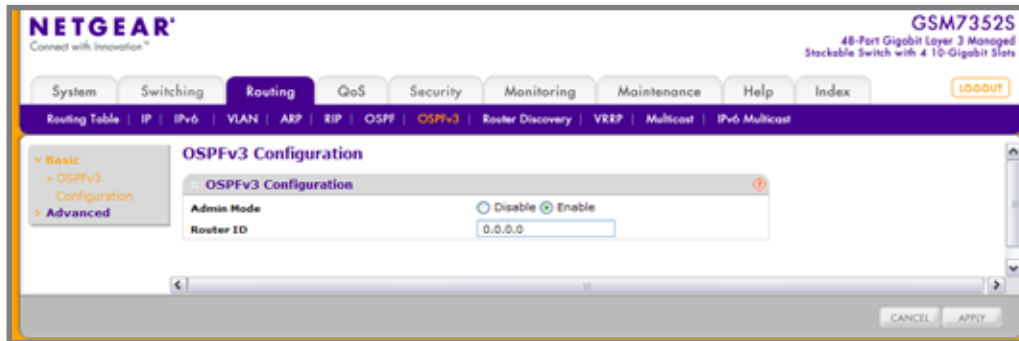
From the Basic link, you can access the following pages:

- [OSPFv3 Configuration](#) on page 297

## OSPFv3 Configuration

Use the OSPFv3 Configuration page to activate and configure OSPFv3 for a switch.

To display the OSPFv3 Configuration page, click **Routing** > **OSPFv3** > **Basic** > **OSPFv3 Configuration**.



1. Use **Admin Mode**\* to select enable or disable. If you select enable, OSPFv3 will be activated for the switch. The default value is disable. You must configure a Router ID before OSPFv3 can become operational. This can also be done by issuing the CLI command `router-id`, in the IPv6 router OSPF mode.
2. Use **Router ID** to specify the 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID you must first disable OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.

---

**Note:** \*Once OSPFv3 is initialized on the router, it will remain initialized until the router is reset.

---

## Advanced

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

- [\*OSPFv3 Configuration\*](#) on page 299
- [\*Common Area Configuration\*](#) on page 302
- [\*Stub Area Configuration\*](#) on page 304
- [\*NSSA Area Configuration\*](#) on page 306
- [\*Area Range Configuration\*](#) on page 308
- [\*Interface Configuration\*](#) on page 309
- [\*Interface Statistics\*](#) on page 313
- [\*Neighbor Table\*](#) on page 316
- [\*Link State Database\*](#) on page 318
- [\*Virtual Link Configuration\*](#) on page 321
- [\*Route Redistribution\*](#) on page 323

## OSPFv3 Configuration

Use the OSPFv3 Configuration page to activate and configure OSPFv3 for a switch.

To display the OSPFv3 Configuration page, click **Routing** > **OSPFv3** > **Advanced** > **OSPFv3 Configuration**.

### Default Route Advertise

1. Use **Default Information Originate** to enable or disable Default Route Advertise. Note that the values for 'Always', 'Metric' and 'Metric Type' can only be configured after Default Information Originate is set to enable. If Default Information Originate is set to enable and values for 'Always', 'Metric' and 'Metric Type' are already configured, then setting Default Information Originate back to disable will set the 'Always', 'Metric' and 'Metric Type' values to default.
2. Use **Always** to set the router advertise when set to "True".
3. Use **Metric** to specify the metric of the default route. The valid values are 0 to 16777214.
4. Use **Metric Type** to set the metric type of the default route. Valid values are External Type 1 and External Type 2.

## OSPFv3 Configuration

1. Use **Router ID** to specify the 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID you must first disable OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
2. Use **Admin Mode**\* to select enable or disable. If you select enable, OSPFv3 will be activated for the switch. The default value is enable. You must configure a Router ID before OSPFv3 can become operational. This can also be done by issuing the CLI command `router-id`, in the IPv6 router OSPF mode.

---

**Note:** \*Once OSPFv3 is initialized on the router, it will remain initialized until the router is reset.

---

3. Use **Exit Overflow Interval** to enter the number of seconds that, after entering overflow state, the router should wait before attempting to leave overflow state. This allows the router to again originate non-default AS-external-LSAs. If you enter 0, the router will not leave Overflow State until restarted. The range is 0 to 2147483647 seconds.
4. Use **External LSDB Limit** to specify the maximum number of AS-External-LSAs that can be stored in the database. A value of -1 implies there is no limit on the number that can be saved. The valid range of values is -1 to 2147483647.
5. Use **Default Metric** to set a default for the metric of redistributed routes. This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are 1 to 16777214.
6. Use **Maximum Paths** to configure the maximum number of paths that OSPFv3 can report to a given destination. The valid values are 1 to 4.
7. Use **AutoCost Reference Bandwidth** to configure the auto-cost reference-bandwidth to control how OSPF calculates default metrics for the interface. The valid values are 1 to 4294967.
8. Use **Default Passive Setting** to configure the global passive mode setting for all OSPF interfaces. Configuring this field overwrites any present interface level passive mode setting. OSPF does not form adjacencies on passive interfaces, but does advertise attached networks as stub networks.



**Table 37.**

Field	Description
ASBR Mode	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol.
ABR Status	The values of this are enabled or disabled. Enabled implies that the router is an area border router. Disabled implies that it is not an area border router.
External LSA Count	The number of external (LS type 5) LSAs (link state advertisements) in the link state database.
External LSA Checksum	The sum of the LS checksums of the external LSAs (link state advertisements) contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers.
New LSAs Originated	In any given OSPFv3 area, a router will originate several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it will originate network-LSAs for those networks. This value represents the number of LSAs originated by this router.
LSAs Received	The number of LSAs (link state advertisements) received that were determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.

## Common Area Configuration

Use the Common Area Configuration page to create and configure an OSPFv3 area.

To display the Common Area Configuration page, click **Routing** > **OSPFv3** > **Advanced** > **Common Area Configuration**.

**NETGEAR**  
Connected with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | **OSPFv3** | Router Discovery | VRRP | Multicast | IPv6 Multicast

**Common Area Configuration**

OSPFv3 Common Area Configuration

Area ID	External Routing	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSA's
<input type="checkbox"/> 0.0.0.0	<input type="checkbox"/> Import External LSAs					<input checked="" type="checkbox"/> Originate and propagate summary LSAs

ADD DELETE CANCEL

Copyright © 1996-2010 Netgear, Inc.

1. Use **Area ID** to enter the OSPF area ID. An Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Click **ADD** to configure the area as a common area.
3. Click **DELETE** to delete the common area.

**Table 38.**

Field	Description
External Routing	A definition of the router's capabilities for the area, including whether or not AS-external-LSAs are flooded into/throughout the area.
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Import Summary LSAs	The summary LSAs will be enabled/disabled imported into this area.

## Stub Area Configuration

To display the Stub Area Configuration page, click **Routing** > **OSPFv3** > **Advanced** > **Stub Area Configuration**.

**NETGEAR**  
Connected with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | **OSPFv3** | Router Discovery | VRRP | Multicast | IPv6 Multicast

Basic  
Advanced  
OSPFv3 Configuration  
Common Area Configuration  
Stub Area Configuration  
NSSA Area Configuration  
Area Range Configuration  
Interface Configuration  
Interface Statistics  
Neighbor Table  
Link State Database  
Virtual Link Configuration  
Route Redistribution

### Stub Area Configuration

#### OSPFv3 Stub Area Configuration

Area ID	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSA's	Default Cost	Type of Service
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

ADD DELETE CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

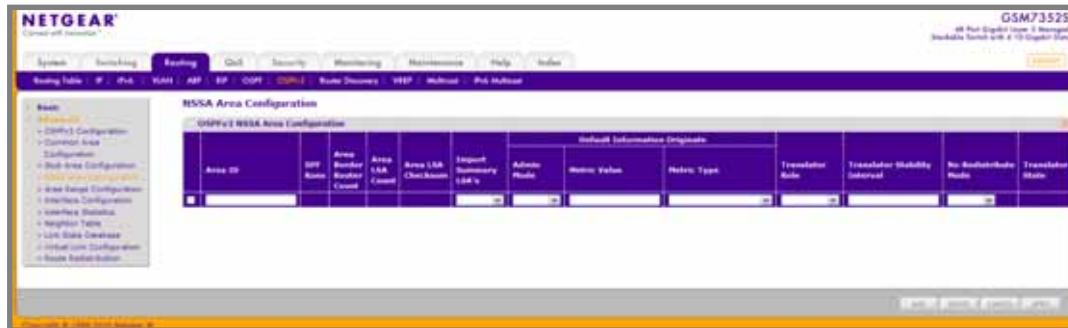
1. Use **Area ID** to enter the OSPF area ID. An Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Use **Import Summary LSAs** to select enable or disable. If you select enable, summary LSAs will be imported into areas. Defaults to Enable.
3. Use **Default Cost** to enter the metric value you want applied for the default route advertised into the stub area. Valid values range from 1 to 16,777,215. This value is applicable only to Stub areas.
4. Click **ADD** to configure the area as a stub area.
5. Click **DELETE** to delete the stub area designation. The area will be returned to normal state.

**Table 39.**

Field	Description
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Type of Service	This field is the normal TOS associated with the stub metric.

## NSSA Area Configuration

To display the NSSA Area Configuration page, click **Routing** > **OSPFv3** > **Advanced** > **NSSA Area Configuration**.



1. Use **Area ID** to enter the OSPF area ID. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Use **Import Summary LSAs** to select enable or disable. If you select enable summary LSAs will be imported into areas. Defaults to Enable.
3. Use **Default Information Originate** to advertise a default route into the NSSA when Import Summary LSAs is disabled. This can also be applied by the CLI command `area <areaid> nssa default-info-originate` in the IPv6 router OSPF config mode.
4. Use **Admin Mode** to enable or disable the default information originate. Valid values are True or False.
5. Use **Metric Value** to set the Default Metric value for default information originate. The valid range of values is 1 to 16777214.
6. Use **Metric Type** to select the type of metric specified in the Metric Value field.
  - **Comparable Cost** - External Type 1 metrics that are comparable to the OSPFv3 metric
  - **Non-comparable Cost** - External Type 2 metrics that are assumed to be larger than the cost of the OSPFv3 metric
7. Use **Translator Role** to specify the NSSA Border router's ability to perform NSSA translation of type-7 LSAs into type-5 LSAs. The valid values are 'Always' and 'Candidate'.
8. Use **Translator Stability Interval** to specify the number of seconds after an elected translator determines its services are no longer required, that it should continue to perform its translation duties. The valid range of values is 0 to 3600.
9. Use **No-Redistribute Mode** to enable or disable the No-Redistribute Mode.
10. Click **ADD** to configure the area as a NSSA area.
11. Click **DELETE** to delete the NSSA area designation. The area will be returned to normal state.

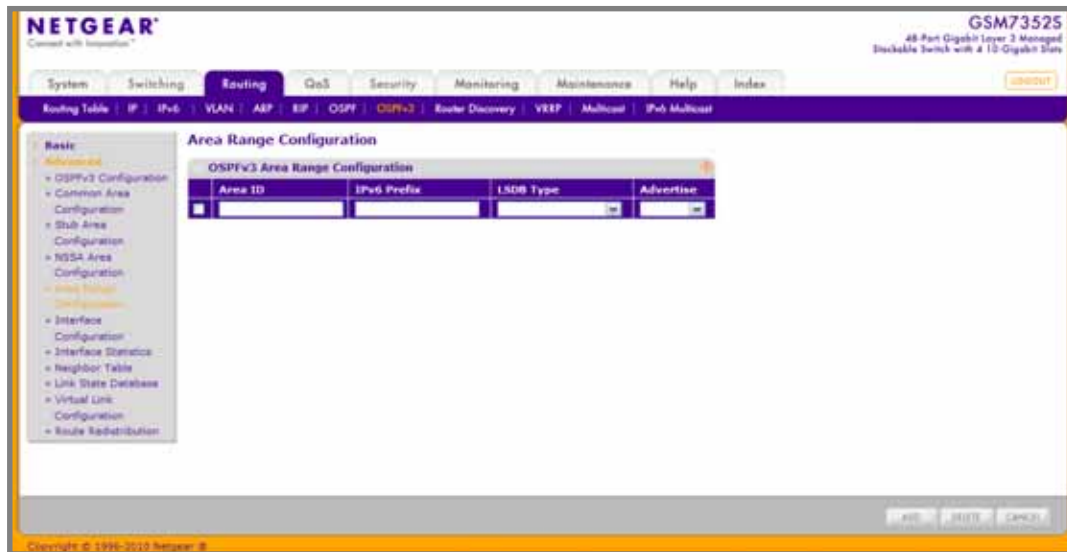
**Table 40.**

Field	Description
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Translator State	Translator State 'Enabled' means that the NSSA router OSPFv3 Area Nssa Translator Role has been set to always. Translator State of 'Elected' means a candidate NSSA Border router is translating type-7 LSAs into type-5.' Disabled' implies that a candidate NSSA Border router is NOT translating type-7 LSAs into type-5.

## Area Range Configuration

Use the Area Range Configuration page to configure OSPFv3 area ranges.

To display the Area Range Configuration page, click **Routing** > **OSPFv3** > **Advanced** > **Area Range Configuration**.



1. Use **Area ID** to specify the area for which data is to be configured.
2. Use **IPv6 Prefix** to enter the IPv6 Prefix/Prefix Length for the address range for the selected area.
3. Use **LSDB Type** to select the type of Link Advertisement associated with the specified area and address range. The default type is 'Network Summary'.
4. Use **Advertise** to select Enable or Disable. If you select Enable, the address range will be advertised outside the area via a Network Summary LSA. The default is Enable.
5. Click **ADD** to add the new address range to the switch.
6. Click **DELETE** to remove the specified address range from the area configuration.



## Interface Configuration

Use the OSPFv3 Interface Configuration page to create and configure OSPFv3 interfaces.

To display the Interface Configuration page, click **Routing** > **OSPFv3** > **Advanced** > **Interface Configuration**.

OSPFv3 Interface Configuration											
OSPFv3 Interface Configuration											
All											
Interface	IPv6 Address	Area ID	Admin Mode	Router Priority	Transmit Interval	Hello Interval	Dead Interval	LSA Ack Interval	Transmit Delay Interval	MTU Square	Passive Mode
<input type="checkbox"/> 1/0/1	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/2	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/3	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/4	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/5	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/6	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/7	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/8	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/9	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/10	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/11	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/12	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/13	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/14	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/15	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/16	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/17	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/18	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/19	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/20	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/21	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable
<input type="checkbox"/> 1/0/22	0.0.0.0	0.0.0.0	Disable	1	0	10	40	1	1	Disable	Disable

[illegible]

1. **Interface** - The interface for which data is to be displayed or configured.
2. Use **Area ID** to enter the 32-bit integer in dotted decimal format that uniquely identifies the OSPFv3 area to which the selected router interface connects. If you assign an Area ID which does not exist, the area will be created with default values.
3. Use **Admin Mode\*** to select enable or disable. The default value is 'disable.' You can configure OSPFv3 parameters without enabling OSPFv3 Admin Mode, but they will have no effect until you enable Admin Mode. The following information will be displayed only if the Admin Mode is enabled: State, Designated Router, Backup Designated Router, Number of

Link Events, LSA ACK Interval, and Metric Cost. For OSPFv3 to be fully functional, the interface must have a valid IPv6 Prefix/Prefix Length. This can be done through the CLI using the IPv6 address command in the interface configuration mode.

---

**Note:** \*Once OSPFv3 is initialized on the router, it will remain initialized until the router is reset.

---

4. Use **Router Priority** to enter the OSPFv3 priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. The default is 1, which is the highest router priority. A value of '0' indicates that the router is not eligible to become the designated router on this network.
5. Use **Retransmit Interval** to enter the OSPFv3 retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 0 to 3600 seconds (1 hour). The default is 5 seconds.
6. Use **Hello Interval** to enter the OSPFv3 hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.
7. Use **Dead Interval** to enter the OSPFv3 dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should be a multiple of the Hello Interval (e.g. 4). Valid values range from 1 to 65535. The default is 40.
8. Use **Iftransit Delay Interval** to enter the OSPFv3 Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
9. Use **MTU Ignore** to disable OSPFv3 MTU mismatch detection on receiving packets. Default value is Disable.
10. Use **Passive Mode** to make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default.
11. Use **Interface Type** to set the interface type to broadcast mode or point to point mode. The default interface type is broadcast.
12. Use **Metric Cost** to enter the value on this interface for the cost TOS (type of service). The range for the metric cost is between 1 and 65,535. Metric Cost is only configurable if OSPFv3 is initialized on the interface.

Table 41.

Field	Description
IPv6 Address	The IPv6 address of the interface.
LSA Ack Interval	The number of seconds between LSA Acknowledgment packet transmissions, which must be less than the Retransmit Interval.
State	<p>The current state of the selected router interface. One of:</p> <ul style="list-style-type: none"> <li>• Down: This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface.</li> <li>• Loopback: In this state, the router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. However, it may still be desirable to gain information on the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets may still be addressed to an interface in Loopback state. To facilitate this, such interfaces are advertised in router- LSAs as single host routes, whose destination is the IP interface address.</li> <li>• Waiting: The router is trying to determine the identity of the (Backup) Designated Router for the network by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.</li> <li>• Designated Router: This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network.</li> <li>• Backup Designated Router: This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.</li> <li>• Other Designated Router: The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.</li> </ul> <p>The State is only displayed if the OSPFv3 admin mode is enabled.</p>
Designated Router	The identity of the Designated Router for this network, in the view of the advertising router. The Designated Router is identified here by its router ID. The value 0.0.0.0 means that there is no Designated Router. This field is only displayed if the OSPFv3 admin mode is enabled.

**Table 41.**

Field	Description
Backup Designated Router	The identity of the Backup Designated Router for this network, in the view of the advertising router. The Backup Designated Router is identified here by its router ID. Set to 0.0.0.0 if there is no Backup Designated Router. This field is only displayed if the OSPFv3 admin mode is enabled.
Number of Link Events	This is the number of times the specified OSPFv3 interface has changed its state. This field is only displayed if the OSPFv3 admin mode is enabled.

## Interface Statistics

This screen displays statistics for the selected interface. The information will be displayed only if OSPFv3 is enabled.

To display the Interface Statistics page, click **Routing > OSPFv3 > Advanced > Interface Statistics**.

**OSPFv3 Interface Statistics**

**OSPFv3 Interface Selection**

Interface: 1/0/1

**OSPFv3 Interface Statistics**

- OSPFv3 Area ID
- Area Border Router Count
- AS Border Router Count
- Area LSA Count
- IPv6 Address
- Interface Events
- Virtual Events
- Neighbor Events
- External LSA Count
- Sent Packets
- Received Packets
- Discards
- Bad Version
- Virtual Link Not Found
- Area Mismatch
- Invalid Destination Address
- No Neighbor at Source Address
- Invalid OSPF Packet Type
- Hellos Ignored
- Hellos Sent
- Hellos Received
- DD Packets Sent
- DD Packets Received
- LS Requests Sent
- LS Requests Received
- LS Updates Sent
- LS Updates Received
- LS Acknowledgements Sent
- LS Acknowledgements Received

1. Use **Interface** to select the interface for which data is to be displayed.

**Table 42.**

Field	Description
OSPFv3 Area ID	The OSPFv3 area to which the selected router interface belongs. An OSPFv3 Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which the interface connects.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
AS Border Router Count	The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IPv6 Address	The IPv6 address of the interface.
Interface Events	The number of times the specified OSPFv3 interface has changed its state or an error has occurred.
Virtual Events	The number of state changes or errors that have occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state or an error has occurred.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
Sent packets	The number of OSPFv3 packets transmitted on the interface.
Received packets	The number of valid OSPFv3 packets received on the interface.
Discards	The number of received OSPFv3 packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPFv3 packets whose version field in the OSPFv3 header does not match the version of the OSPFv3 process handling the packet.
Virtual Link Not Found	The number of received OSPFv3 packets discarded where the ingress interface is in a non-backbone area and the OSPFv3 header identifies the packet as belonging to the backbone, but OSPFv3 does not have a virtual link to the packet's sender.

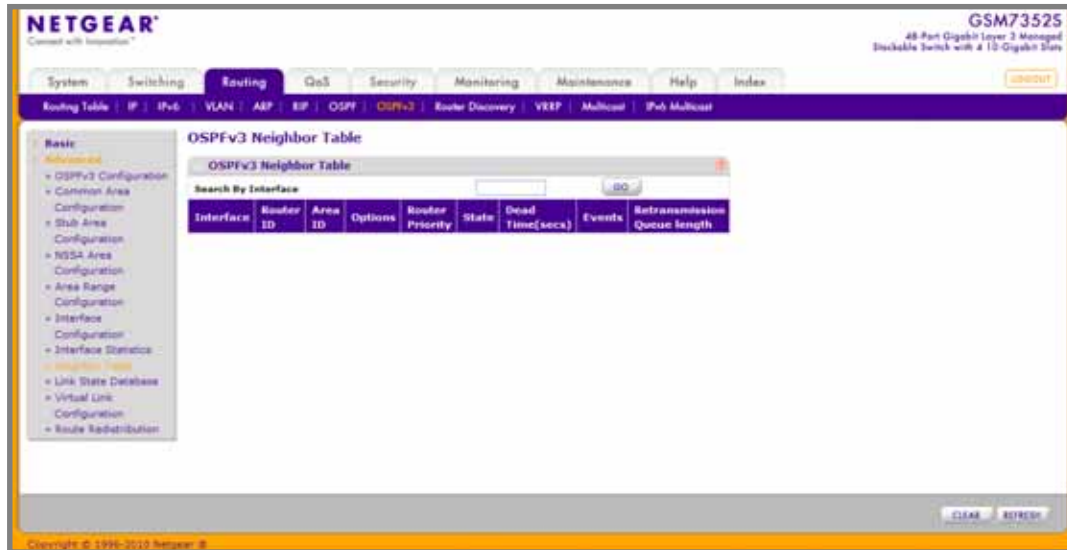
**Table 42.**

Field	Description
Area Mismatch	The number of OSPFv3 packets discarded because the area ID in the OSPFv3 header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPFv3 packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
No Neighbor at Source Address	The number of OSPFv3 packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
Invalid OSPF Packet Type	The number of OSPFv3 packets discarded because the packet type field in the OSPFv3 header is not a known type.
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.
Hellos Sent	The number of Hello packets sent on this interface by this router.
Hellos Received	The number of Hello packets received on this interface by this router.
DD Packets Sent	The number of Database Description packets sent on this interface by this router.
DD Packets Received	The number of Database Description packets received on this interface by this router.
LS Requests Sent	The number of LS Requests sent on this interface by this router.
LS Requests Received	The number of LS Requests received on this interface by this router.
LS Updates Sent	The number of LS updates sent on this interface by this router.
LS Updates Received	The number of LS updates received on this interface by this router.
LS Acknowledgements Sent	The number of LS acknowledgements sent on this interface by this router.
LS Acknowledgements Received	The number of LS acknowledgements received on this interface by this router.

## Neighbor Table

This screen shows the OSPFv3 Neighbor Table. This information is displayed only if OSPFv3 is enabled and there exists at least on OSPFv3 enabled interface having a valid neighbor.

To display the Neighbor Table page, click **Routing** > **OSPFv3** > **Advanced** > **Neighbor Table**.





**Table 43.**

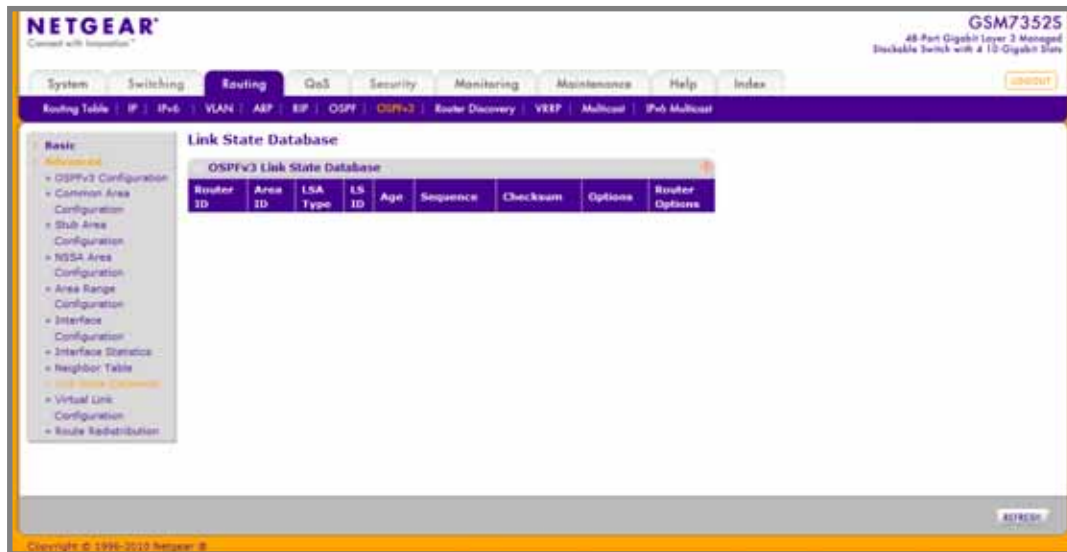
Field	Description
Interface	The Interface for which the data needs to be displayed.
Router ID	A 32-bit integer in dotted decimal format representing the Router ID of the neighbor on the selected Interface.
Area ID	A 32-bit integer in dotted decimal format representing the area common to the neighbor selected.
Options	A Bit Mask corresponding to the neighbor's options field.
Router Priority	The priority of this neighbor in the designated router election algorithm. A value of 0 signifies that the neighbor is not eligible to become the designated router on this particular network.
State	State of the relationship with this neighbor.
Dead Time	Number of seconds since last Hello was received from Adjacent Neighbors. Set to 0 for neighbors in a state less than or equal to Init.
Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	Length of the selected neighbor's retransmit queue.

1. Click **REFRESH** to refresh the page with the latest OSPFv3 neighbor information for the selected interface.
2. Click **CLEAR** to clear all the neighbor in the table.

## Link State Database

Use the OSPFv3 Link State Database page to display the link state database.

To display the Link State Database page, click **Routing** > **OSPFv3** > **Advanced** > **Link State Database**.



**Table 44.**

Field	Description
Router ID	The 32 bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the OSPFv3 Configuration page. If you want to change the Router ID you must first disable OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
Area ID	The ID of an OSPFv3 area to which one of the router interfaces is connected. An Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which an interface is connected.

Table 44.

Field	Description
LSA Type	<p>The format and function of the link state advertisement. One of the following:</p> <ul style="list-style-type: none"> <li>• Router LSA: A router may originate one or more router-lsas for a given area. Each router-lsa originated in an area describes the collected states of all the router's interfaces to the area.</li> <li>• Network LSA: A network lsa is originated for every link having two or more attached routers, by the designated router. It lists all the routers attached to the link.</li> <li>• Inter-Area Router LSA: This type describes a prefix external to the area, yet internal to the autonomous system. It is originated by an Area Border Router.</li> <li>• AS-External LSA: This LSA type describes a path to a prefix external to the autonomous system and is originated by an Autonomous System Border Router.</li> <li>• Link LSA: A router originates a separate Link-lsa for each attached link. It provides router's link local address to routers attached to the link and also inform them of a list of IPv6 prefixes to associate with the link.</li> <li>• Intra-Area-Prefix LSA: A link's designated router originates one or more intra-area-prefix lsas to advertise the link's prefixes throughout the area. A router may originate multiple intra-area-prefix lsas for a given area to advertise its own prefixes and those of its attached stub links.</li> </ul>
LS ID	The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

Table 44.

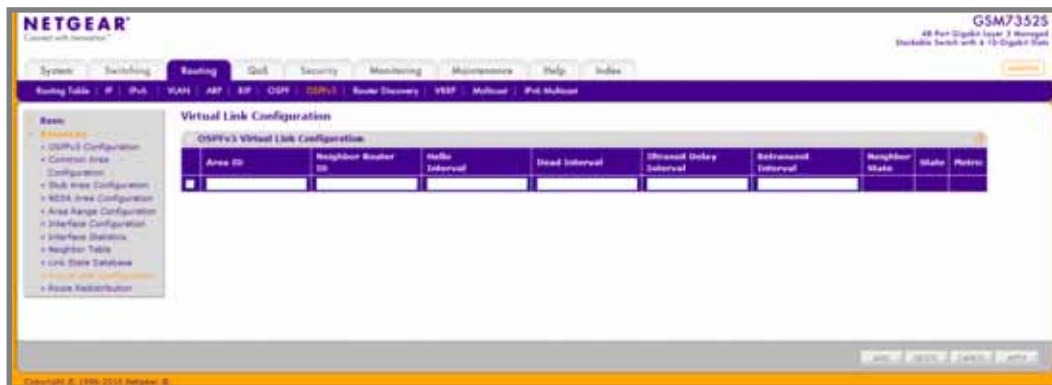
Field	Description
Options	<p>The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. The options are:</p> <ul style="list-style-type: none"><li>• Q: This enables support for QoS Traffic Engineering.</li><li>• E: This describes the way AS-external-LSAs are flooded.</li><li>• MC: This describes the way IP multicast datagrams are forwarded according to the standard specifications.</li><li>• O: This describes whether Opaque-LSAs are supported.</li><li>• V: This describes whether OSPF++ extensions for VPN/COS are supported.</li></ul>
Router Options	The router specific options.

Click **REFRESH** to show the latest OSPFv3 Link State information.

## Virtual Link Configuration

Use the Virtual Link Configuration page to define a new or configure an existing virtual link. To display this page, a valid OSPFv3 area must be defined via the OSPFv3 Area Configuration page.

To display the Virtual Link Configuration page, click **Routing > OSPFv3 > Advanced > Virtual Link Configuration**.



1. Use **Area ID** to specify the Area ID portion of the virtual link identification for which data is to be displayed. The Area ID and Neighbor Router ID together define the virtual link.
2. Use **Neighbor Router ID** to specify the neighbor portion of the virtual link identification. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.
3. Use **Hello Interval** to specify the OSPFv3 hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.
4. Use **Dead Interval** to specify the OSPFv3 dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should be a multiple of the Hello Interval (e.g. 4). Valid values range from 1 to 65535. The default is 40.
5. Use **Iftransit Delay Interval** to specify the OSPFv3 Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
6. Use **Retransmit Interval** to specify the OSPFv3 retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.
7. Click **ADD** to add a new virtual link to the switch.
8. Click **DELETE** to remove the specified virtual link from the switch configuration.

Table 45.

Field	Description
Neighbor State	The state of the Virtual Neighbor Relationship.
State	<p>The state of the interface:</p> <ul style="list-style-type: none"> <li>• Down: This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface.</li> <li>• Waiting: The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router.</li> <li>• Point-to-Point: The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every HelloInterval seconds.</li> <li>• Designated Router: This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network.</li> <li>• Backup Designated Router: This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router.</li> <li>• Other Designated Router: The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.</li> </ul>
Metric	The metric value used by the Virtual Link.

## Route Redistribution

This screen can be used to configure the OSPFv3 Route Redistribution parameters. The allowable range for each field is displayed next to it. If an invalid value is entered in one or multiple fields, an alert message will be displayed with the list of all the valid values.

To display the Route Redistribution page, click **Routing > OSPFv3 > Advanced > Route Redistribution**.

The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches software interface. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Routing tab is selected, and the sub-menu includes Routing Table, IP, IPv6, VLAN, ARP, RIP, OSPF, OSPFv3, Router Discovery, VRRP, Multicast, and IPv6 Multicast. The OSPFv3 tab is selected, and the sub-menu includes Basic, Advanced, OSPFv3 Configuration, Common Area Configuration, Stub Area Configuration, NSSA Area Configuration, Area Range Configuration, Interface Configuration, Interface Statistics, Neighbor Table, Link State Database, and Virtual Link Configuration. The Advanced tab is selected, and the sub-menu includes OSPFv3 Route Redistribution. The OSPFv3 Route Redistribution page shows a table with columns for Source, Redistribute Option, Metric, Metric Type, and Tag. The table has two rows: Connected and Static. The Redistribute Option column has a dropdown menu with 'Disable' selected. The Metric column has a text input field with a range of 0 to 16777214. The Metric Type column has a dropdown menu with 'External Type 2' selected. The Tag column has a text input field with a range of 0 to 4294967295. The bottom of the page has buttons for Refresh, Cancel, and Apply.

Source	Redistribute Option	Metric	Metric Type	Tag
<input type="checkbox"/> Connected	Disable		External Type 2	0
<input type="checkbox"/> Static	Disable		External Type 2	0

- Use **Source** to select those Source Protocols that have already been configured for redistribution by OSPFv3. The valid values are 'Static' and 'Connected'.
- Use **Redistribute Option** to enable or disable the redistribution for the selected source protocol.
- Use **Metric** to set the metric value to be used as the metric of redistributed routes. This field displays the metric if the source was pre-configured and can be modified. The valid values are 0 to 16777214.
- Use **Metric Type** to set the OSPFv3 metric type of redistributed routes.
- Use **Tag** to set the tag field in routes redistributed. This field displays the tag if the source was pre-configured, else a default tag value of 0 is displayed. The valid values are 0 to 4294967295.

## 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.

From the Router Discovery tab, you can access the following pages:

- [Router Discovery Configuration](#) on page 324

## Router Discovery Configuration

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

To display the Router Discovery Configuration page, click **Routing** > **Router Discovery** > **Router Discovery Configuration**.

The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual. The page is titled "Router Discovery Configuration" and is part of the "Router Discovery" section. The page displays a table of interface configurations for Router Discovery. The table has the following columns: Interface, Advertise Mode, Advertise Address, Maximum Advertise Interval, Minimum Advertise Interval, Advertise Lifetime, and Preference Level. The table lists 18 interfaces, all with "Disable" as the Advertise Mode, "224.0.0.1" as the Advertise Address, "600" as the Maximum Advertise Interval, "450" as the Minimum Advertise Interval, "1800" as the Advertise Lifetime, and "0" as the Preference Level. The interfaces are listed as 1/0/1 through 1/0/18. The page also includes a "Go To Interface" dropdown menu and a "GO" button. The Netgear logo is visible in the top left corner, and the model number "GSM7352S" is in the top right corner. The page footer indicates "Copyright © 1996-2010 Netgear, Inc."

Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval	Minimum Advertise Interval	Advertise Lifetime	Preference Level
<input type="checkbox"/> 1/0/1	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/2	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/3	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/4	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/5	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/6	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/7	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/8	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/9	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/10	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/11	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/12	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/13	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/14	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/15	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/16	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/17	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/18	Disable	224.0.0.1	600	450	1800	0



1. Use **Interface** to select the router interface for which data is to be configured.
2. Use **Advertise Mode** to select enable or disable. If you select enable, Router Advertisements will be transmitted from the selected interface.
3. Use **Advertise Address** to enter the IP Address to be used to advertise the router.
4. Use **Maximum Advertise Interval** to enter the maximum time (in seconds) allowed between router advertisements sent from the interface.
5. Use **Minimum Advertise Interval** to enter the minimum time (in seconds) allowed between router advertisements sent from the interface.
6. Use **Advertise Lifetime** to 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.
7. Use **Preference Level** to 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.

## VRRP

The Virtual Router Redundancy protocol is designed to handle default router failures by providing a scheme to dynamically elect a backup router. The driving force was to minimize “black hole” periods due to the failure of the default gateway router during which all traffic directed towards it is lost until the failure is detected. Though static configuration of default routes is popular, such an approach is susceptible to a single point of failure when the default router fails. VRRP advocates the concept of a “virtual router” associated with one or more IP Addresses that serve as default gateways. In the event that the VRRP Router controlling these IP Addresses (formally known as the Master) fails, the group of IP Addresses and the default forwarding role is taken over by a Backup VRRP Router.

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

- [Basic](#) on page 325
- [Advanced](#) on page 329

### Basic

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

- [VRRP Configuration](#) on page 325

### VRRP Configuration

Use the VRRP Configuration page to enable or disable the administrative status of a virtual router.

To display the VRRP Configuration page, click **Routing > VRRP > Basic > VRRP Configuration**.

The screenshot displays the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual. The page is titled "VRRP Configuration" and is part of the "Routing" section. The interface includes a top navigation bar with tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. A "Logout" button is located in the top right corner. The main content area is divided into two sections: "Global Configuration" and "Table Configuration".

**Global Configuration**

Admin Mode: ☒ Disable ☐ Enable

**Table Configuration**

VRID	Interface	Interface IP Address	Primary IP Address	Mode	State
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

At the bottom of the page, there are buttons for "ADD", "DELETE", "CANCEL", and "APPLY". The footer indicates "Copyright © 1996-2010 Netgear, Inc."

1. VRID is only configurable if you are creating new Virtual Router, in which case enter the VRID in the range 1 to 255.
2. Use **Interface** to select the Unit/Slot/Port for the new Virtual Router from the pull-down menu.
3. Use **Pre-empt Mode** to select enable or disable. If you select enable, a backup router will preempt the master router if it has a priority greater than the master virtual router's priority provided the master is not the owner of the virtual router IP address. The default is enable.
4. Use **Priority** to enter the priority value to be used by the VRRP router in the election for the master virtual router. If the Virtual IP Address is the same as the interface IP Address, the priority gets set to 255 no matter what the user enters. If the user enters a priority of 255 when the Virtual and interface IP Addresses are not the same, the priority gets set to the default value of 100.
5. Use **Advertisement Interval** to enter the time, in seconds, between the transmission of advertisement packets by this virtual router. Enter a number between 1 and 255. The default value is 1 second.
6. Use **Primary IP Address** to enter the IP Address associated with the Virtual Router. The default is 0.0.0.0.
7. Use **Authentication Type** to select the type of Authentication for the Virtual Router from the pull-down menu. The default is None. The choices are:
  - **0-None** - No authentication will be performed.
  - **1-Simple** - Authentication will be performed using a text password.
8. **Authentication Data:** If you selected simple authentication, enter the password.
9. Use **Status** to select active or inactive to start or stop the operation of the Virtual Router. The default is inactive.
10. Click **ADD** to add a new Virtual Router to the switch configuration.
11. Click **DELETE** to delete the selected Virtual Router. Note that the router can not be deleted if there are secondary addresses configured.

**Table 46.**

Field	Description
Interface IP Address	Indicates the IP Address associated with the selected interface.
Owner	Set to 'True' if the Virtual IP Address and the Interface IP Address are the same, otherwise set to 'False'. If this parameter is set to 'True', the Virtual Router is the owner of the Virtual IP Address, and will always win an election for master router when it is active.
VMAC Address	The virtual MAC Address associated with the Virtual Router, composed of a 24 bit organizationally unique identifier, the 16 bit constant identifying the VRRP address block and the 8 bit VRID.
State	The current state of the Virtual Router: <ul style="list-style-type: none"><li>• State</li><li>• Initialize</li><li>• Master</li><li>• Backup</li></ul>

## Advanced

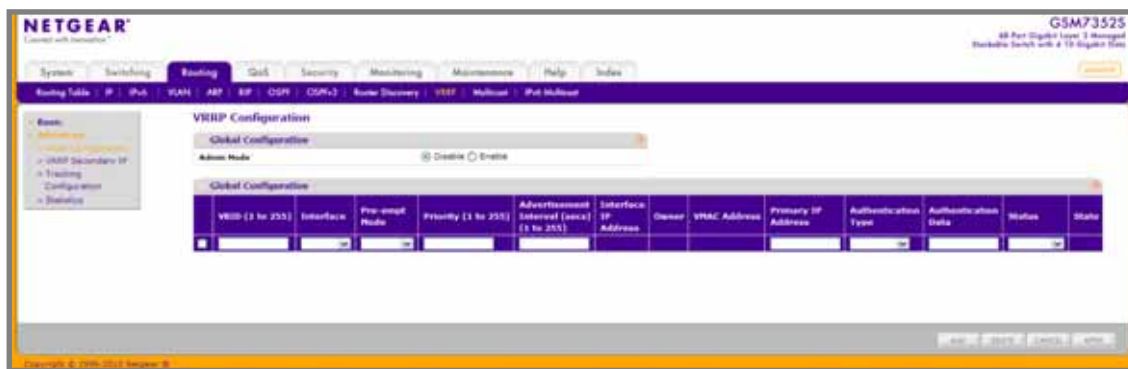
From the Advanced link, you can access the following pages:

- [VRRP Configuration](#) on page 329
- [VRRP Secondary IP](#) on page 331
- [Tracking Configuration](#) on page 332
- [Virtual Router Statistics](#) on page 333

### VRRP Configuration

Use the VRRP Configuration page to enable or disable the administrative status of a virtual router.

To display the VRRP Configuration page, click **Routing > VRRP > Advanced > VRRP Configuration**.



### Global Configuration

1. Use **Admin Mode** to set the administrative status of VRRP in the router to active or inactive. Select enable or disable from the radio button. The default is disable.
2. VRID is only configurable if you are creating new Virtual Router, in which case enter the VRID in the range 1 to 255.
3. Use **Interface** to select the Unit/Slot/Port for the new Virtual Router from the pull-down menu.
4. Use **Pre-empt Mode** to select enable or disable. If you select enable, a backup router will preempt the master router if it has a priority greater than the master virtual router's priority provided the master is not the owner of the virtual router IP address. The default is enable.
5. Use **Priority** to enter the priority value to be used by the VRRP router in the election for the master virtual router. If the Virtual IP Address is the same as the interface IP Address, the priority gets set to 255 no matter what the user enters. If the user enters a priority of 255 when the Virtual and interface IP Addresses are not the same, the priority gets set to the default value of 100.
6. Use **Advertisement Interval** to enter the time, in seconds, between the transmission of advertisement packets by this virtual router. Enter a number between 1 and 255. The default value is 1 second.

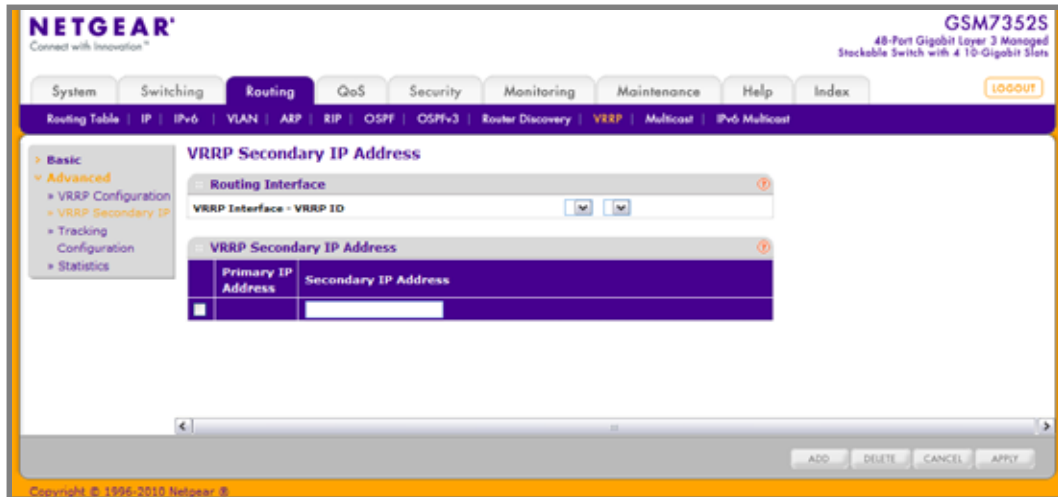
7. Use **Primary IP Address** to enter the IP Address associated with the Virtual Router. The default is 0.0.0.0.
8. Use **Authentication Type** to select the type of Authentication for the Virtual Router from the pull-down menu. The default is None. The choices are:
  - **0-None** - No authentication will be performed.
  - **1-Simple** - Authentication will be performed using a text password.
9. **Authentication Data** - If you selected simple authentication, enter the password.
10. Use **Status** to select active or inactive to start or stop the operation of the Virtual Router. The default is inactive.
11. Click **ADD** to add a new Virtual Router to the switch configuration.
12. Click **DELETE** to delete the selected Virtual Router. Note that the router can not be deleted if there are secondary addresses configured.

Table 47.

Field	Description
Interface IP Address	Indicates the IP Address associated with the selected interface.
Owner	Set to 'True' if the Virtual IP Address and the Interface IP Address are the same, otherwise set to 'False'. If this parameter is set to 'True', the Virtual Router is the owner of the Virtual IP Address, and will always win an election for master router when it is active.
VMAC Address	The virtual MAC Address associated with the Virtual Router, composed of a 24 bit organizationally unique identifier, the 16 bit constant identifying the VRRP address block and the 8 bit VRID.
State	The current state of the Virtual Router: <ul style="list-style-type: none"> <li>• Initialize</li> <li>• Master</li> <li>• Backup</li> </ul>

## VRRP Secondary IP

To display the VRRP Secondary IP page, click **Routing** > **VRRP** > **Advanced** > **VRRP Secondary IP**.



1. Use **VRRP ID and Interface** to select one of the existing Virtual Routers, listed by interface number and VRRP ID.
2. Use **Secondary IP Address** to enter the IP address for the interface. This address must be a member of one of the subnets currently configured on the interface. This value is read only once configured.
3. Click **ADD** to add a new secondary IP address to the selected VRRP interface.
4. Click **DELETE** to delete the selected secondary IP address.

**Table 48.**

Field	Description
Virtual Router ID	The Virtual Router ID for which data is to be displayed or configured.
Primary IP Address	The Primary IP Address of the Virtual Router.

## Tracking Configuration

Use Tracking Configuration to track specific route IP states within the router that can alter the priority level of a virtual router for a VRRP group.

To display the Tracking Configuration page, click **Routing > VRRP > Advanced > Tracking Configuration**.

1. Use **VRRP ID and Interface** to select one of the existing Virtual Routers, listed by interface number and VRRP ID.
2. Use **Tracked Interface** to select a routing interface which is not yet tracked for this VRRP ID and interface configuration. Exception: loopback and tunnels could not be tracked.
3. Use **Tracked Interface Priority Decrement** to specify the priority decrement for the tracked interface. The valid range is 1 - 254. default value is 10.
4. Use **Tracked Route Prefix** to specify the Prefix of the route.
5. Use **Tracked Route Prefix Length** to specify the prefix length of the route.
6. Use **Tracked Route Priority Decrement** to specify the priority decrement for the Route. The valid range is 1 - 254. Default value is 10.
7. Click **ADD** to add a new tracked interface or tracked route to the VRRP.
8. Click **DELETE** to delete a selected tracked interface or tracked route.

**Table 49.**

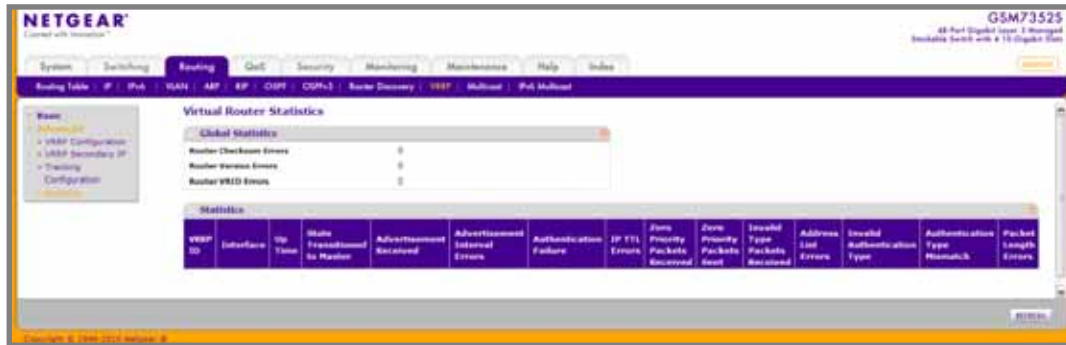
Field	Description
Tracked Interface state	The state of the tracked interface.
Reachable	The reachability of the tracked Route.



## Virtual Router Statistics

Use the Virtual Router Statistics page to display statistics for a specified virtual router.

To display the Virtual Router Statistics page, click **Routing > VRRP > Advanced > Statistics**.



**Table 50.**

Field	Description
Router Checksum Errors	The total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	The total number of VRRP packets received with an unknown or unsupported version number.
Router VRID Errors	The total number of VRRP packets received with an invalid VRID for this virtual router.
VRRP ID	The VRID for the selected Virtual Router.
Interface	The Unit/Slot/Port for the selected Virtual Router.
Up Time	The time, in days, hours, minutes and seconds, that has elapsed since the virtual router transitioned to the initialized state.
State Transitioned to Master	The total number of times that this virtual router's state has transitioned to Master.
Advertisement Received	The total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	The total number of VRRP advertisement packets received for which the advertisement interval was different than the one configured for the local virtual router.
Authentication Failure	The total number of VRRP packets received that did not pass the authentication check.
IP TTL Errors	The total number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.

Table 50.

Field	Description
Zero Priority Packets Received	The total number of VRRP packets received by the virtual router with a priority of '0'.
Zero Priority Packets Sent	The total number of VRRP packets sent by the virtual router with a priority of '0'.
Invalid Type Packets Received	The number of VRRP packets received by the virtual router with an invalid value in the 'type' field.
Address List Errors	The total number of packets received for which the address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	The total number of packets received with an unknown authentication type.
Authentication Type Mismatch	The total number of packets received with an authentication type different to the locally configured authentication method.
Packet Length Errors	The total number of packets received with a packet length less than the length of the VRRP header.

Click **REFRESH** to show the latest VRRP information.

## Multicast

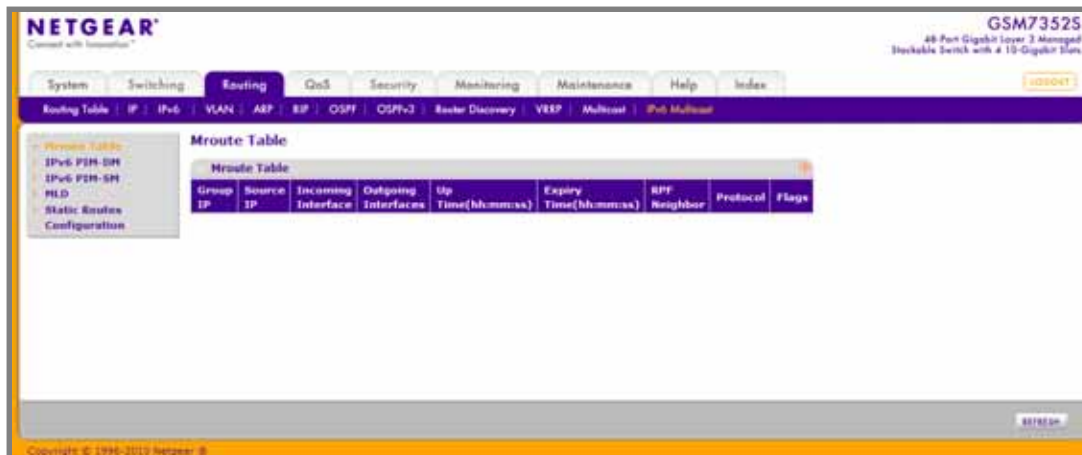
From the Multicast link, you can access the following pages:

- [Mroute Table](#) on page 335
- [Multicast Global Configuration](#) on page 336
- [Multicast Interface Configuration](#) on page 337
- [DVMRP](#) on page 338
- [IGMP](#) on page 346
- [PIM-DM](#) on page 359
- [PIM-SM](#) on page 362
- [Static Routes Configuration](#) on page 370
- [Admin Boundary Configuration](#) on page 371

## Mroute Table

This screen displays contents of the Mroute Table in tabular form.

To display the Mroute Table page, click **Routing** > **Multicast** > **Mroute Table**.



**Table 51.**

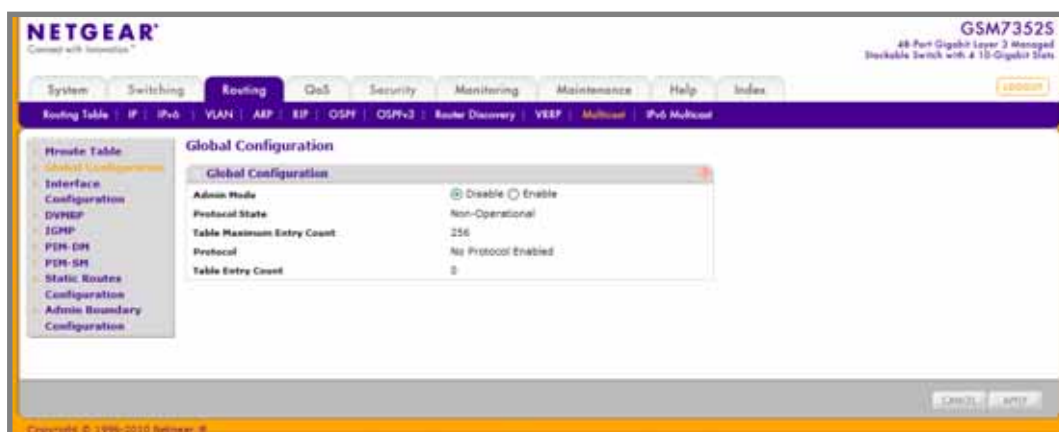
Field	Description
Source IP	The IP address of the multicast packet source to be combined with the Group IP to fully identify a single route whose Mroute table entry.
Group IP	The destination group IP address.
Incoming Interface	The incoming interface on which multicast packets for this source/group arrive.
Outgoing Interface(s)	The list of outgoing interfaces on which multicast packets for this source/group are forwarded.
Up Time(hh:mm:ss)	The time in seconds since the entry was created.
Expiry Time(hh:mm:ss)	The time in seconds before this entry will age out and be removed from the table.
RPF Neighbor	The IP address of the Reverse Path Forwarding neighbor.

Table 51.

Field	Description
Protocol	The multicast routing protocol which created this entry. The possibilities are: <ul style="list-style-type: none"> <li>• PIM-DM</li> <li>• PIM-SM</li> <li>• DVMRP</li> </ul>
Flags	The value displayed in this field is valid if the multicast routing protocol running is PIMSM. The possible values are RPT or SPT. For other protocols an "-----" is displayed.

## Multicast Global Configuration

To display the Multicast Global Configuration page, click **Routing > Multicast > Global Configuration**.



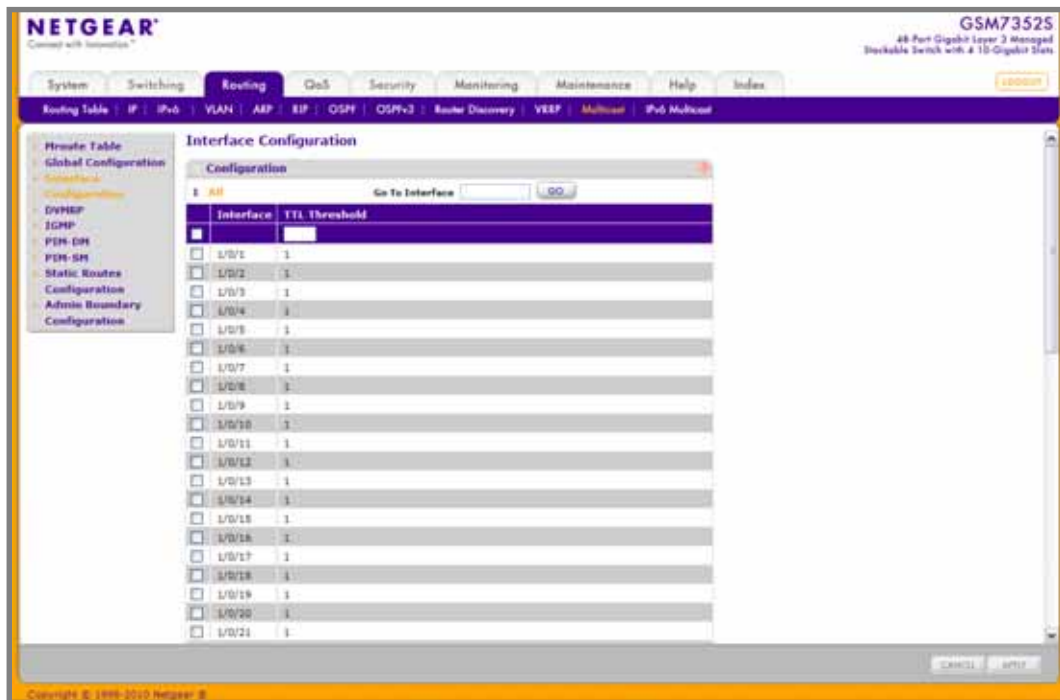
1. Use **Admin Mode** to set the administrative status of Multicast Forwarding in the router. The default is disable.

Table 52.

Field	Description
Protocol State	The operational state of the multicast forwarding module.
Table Maximum Entry Count	The maximum number of entries in the IP Multicast routing table.
Protocol	The multicast routing protocol presently activated on the router, if any.
Table Entry Count	The number of multicast route entries currently present in the Multicast route table.

## Multicast Interface Configuration

To display the Multicast Interface Configuration page, click **Routing > Multicast > Interface Configuration**.



1. **Interface** - The routing interface you want to configure or displayed.
2. Use **TTL Threshold** to enter the TTL threshold below which a multicast data packet will not be forwarded from the selected interface. You should enter a number between 0 and 255. If you enter 0 all multicast packets for the selected interface will be forwarded. You must configure at least one router interface before you will see this field.

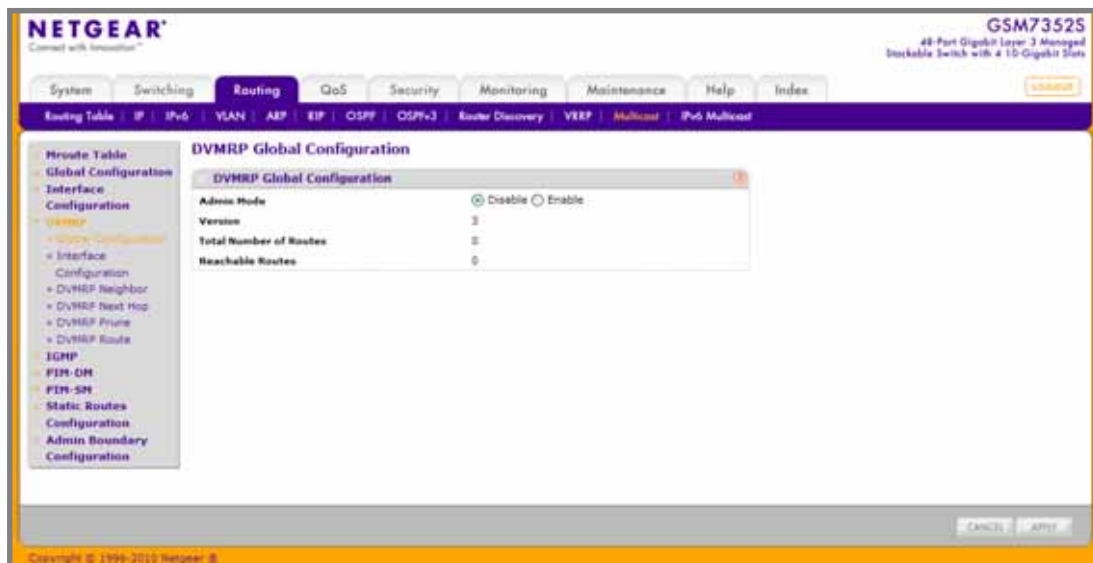
## DVMRP

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

- [DVMRP Global Configuration](#) on page 338
- [DVMRP Interface Configuration](#) on page 339
- [DVMRP Neighbor](#) on page 341
- [DVMRP Next Hop](#) on page 343
- [DVMRP Prune](#) on page 344
- [DVMRP Route](#) on page 345

### DVMRP Global Configuration

To display the Global Configuration page, click **Routing** > **Multicast** > **DVMRP** > **Global Configuration**.



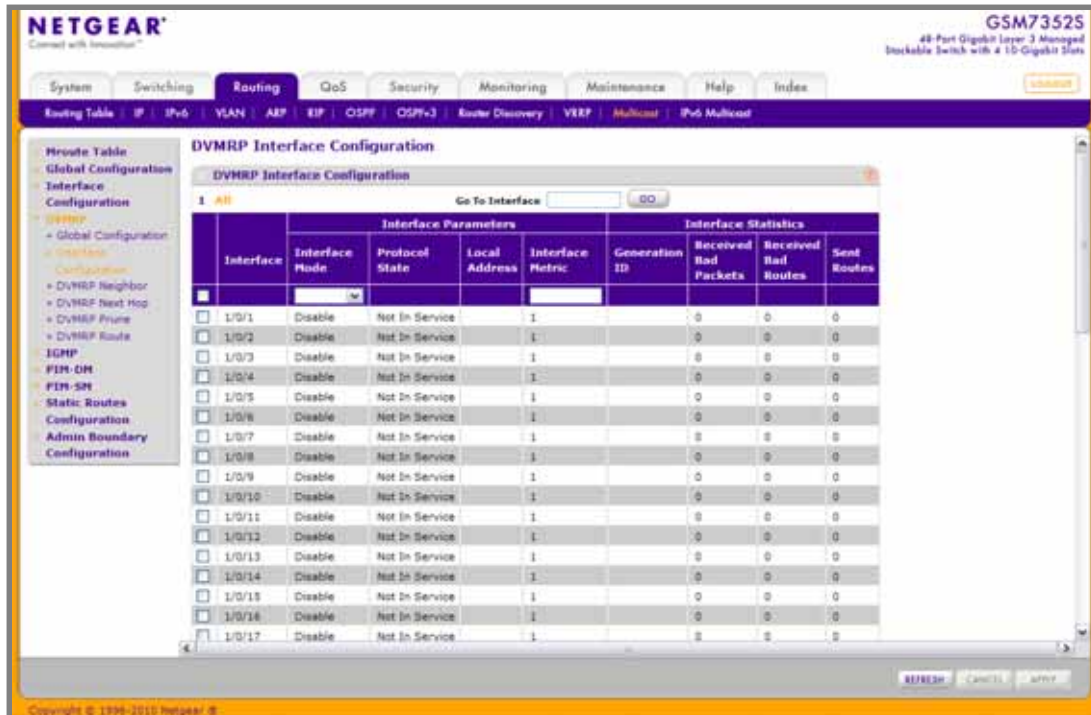
1. Use **Admin Mode** to set the administrative status of DVMRP to active or inactive. The default is disable.

**Table 53.**

Field	Description
Version	The current value of the DVMRP version string.
Total Number of Routes	The number of routes in the DVMRP routing table.
Reachable Routes	The number of routes in the DVMRP routing table that have a non-infinite metric.

## DVMRP Interface Configuration

To display the DVMRP Interface Configuration page, click **Routing** > **Multicast** > **DVMRP** > **Interface Configuration**.



1. Use **Interface** to select the interface for which data is to be configured.
2. Use **Interface Mode** to set the administrative mode of the selected DVMRP routing interface.
3. Use **Interface Metric** to enter the DVMRP metric for the selected interface. This value is sent in DVMRP messages as the cost to reach this network. Valid values are from(1 to 31). The default value is 1.
4. Click **REFRESH** to show the latest DVMRP interface information.

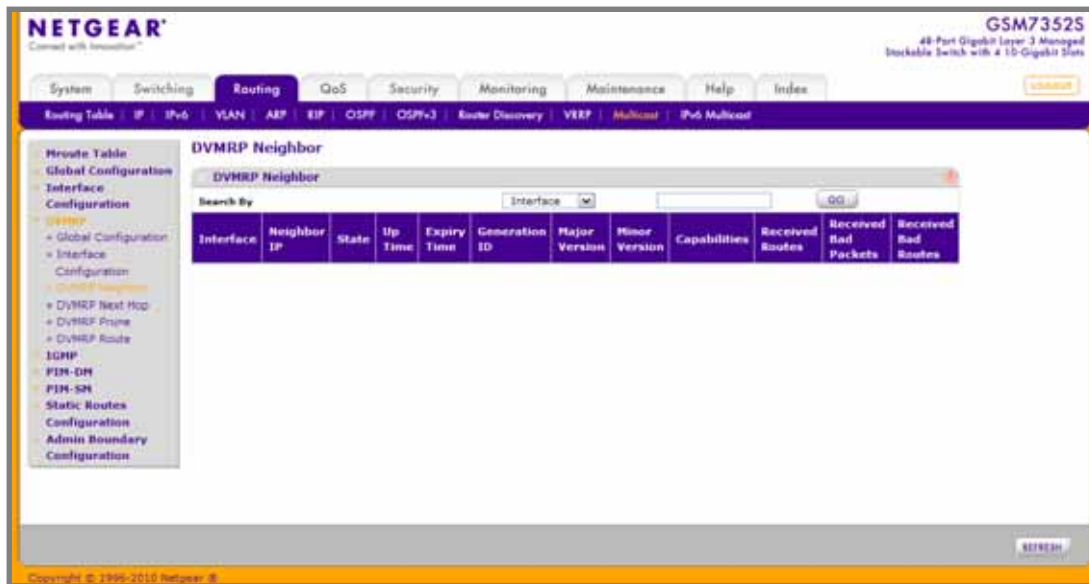
**Table 54.**

Field	Description
Protocol State	The operational state of the DVMRP protocol on the selected interface, either operational or non-operational.
Local Address	The IP address used as a source address in packets sent from the selected interface.
Generation ID	The DVMRP generation ID used by the router for the selected interface. This value is reset every time an interface is (re)started and is placed in prune messages. A change in generation ID informs the neighbor routers that any previous information about this router should be discarded.
Received Bad Packets	The number of invalid packets received on the selected interface.
Received Bad Routes	The number of invalid routes received on the selected interface.
Sent Routes	The number of routes sent on the selected interface.



## DVMRP Neighbor

To display the DVMRP Neighbor page, click **Routing** > **Multicast** > **DVMRP** > **DVMRP Neighbor**.



1. **Interface** - Select the interface for which data is to be displayed, or all interfaces will be displayed.
2. Use **Neighbor IP** to specify the IP address of the neighbor whose information is displayed.

**Table 55.**

Field	Description
State	The state of the specified neighbor router on the selected interface, either active or down.
Up Time	The DVMRP uptime for the specified neighbor on the selected interface. This is the time since the neighbor entry was learned.
Expiry Time	The DVMRP expiry time for the specified neighbor on the selected interface. This is the time left before this neighbor entry will age out, and is not applicable if the neighbor router's state is down.
Generation ID	The DVMRP generation ID for the specified neighbor on the selected interface.
Major Version	The DVMRP Major Version for the specified neighbor on the selected interface.
Minor Version	The DVMRP Minor Version for the specified neighbor on the selected interface.
Capabilities	The DVMRP capabilities of the specified neighbor on the selected interface.
Received Routes	The number of routes received for the specified neighbor on the selected interface.
Received Bad Packets	The number of invalid packets received for the specified neighbor on the selected interface.
Received Bad Routes	The number of invalid routes received for the specified neighbor on the selected interface.

## DVMRP Next Hop

To display the DVMRP Next Hop page, click **Routing** > **Multicast** > **DVMRP** > **DVMRP Next Hop**.

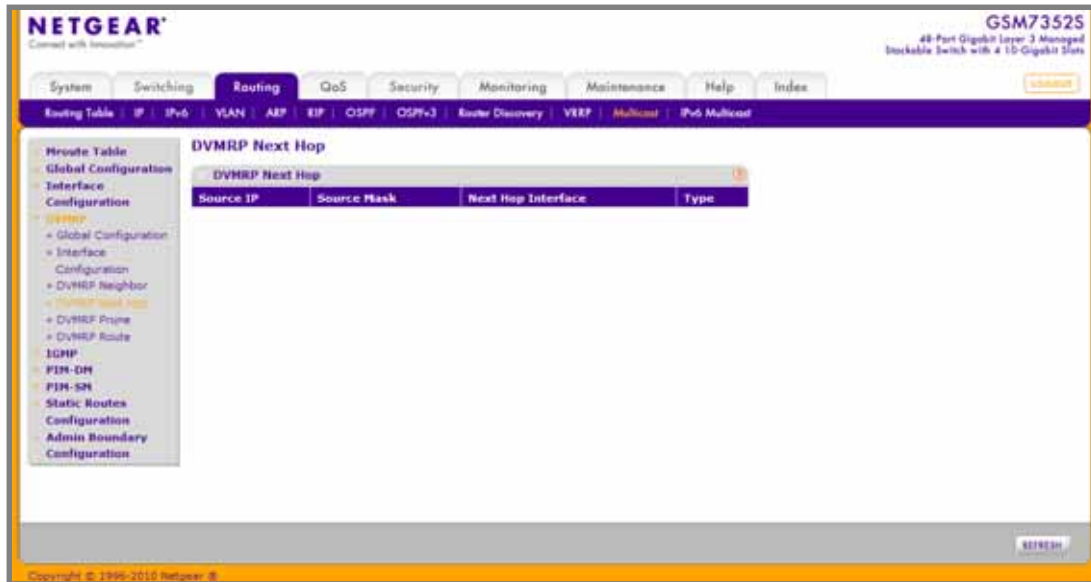


Table 56.

Field	Description
Source IP	The IP address used with the source mask to identify the source network for this table entry.
Source Mask	The network mask used with the source IP address.
Next Hop Interface	The outgoing interface for this next hop.
Type	The next hop type. 'Leaf' means that no downstream dependent neighbors exist on the outgoing interface. Otherwise, the type is 'branch'.

## DVMRP Prune

To display the DVMRP Prune page, click **Routing** > **Multicast** > **DVMRP** > **DVMRP Prune**.

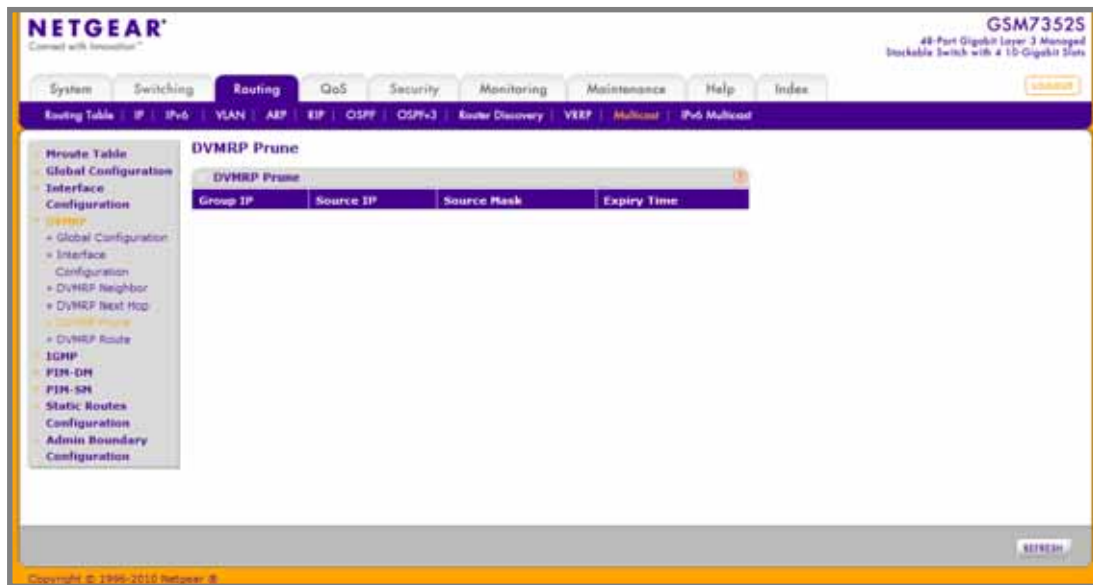


Table 57.

Field	Description
Group IP	The group address which has been pruned.
Source IP	The address of the source or source network which has been pruned.
Source Mask	The subnet mask to be combined with the source IP address to identify the source or source network which has been pruned.
Expiry Time	The amount of time remaining before this prune should expire at the upstream neighbor. If no prune messages have been received from downstream neighbors, this is set to value of the default prune lifetime timer, otherwise it is set to the smallest received value or the default timer, whichever is less.

## DVMRP Route

To display the DVMRP Route page, click **Routing** > **Multicast** > **DVMRP** > **DVMRP Route**.

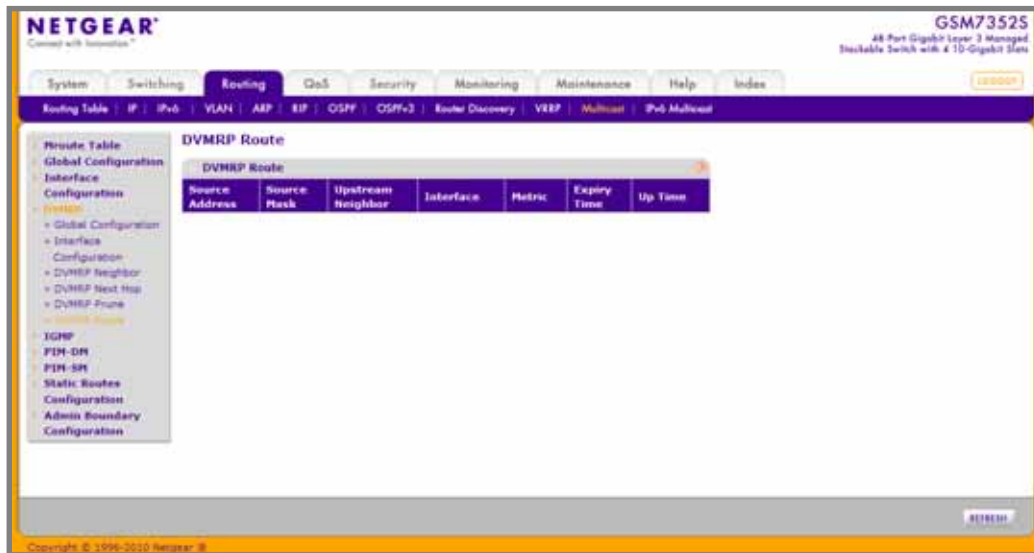


Table 58.

Field	Description
Source Address	The network address that is combined with the source mask to identify the sources for this entry.
Source Mask	The subnet mask to be combined with the source address to identify the sources for this entry.
Upstream Neighbor	The address of the upstream neighbor (e.g., RPF neighbor) from which IP datagrams from these sources are received.
Interface	The interface on which IP datagrams sent by these sources are received. A value of 0 typically means the route is an aggregate for which no next-hop interface exists.
Metric	The distance in hops to the source subnet.
Expiry Time	The minimum amount of time remaining before this entry will be aged out.
Up Time	The time since the route represented by this entry was learned by the router.

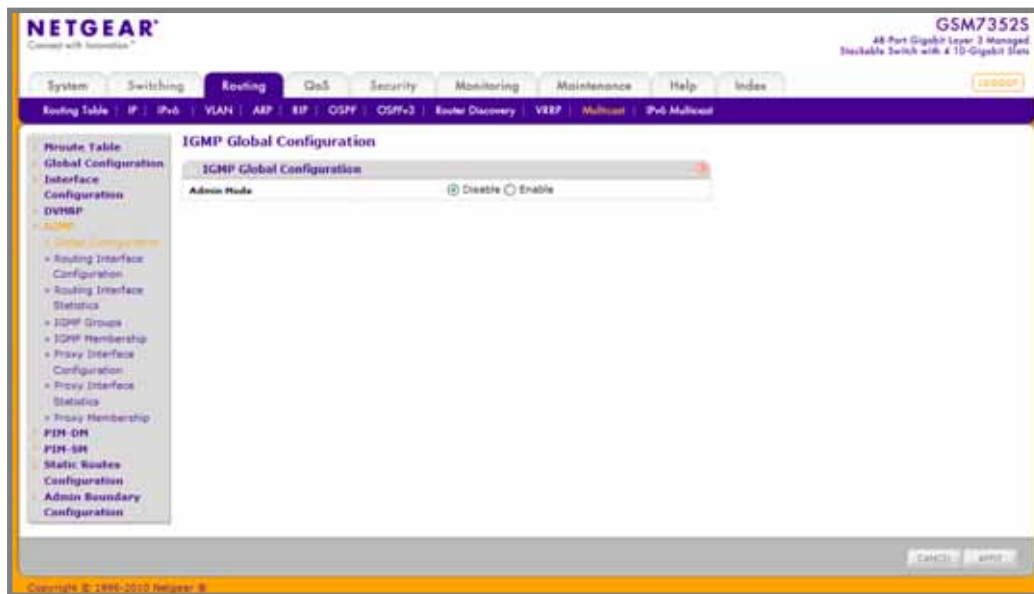
## IGMP

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

- [IGMP Global Configuration](#) on page 346
- [IGMP Routing Interface Configuration](#) on page 347
- [IGMP Routing Interface Statistics](#) on page 349
- [IGMP Groups](#) on page 351
- [IGMP Membership](#) on page 353
- [IGMP Proxy Interface Configuration](#) on page 354
- [IGMP Proxy Interface Statistics](#) on page 356
- [IGMP Proxy Membership](#) on page 357

### IGMP Global Configuration

To display the IGMP Global Configuration page, click **Routing** > **Multicast** > **IGMP** > **Global Configuration**.



1. Use **Admin Mode** to set the administrative status of IGMP in the router to active or inactive. The default is disable.

## IGMP Routing Interface Configuration

To display the IGMP Routing Interface Configuration page, click **Routing > Multicast > IGMP > Routing Interface Configuration**.

**NETGEAR**  
GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv2 | Router Discovery | VRRP | **Multicast** | IPv6 Multicast

**IGMP Routing Interface Configuration**

Go To Interface:

Interface	Admin Mode	Version	Robustness	Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval	Last Member Query Count
<input type="checkbox"/> 1/0/1	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/2	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/3	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/4	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/5	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/6	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/7	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/8	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/9	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/10	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/11	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/12	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/13	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/14	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/15	Disable	V3	2	125	100	31	2	10	2
<input type="checkbox"/> 1/0/16	Disable	V3	2	125	100	31	2	10	2

Copyright © 1999-2010 Netgear, Inc.

1. **Interface** - The interface for which data is to be displayed or configured.
2. Use **Admin Mode** to set the administrative status of IGMP on the selected interface. The default is disable.
3. Use **Version** to enter the version of IGMP you want to configure on the selected interface. Valid values are (1 to 3) and the default value is 3. This field is configurable only when IGMP interface mode is enabled.
4. Use **Robustness** to enter the robustness value. This variable allows tuning for the expected packet loss on a subnet. If you expect the subnet to be lossy, you should enter a higher number for this parameter. IGMP is robust to (robustness variable-1) packet losses. Valid values are from 1 to 255. The default value is 2.
5. Use **Query Interval** to enter the frequency in seconds at which IGMP host-query packets are to be transmitted on this interface. Valid values are from 1 to 1800. The default value is 125.
6. Use **Query Max Response Time** to enter the maximum query response time to be advertised in IGMPv2 queries on this interface, in tenths of a second. The default value is 100. Valid values are from (0 to 255).
7. Use **Startup Query Interval** to enter the number of seconds between the transmission of startup queries on the selected interface. The valid values are from 1 to 300. The default value is 31.
8. Use **Startup Query Count** to enter the number of queries to be sent on startup. The valid values are from 1 to 20. The default value is 2.
9. Use **Last Member Query Interval** to enter the last member query interval in tenths of a second. This is the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 255. The default value is 10. This value is not used for IGMP version 1.
10. Use **Last Member Query Count** to enter the number of queries to be sent on receiving a leave group report. Valid values are from 1 to 20. The default value is 2.



## IGMP Routing Interface Statistics

To display the IGMP Routing Interface Statistics page, click **Routing** > **Multicast** > **IGMP** > **Routing Interface Statistics**.

**NETGEAR**  
GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Routing Table | IP | IPv6 | VLAN | ARP | RIP | OSPF | OSPFv2 | Router Discovery | VRRP | **Multicast** | IPv6 Multicast

**IGMP Routing Interface Statistics**

1 All

Interface	IP Address	Subnet Mask	Protocol State	Querier IP	Querier Status	Querier Up Time	Querier Expiry Time	Wrong Version Queries Received	Number of Joins Received	Number of Groups
1/0/1	0.0.0.0	0.0.0.0	Non-Operational							
1/0/2	0.0.0.0	0.0.0.0	Non-Operational							
1/0/3	0.0.0.0	0.0.0.0	Non-Operational							
1/0/4	0.0.0.0	0.0.0.0	Non-Operational							
1/0/5	0.0.0.0	0.0.0.0	Non-Operational							
1/0/6	0.0.0.0	0.0.0.0	Non-Operational							
1/0/7	0.0.0.0	0.0.0.0	Non-Operational							
1/0/8	0.0.0.0	0.0.0.0	Non-Operational							
1/0/9	0.0.0.0	0.0.0.0	Non-Operational							
1/0/10	0.0.0.0	0.0.0.0	Non-Operational							
1/0/11	0.0.0.0	0.0.0.0	Non-Operational							
1/0/12	0.0.0.0	0.0.0.0	Non-Operational							
1/0/13	0.0.0.0	0.0.0.0	Non-Operational							
1/0/14	0.0.0.0	0.0.0.0	Non-Operational							
1/0/15	0.0.0.0	0.0.0.0	Non-Operational							
1/0/16	0.0.0.0	0.0.0.0	Non-Operational							
1/0/17	0.0.0.0	0.0.0.0	Non-Operational							
1/0/18	0.0.0.0	0.0.0.0	Non-Operational							
1/0/19	0.0.0.0	0.0.0.0	Non-Operational							

Copyright © 1999-2010 Netgear, Inc.

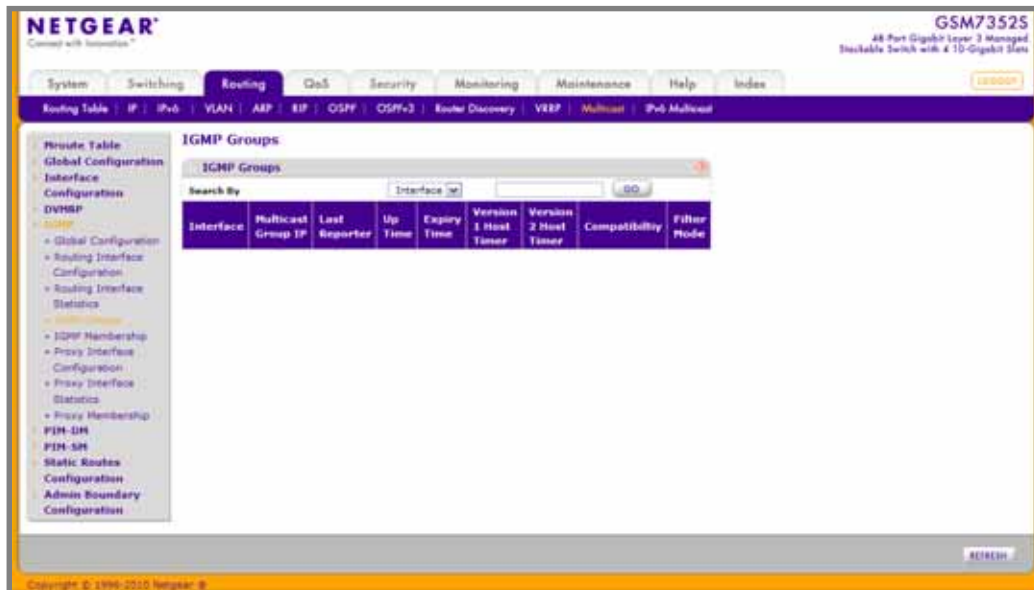
**Table 59.**

Field	Description
Interface	The interface on which the IGMP is enabled.
IP Address	The IP address of the selected interface.
Subnet Mask	The subnet mask for the IP address of the selected interface.
Protocol State	The operational state of IGMP on the selected interface.
Querier IP	The address of the IGMP querier on the IP subnet to which the selected interface is attached.
Querier Status	Indicates whether the selected interface is in querier or non querier mode.
Querier Up Time	The time in seconds since the IGMP interface querier was last changed.
Querier Expiry Time	The time in seconds remaining before the other querier present timer expires. If the local system is the querier, this will be zero.
Wrong Version Queries Received	The number of queries that have been received on the selected interface with an IGMP version that does not match the IGMP version configured for the interface, over the lifetime of the entry. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Therefore, a configuration error is indicated if any queries are received with the wrong version number.
Number of Joins Received	The number of times a group membership has been added on the selected interface; that is, the number of times an entry for this interface has been added to the cache table. This gives an indication of the amount of IGMP activity on the interface.
Number of Groups	The current number of entries for the selected interface in the cache table.

Click **REFRESH** to refresh the data on the screen with the latest IGMP interface statistics.

## IGMP Groups

To display the IGMP Groups page, click **Routing** > **Multicast** > **IGMP** > **IGMP Groups**.



**Table 60.**

Field	Description
Interface	The interface which data is to be displayed.
Multicast Group IP	The IP multicast group address for which data is to be displayed.
Last Reporter	The IP address of the source of the last membership report received for the IP Multicast group address on the selected interface.
Up Time	The time elapsed since this entry was created.
Expiry Time	The minimum amount of time remaining before this entry will be aged out.
Version 1 Host Timer	The time remaining until the local router will assume that there are no longer any IGMP version 1 members on the IP subnet attached to this interface. When an IGMPv1 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv2 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 1.
Version 2 Host Timer	The time remaining until the local router will assume that there are no longer any IGMP version 2 members on the IP subnet attached to this interface. When an IGMPv2 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv1 and IGMPv3 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 2.
Compatibility	This parameter shows group compatibility mode(v1, v2 and v3) for this group on the specified interface.
Filter Mode	The source filter mode (Include/Exclude/NA) for the specified group on this interface. When NA mode is active the field is blank

Click **REFRESH** to refresh the data on the screen with latest IGMP groups information.

## IGMP Membership

To display the IGMP Membership page, click **Routing** > **Multicast** > **IGMP** > **IGMP Membership**.

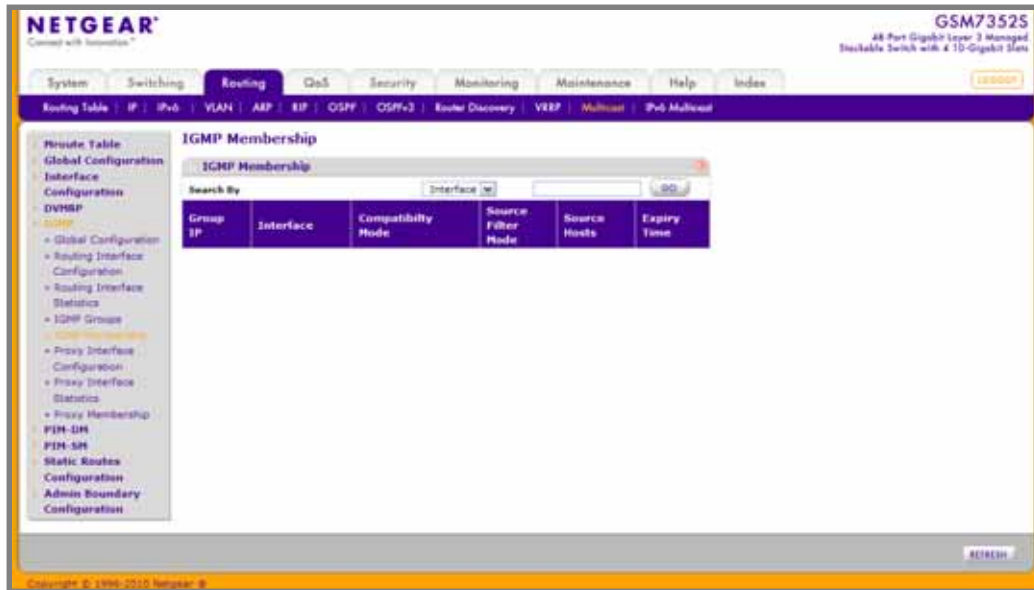


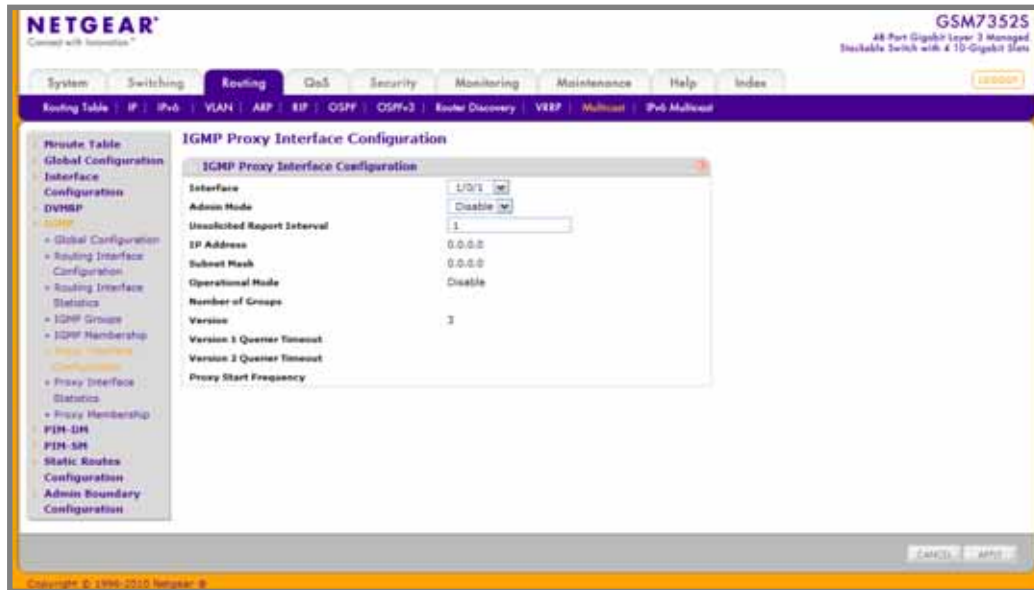
Table 61.

Field	Description
Group IP	The IP multicast group address for which data is to be displayed.
Interface	This parameter shows the interface on which multicast packets are forwarded.
Compatibility Mode	This parameter shows group compatibility mode (v1, v2 and v3) for this group on the specified interface.
Source Filter Mode	The source filter mode (Include/Exclude/NA) for the specified group on this interface.
Source Hosts	This parameter shows source addresses which are members of this multicast address.
Expiry Time	This parameter shows expiry time interval against each source address which are members of this multicast group. This is the amount of time after which the specified source entry is aged out.

Click **REFRESH** to refresh the data on the screen with latest IGMP member information.

## IGMP Proxy Interface Configuration

To display the IGMP Proxy Interface Configuration page, click **Routing > Multicast > IGMP > Proxy Interface Configuration**.



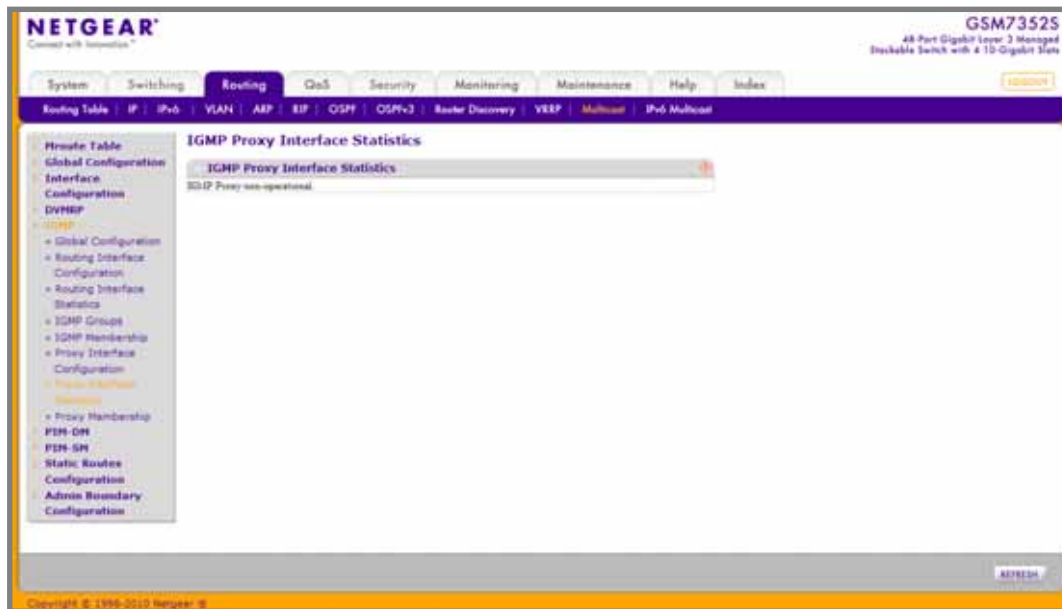
1. Use **Interface** to select the port for which data is to be configured. You must have configured at least one router interface before configuring or displaying data for an IGMP Proxy interface and it should not be a IGMP routing interface.
2. Use **Admin Mode** to set the administrative status of IGMP Proxy on the selected interface. The default is disable. Routing, IGMP and Multicast global admin modes should be enabled to enable IGMP Proxy interface mode.
3. Use **Version** to enter the version of IGMP you want to configure on the selected interface. Valid values are (1 to 3) and the default value is 3. This field is configurable only when IGMP Proxy interface mode is enabled.
4. Use **Unsolicited Report Interval** to enter the unsolicited time interval value in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Valid values are from (1 to 260). The default value is 1.

**Table 62.**

Field	Description
IP Address	The IP address of the IGMP Proxy interface.
Subnet Mask	The subnet mask for the IP address of the IGMP Proxy interface.
Operational Mode	The operational state of IGMP Proxy interface.
Number of Groups	The current number of multicast group entries for the IGMP Proxy interface in the cache table.
Version 1 Querier Timeout	The older IGMP version 1 querier timeout value in seconds. The Older Version Querier Interval is the time-out for transitioning a host back to IGMPv3 mode once an older version query is heard. When an older version query is received, hosts set their Older Version Querier Present Timer to Older Version Querier Interval.
Version 2 Querier Timeout	The older IGMP version 2 querier timeout value in seconds.
Proxy Start Frequency	The number of times the proxy was brought up.

## IGMP Proxy Interface Statistics

To display the IGMP Proxy Interface Statistics page, click **Routing > Multicast > IGMP > Proxy Interface Statistics**.



**Table 63.**

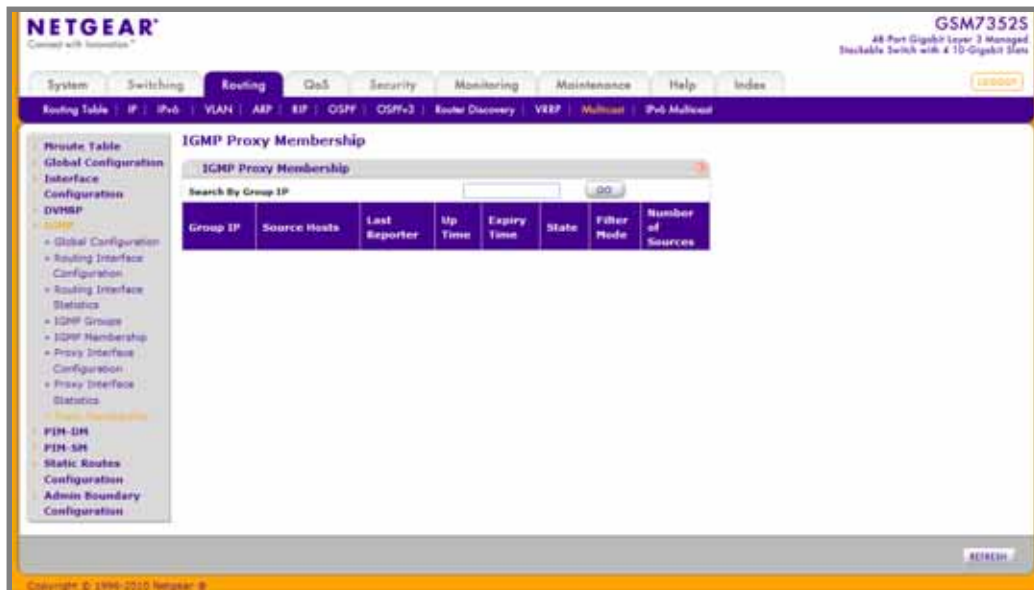
Field	Description
Interface	Displays the interface on which IGMP packets received.
Version	The version of IGMP packets received.
Queries Received	The number of IGMP queries received.
Report Received	The number of IGMP reports received.
Reports Sent	The number of IGMP reports sent.
Leaves Received	The number of IGMP leaves received.
Leaves Sent	The number of IGMP leaves sent.

Click **REFRESH** to refresh the data on the screen with the latest IGMP Proxy interface statistics.



## IGMP Proxy Membership

To display the IGMP Proxy Membership page, click **Routing** > **Multicast** > **IGMP** > **Proxy Membership**.



**Table 64.**

Field	Description
Group IP	Displays the IP multicast group address.
Proxy Interface	Displays the interface on which IGMP proxy is enabled.
Source Hosts	This parameter shows source addresses which are members of this multicast address.
Last Reporter	The IP address of the source of the last membership report received for the IP Multicast group address on the IGMP Proxy interface.
Uptime	The time elapsed since this entry was created.
Expiry Time	This parameter shows expiry time interval against each source address which is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.
State	The state of the host entry. A Host can be in one of the state. Non-member state - does not belong to the group on the interface. Delaying member state - host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. Idle member state - host belongs to the group on the interface and no report timer running.
Filter Mode	The group filter mode (Include/Exclude/None) for the specified group on the IGMP Proxy interface.
Number of Sources	The number of source hosts present in the selected multicast group.

Click **REFRESH** to refresh the data on the screen with latest IGMP proxy member information.

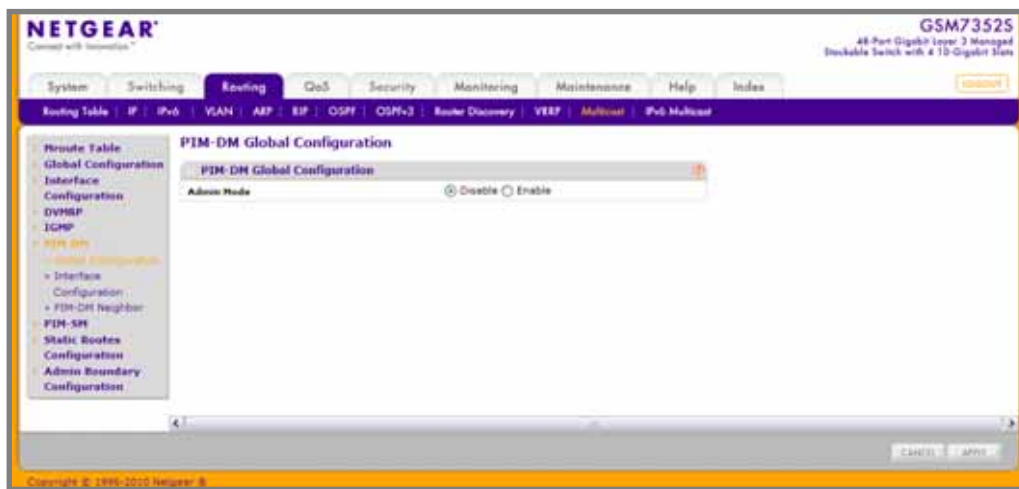
## PIM-DM

From the PIM-DM link, you can access the following pages:

- [PIM-DM Global Configuration](#) on page 359
- [PIM-DM Interface Configuration](#) on page 360
- [PIM-DM Neighbor](#) on page 361

### PIM-DM Global Configuration

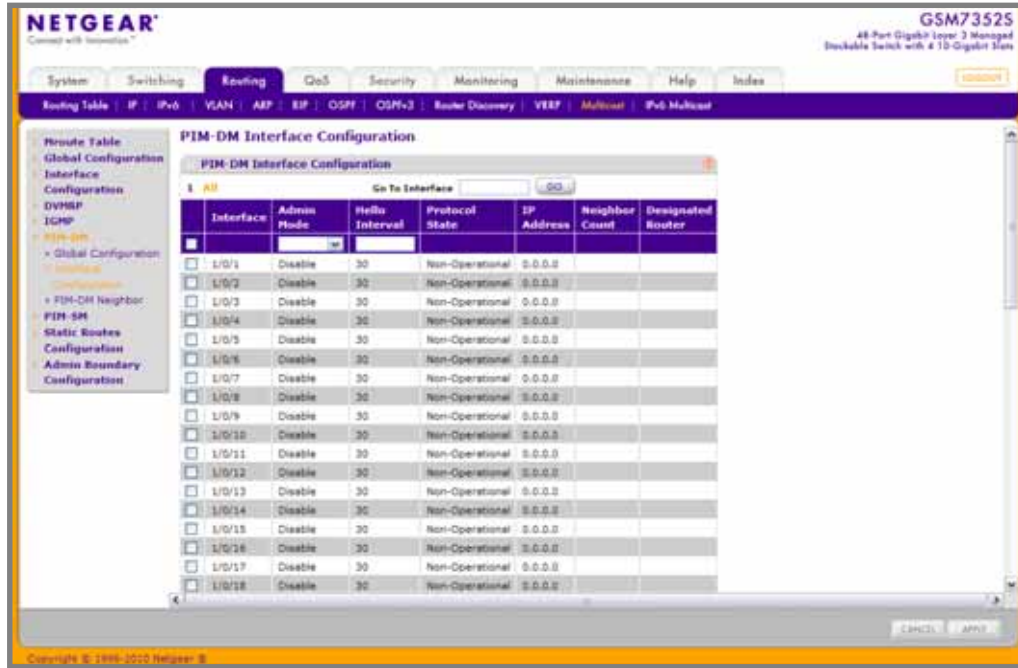
To display the PIM-DM Global Configuration page, click **Routing** > **Multicast** > **PIM-DM** > **Global Configuration**.



1. Use **Admin Mode** to set the administrative status of PIM-DM in the router. The default is disable.

## PIM-DM Interface Configuration

To display the PIM-DM Interface Configuration page, click **Routing** > **Multicast** > **PIM-DM** > **Interface Configuration**.



1. **Interface** - The interface for which data is to be displayed or configured. You must have configured at least one router interface before configuring or displaying data for a PIM-DM interface.
2. Use **Admin Mode** to set the administrative status of PIM-DM for the selected interface. The default is disable.
3. Use **Hello Interval** to enter the number of seconds between PIM hello messages transmitted from the selected interface. The default value is 30. Valid values are from 10 to 3600.

**Table 65.**

Field	Description
Protocol State	The operational state of the PIM-DM protocol on this interface.
IP Address	The IP address of the selected interface.
Neighbor Count	The number of PIM neighbors on the selected interface.
Designated Router	The designated router on the selected PIM interface. For point-to-point interfaces, this will be 0.0.0.0.

## PIM-DM Neighbor

To display the PIM-DM Neighbor page, click **Routing** > **Multicast** > **PIM-DM** > **Neighbor Configuration**.

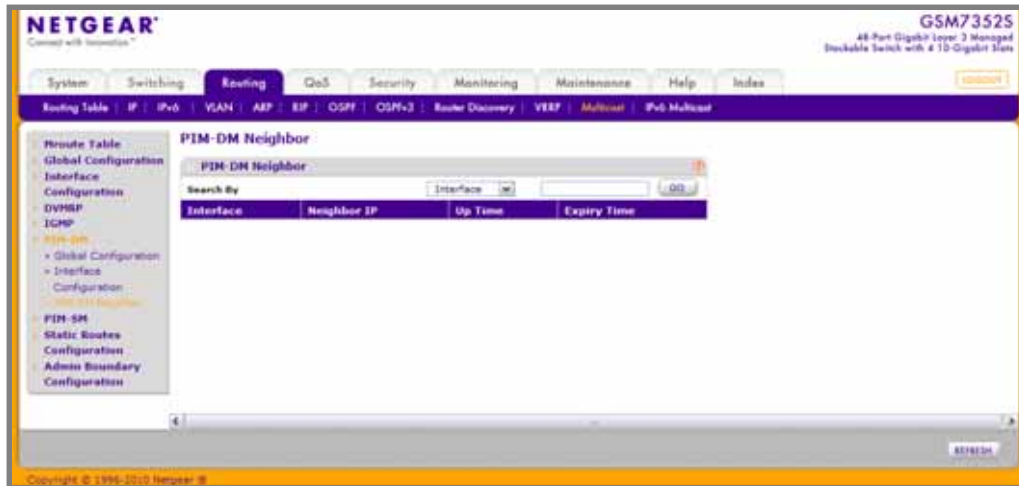


Table 66.

Field	Description
Interface	The physical interface on which PIM-DM is enabled.
Neighbor IP	The IP address of the PIM neighbor for which this entry contains information.
Up Time	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time	The minimum time remaining before this PIM neighbor will be aged out.

Click **REFRESH** to refresh the data on the screen with latest PIM-DM neighbor information

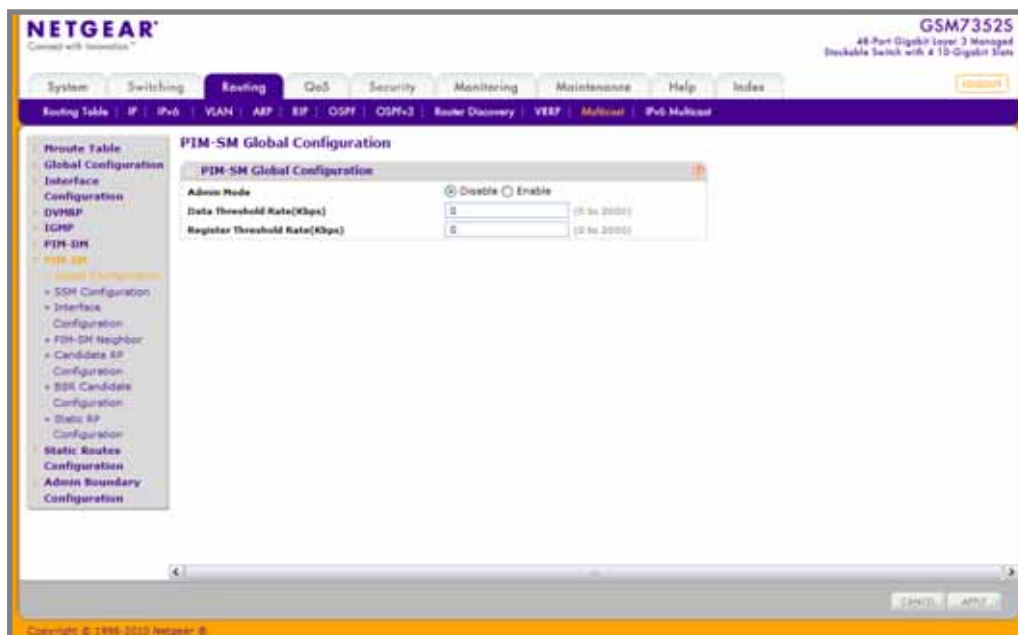
## PIM-SM

From the PIM-SM link, you can access the following pages:

- [PIM-SM Global Configuration](#) on page 362
- [PIM SSM Configuration](#) on page 363
- [PIM-SM Interface Configuration](#) on page 364
- [PIM-SM Neighbor](#) on page 366
- [PIM-SM Candidate RP Configuration](#) on page 367
- [PIM-SM BSR Candidate Configuration](#) on page 368
- [PIM-SM Static RP Configuration](#) on page 369

### PIM-SM Global Configuration

To display the PIM-SM Global Configuration page, click **Routing** > **Multicast** > **PIM-SM** > **Global Configuration**.

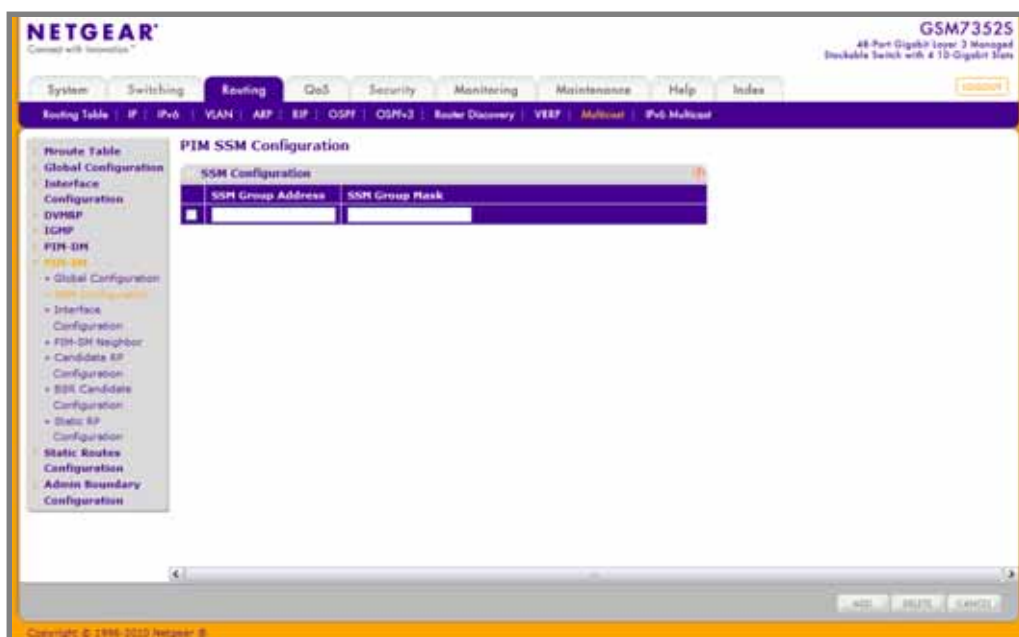


1. Use **Admin Mode** to set the administrative status of PIM-SM in the router. The default is disable.
2. Use **Data Threshold Rate (kbps)** to enter the rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree. The valid values are from 0 to 2000. The default value is 0
3. Use **Register Threshold Rate (kbps)** to enter the rate in K bits/second above which the Rendezvous Point router will switch to a source-specific shortest path tree. The valid values are from 0 to 2000. The default value is 0

## PIM SSM Configuration

While PIM-SM employs a specially-configured RP router that serves as a meeting junction for multicast senders and listeners, Protocol-Independent Multicast Source Specific Multicast (PIM-SSM) does not use an RP. It supports only source route deliver trees. It is used between routers so that they can track which multicast packets to forward to each other and to their directly-connected LANs. The SSM service model can be implemented with a strict subset of the PIM-SM protocol mechanisms. Both regular IP Multicast and SSM semantics can coexist on a single router and both can be implemented using the PIM-SM protocol. A range of multicast addresses, currently 232.0.0.0/8 in IPv4, is reserved for SSM.

To display the PIM SSM Configuration page, click **Routing > Multicast > PIM-SM > SSM Configuration**.



1. Use **SSM Group Address** to enter the source-specific multicast group ip-address.
2. Use **SSM Group Mask** to enter the source-specific multicast group ip-address mask.
3. Click **ADD** to add a new source-specific group.
4. Click **DELETE** to delete an existing source-specific group.

## PIM-SM Interface Configuration

To display the PIM-SM Interface Configuration page, click **Routing** > **Multicast** > **PIM-SM** > **Interface Configuration**.

**NETGEAR**  
Connect with Innovation™

GSM73525  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Routing Table IP IPv6 VLAN ARP RIP OSPF OSPF-3 Router Discovery VRRP **Multicast** IPv6 Multicast

Route Table  
Global Configuration  
Interface Configuration  
IGMP  
PIM-DM  
**PIM-SM**  
+ Global Configuration  
+ SM Configuration  
+ PIM-SM Neighbor Configuration  
+ Candidate RP Configuration  
+ SDA Candidate Configuration  
+ Static RP Configuration  
Static Routes  
Configuration  
Admin Boundary Configuration

### PIM-SM Interface Configuration

Go To Interface:

Interface	Admin. Mode	Protocol State	IP Address	Hello Interval(secs)	Join/Prune Interval(secs)	RSR Border	DR Priority	Designated Router	Neighbor Count
<input type="checkbox"/> 1/0/1	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/2	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/3	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/4	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/5	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/6	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/7	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/8	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/9	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/10	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/11	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/12	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/13	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/14	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/15	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/16	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/17	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/18	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	
<input type="checkbox"/> 1/0/19	Disable	Non-Operational	0.0.0.0	30	60	Disable	1	1	

Copyright © 1999-2013 Netgear, Inc.



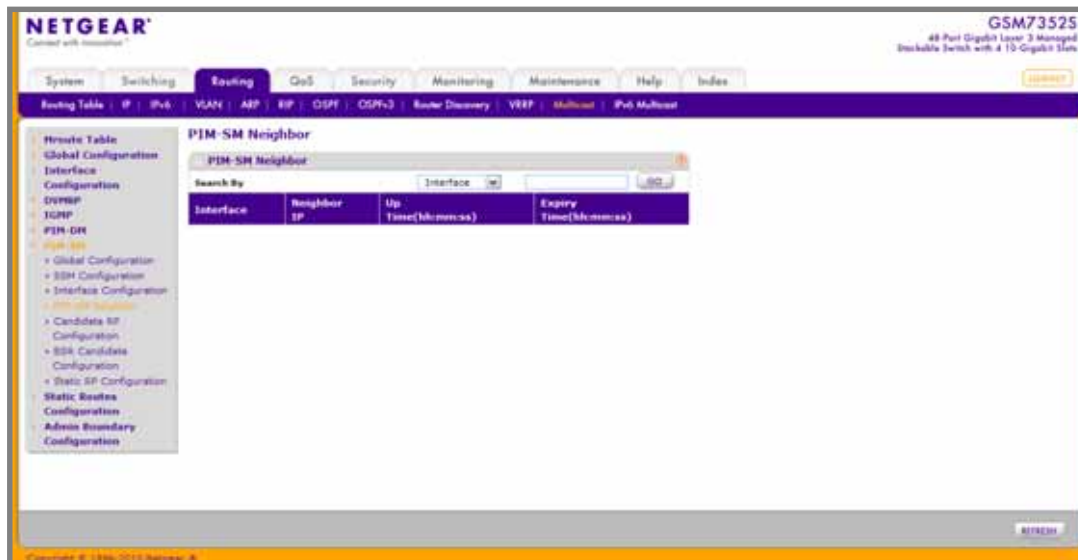
1. **Interface** - The interface for which data is to be configured or to be displayed.
2. Use **Admin Mode** to set the administrative status of PIM-SM in the router. The default is disable.
3. Use **Hello Interval(secs)** to enter the time in seconds between the transmission of which PIM Hello messages on this interface. The valid values are from 0 to 18000. The default value is 30.
4. Use **Join/Prune Interval(secs)** to enter the frequency at which PIM Join/Prune messages are transmitted on this PIM interface. The valid values are from 0 to 18000. The default value is 60.
5. Use **BSR Border** to set BSR border status on the selected interface.
6. Use **DR Priority** to enter the DR priority for the selected interface. The valid values are from 0 to 2147483647. The default value is 1.

**Table 67.**

Field	Description
Protocol State	The state of PIM-SM in the router: either operational or non-operational.
IP Address	The IPv4 address of the selected PIM interface.
Designated Router	The Designated Router on the selected PIM interface.
Neighbor Count	The number of PIM neighbors on the selected interface.

## PIM-SM Neighbor

To display the PIM-SM Neighbor page, click **Routing > Multicast > PIM-SM > PIM-SM Neighbor**.



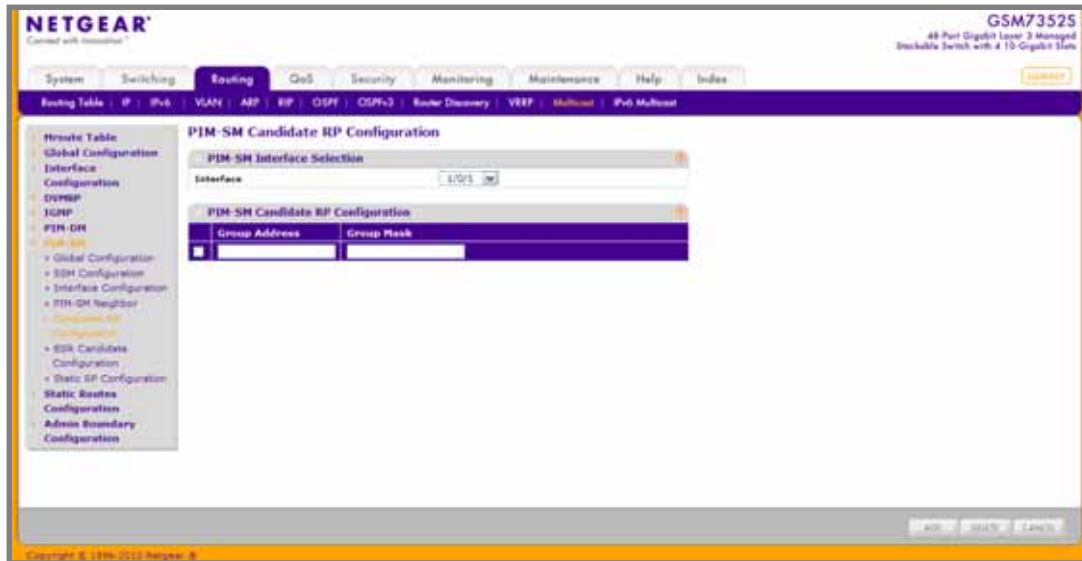
**Table 68.**

Field	Description
Interface	The interface on which neighbor is displayed.
Neighbor IP	The IP address of the PIM neighbor for this entry.
Up Time	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time	The minimum time remaining before this PIM neighbor will be aged out.

Click **REFRESH** to refresh the data on the screen with the latest PIM-SM neighbor information.

## PIM-SM Candidate RP Configuration

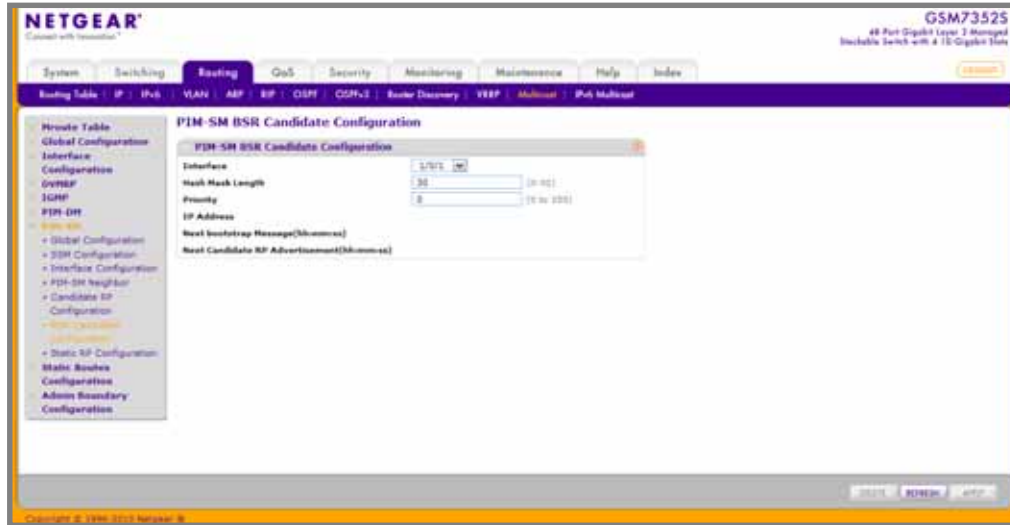
To display the PIM-SM Candidate RP Configuration page, click **Routing** > **Multicast** > **PIM-SM** > **Candidate RP Configuration**.



1. Use **Interface** to select the interface for which data is to be displayed.
2. Use **Group Address** to specify the group address transmitted in Candidate-RP-Advertisements.
3. Use **Group Mask** to specify the group address mask transmitted in Candidate-RP-Advertisements.
4. Click **ADD** to add a new Candidate RP Address for the PIM-SM router.
5. Click **DELETE** to delete an extant Candidate RP Address for the PIM-SM router.

## PIM-SM BSR Candidate Configuration

To display the PIM-SM BSR Candidate Configuration page, click **Routing > Multicast > PIM-SM > BSR Candidate Configuration**.



1. Use **Interface** to select the interface for which data is to be configured.
2. Use **Priority** to enter the priority of C-BSR.
3. Use **Hash Mask Length** to enter the C-BSR hash mask length to be advertised in bootstrap messages. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid values are from 0 to 32. Default value is 30.
4. Click **DELETE** to delete the RP address selected.
5. Click **REFRESH** to refresh the data on the screen with the latest PIM-SM neighbor information.

**Table 69.**

Field	Description
IP Address	Displays the IP address of the Elected BSR.
Next bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP Advertisement	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

## PIM-SM Static RP Configuration

This page is used to statically configure the RP address for one or more multicast groups.

To display the PIM-SM Static RP Configuration page, click **Routing > Multicast > PIM-SM > Static RP Configuration**.

The screenshot shows the NETGEAR ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual. The page is titled "PIM-SM Static RP Configuration". The navigation menu on the left includes System, Switching, Routing, and Multicast. The main content area is titled "PIM-SM Static RP Configuration" and contains a table for configuring static RP addresses. The table has columns for RP Address, Group Address, Group Mask, and Override. Below the table are buttons for ADD, DELETE, and APPLY.

RP Address	Group Address	Group Mask	Override
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Buttons: ADD, DELETE, APPLY

1. Use **RP Address** to specify the IP Address of the RP to be created or deleted.
2. Use **Group Address** to specify the Group Address of the RP to be created or deleted.
3. Use **Group Mask** to specify the Group Mask of the RP to be created or deleted.
4. Use **Override** to indicate that if there is a conflict, the RP configured with this option prevails over the RP learned by BSR.
5. Click **ADD** to add a new static RP address for one or more multicast groups.
6. Click **DELETE** to delete the RP address selected.

## Static Routes Configuration

To display the Static Routes Configuration page, click **Routing** > **Multicast** > **Static Routes Configuration**.

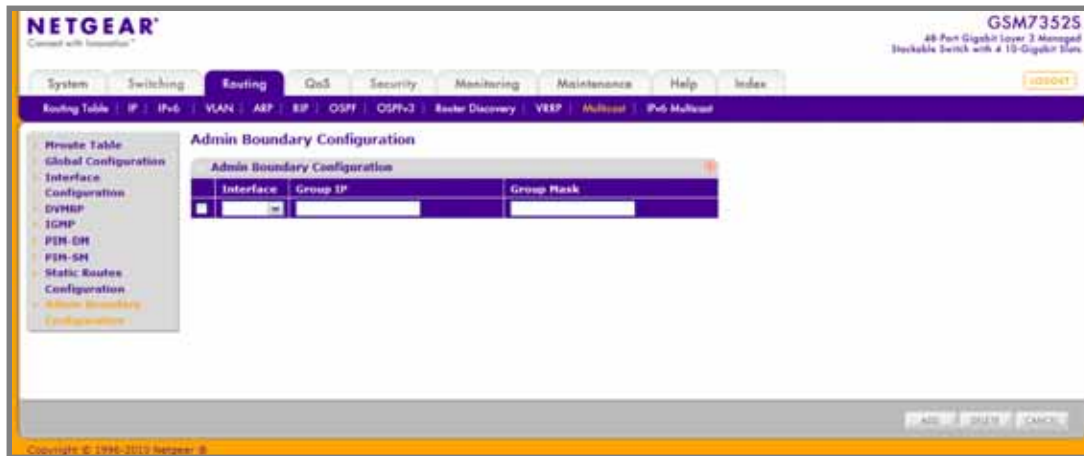


1. Use **Source IP** to enter the IP Address that identifies the multicast packet source for the entry you are creating.
2. Use **Source Mask** to enter the subnet mask to be applied to the Source IP address.
3. Use **RPF Neighbor** to enter the IP address of the neighbor router on the path to the source.
4. Use **Metric** to enter the link state cost of the path to the multicast source. The range is 0 - 255 and the default is one. You can change the metric for a configured route by selecting the static route and editing this field.
5. Use **RPF Interface** to select the interface number. This is the interface that connects to the neighbor router for the given source IP address.
6. Click **ADD** to add a new static route to the switch.
7. Click **DELETE** to delete the multicast static routes selected.

## Admin Boundary Configuration

The definition of an administratively scoped boundary is a mechanism to stop the ingress and egress of multicast traffic for a given range of multicast addresses on a given routing interface.

To display the Admin Boundary Configuration page, click **Routing** > **Multicast** > **Admin Boundary Configuration**.



1. Use **Interface** to select the router interface for which the administratively scoped boundary is to be configured.
2. Use **Group IP** to enter the multicast group address for the start of the range of addresses to be excluded. The address must be in the range of 239.0.0.0 through 239.255.255.255.
3. Use **Group Mask** to enter the mask to be applied to the multicast group address. The combination of the mask and the Group IP gives the range of administratively scoped addresses for the selected interface.
4. Click **ADD** to add a new administratively scoped boundary.
5. Click **DELETE** to delete the administratively scoped boundary selected.

## IPv6 Multicast

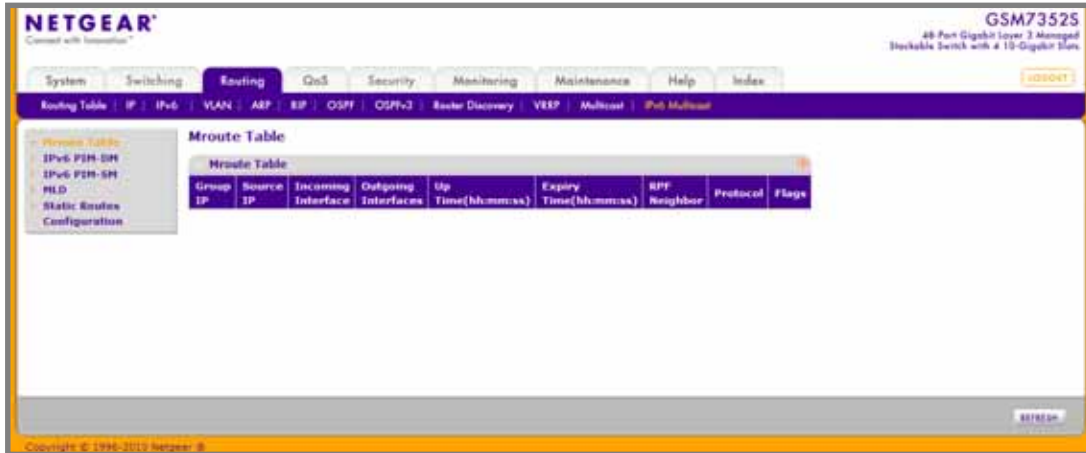
From the IPv6 Multicast link, you can access the following pages:

- [Mroute Table](#) on page 372
- [IPv6 PIM-DM](#) on page 374
- [IPv6 PIM-SM](#) on page 377
- [MLD](#) on page 385
- [Static Routes Configuration](#) on page 397

## Mroute Table

This screen displays contents of the Mroute Table in tabular form.

To display the Mroute Table page, click **Routing > IPv6 Multicast > Mroute Table**.



The screenshot shows the Netgear web interface for a GSM7352S switch. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Routing tab is selected, and the sub-menu shows Routing Table, IP, IPv6, VLAN, ARP, RIP, OSPF, OSPFv2, Route Discovery, VRRP, Multicast, and IPv6 Multicast. The IPv6 Multicast sub-menu is selected, and the Mroute Table page is displayed. The Mroute Table is a table with columns: Group, Source, Incoming Interface, Outgoing Interfaces, Up Time, Expiry Time, RPF Neighbor, Protocol, and Flags. The table is currently empty. The bottom of the page shows the copyright notice: Copyright © 1998-2012 Netgear, Inc.



**Table 70.**

Field	Description
Source IP	The IP address of the multicast packet source to be combined with the Group IP to fully identify a single route whose Mroute table entry.
Group IP	The destination group IP address.
Incoming Interface	The incoming interface on which multicast packets for this source/group arrive.
Outgoing Interface(s)	The list of outgoing interfaces on which multicast packets for this source/group are forwarded.
Up Time(hh:mm:ss)	The time in seconds since the entry was created.
Expiry Time(hh:mm:ss)	The time in seconds before this entry will age out and be removed from the table.
RPF Neighbor	The IP address of the Reverse Path Forwarding neighbor.
Protocol	The multicast routing protocol which created this entry. The possibilities are: <ul style="list-style-type: none"> <li>• PIM-DM</li> <li>• PIM-SM</li> </ul>
Flags	The value displayed in this field is valid if the multicast routing protocol running is PIMSM. The possible values are RPT or SPT. For other protocols an "-----" is displayed.

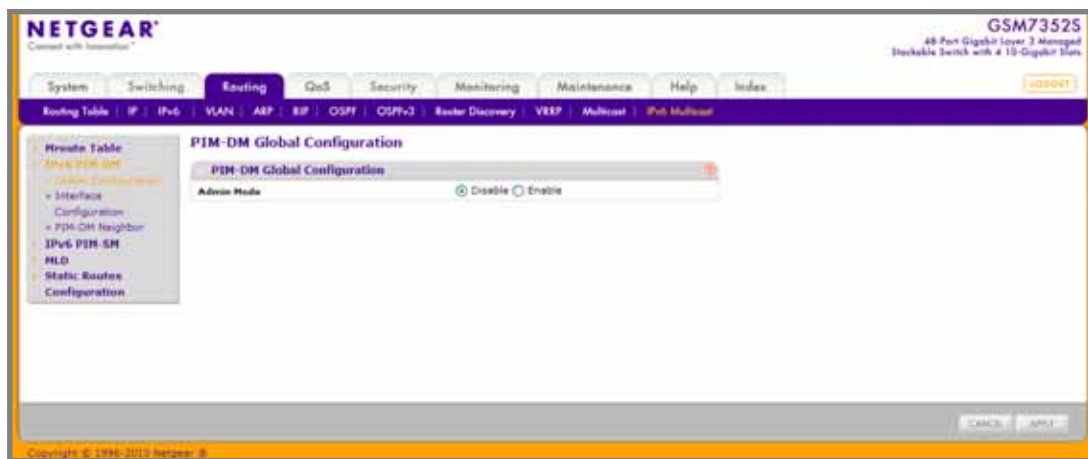
## IPv6 PIM-DM

From the IPv6 PIM-DM link, you can access the following pages:

- [PIM-DM Global Configuration](#) on page 374
- [PIM-DM Interface Configuration](#) on page 375
- [PIM-DM Neighbor](#) on page 376

### PIM-DM Global Configuration

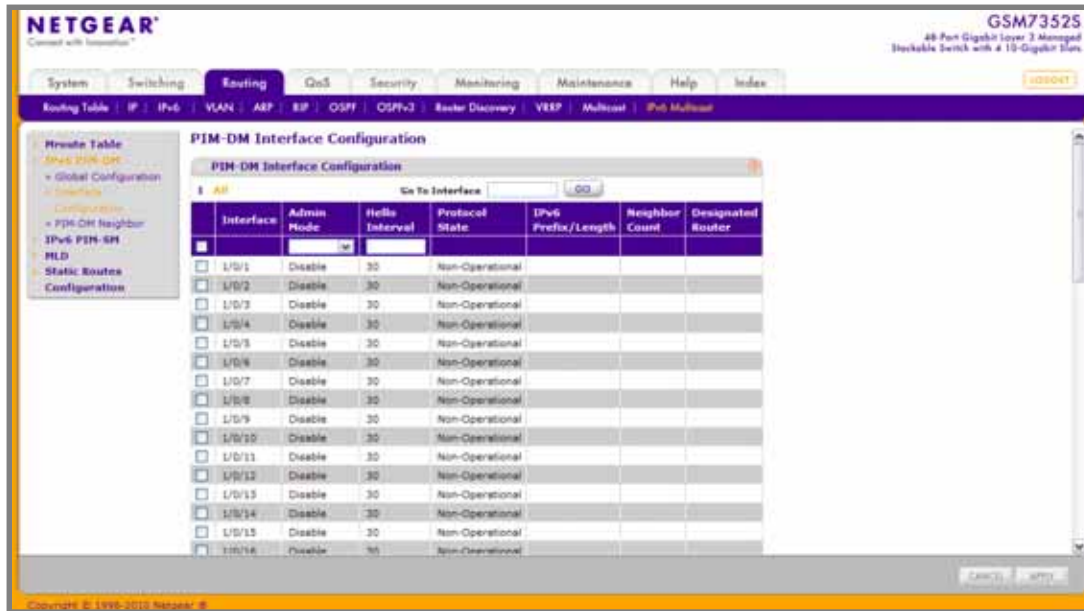
To display the IPv6 PIM-DM Global Configuration page, click **Routing > IPv6 Multicast > PIM-DM > Global Configuration**.



1. Use **Admin Mode** to set the administrative status of PIM-DM in the router. The default is disable.

## PIM-DM Interface Configuration

To display the IPv6 PIM-DM Interface Configuration page, click **Routing > IPv6 Multicast > PIM-DM > Interface Configuration**.



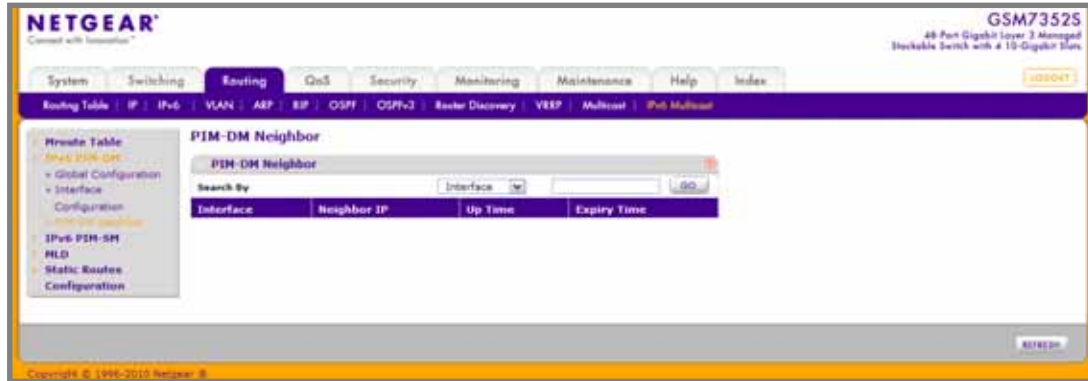
1. **Interface** - The interface for which data is to be displayed or configured. You must have configured at least one router interface before configuring or displaying data for a PIM-DM interface.
2. Use **Admin Mode** to set the administrative status of PIM-DM for the selected interface. The default is disable.
3. Use **Hello Interval** to enter the number of seconds between PIM hello messages transmitted from the selected interface. The default value is 30. Valid values are from 10 to 3600.

**Table 71.**

Field	Description
Protocol State	The operational state of the PIM-DM protocol on this interface.
IPv6 Prefix/Length	The IPv6 Address Prefix and the Length of the selected interface.
Neighbor Count	The number of PIM neighbors on the selected interface.
Designated Router	The designated router on the selected PIM interface. For point-to-point interfaces, this will be 0.0.0.0.

## PIM-DM Neighbor

To display the IPv6 PIM-DM Neighbor page, click **Routing > IPv6 Multicast > PIM-DM > PIM-DM Neighbor**.



**Table 72.**

Field	Description
Interface	The physical interface on which PIM-DM is enabled.
Neighbor IP	The IP address of the PIM neighbor for which this entry contains information.
Up Time	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time	The minimum time remaining before this PIM neighbor will be aged out.

Click **REFRESH** to refresh the data on the screen with the latest PIM-DM neighbor information.

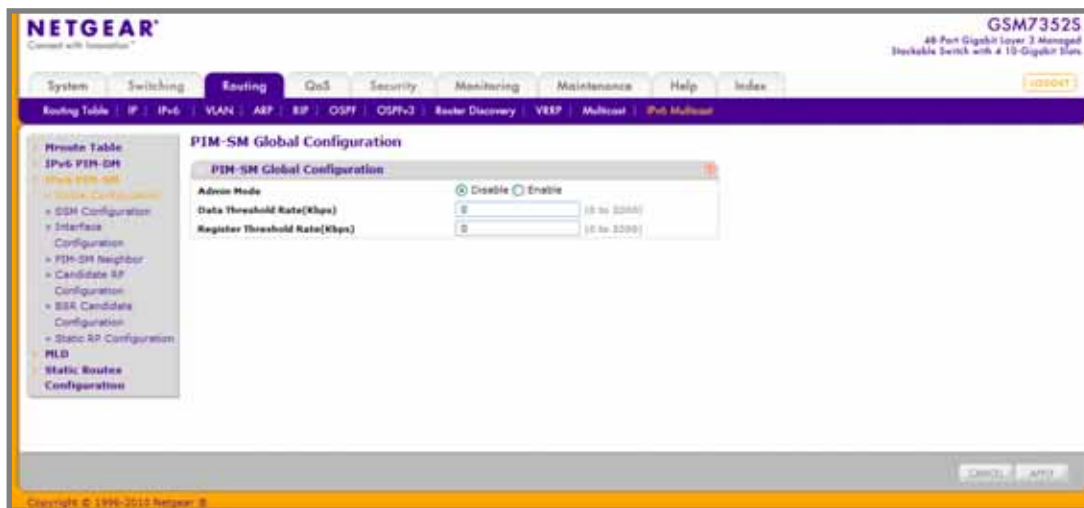
## IPv6 PIM-SM

From the IPv6 PIM-SM link, you can access the following pages:

- *PIM-SM Global Configuration* on page 377
- *PIM SSM Configuration* on page 378
- *PIM-SM Interface Configuration* on page 379
- *PIM-SM Neighbor* on page 381
- *PIM-SM Candidate RP Configuration* on page 382
- *PIM-SM BSR Candidate Configuration* on page 383
- *PIM-SM Static RP Configuration* on page 384

## PIM-SM Global Configuration

To display the IPv6 PIM-SM Global Configuration page, click **Routing > IPv6 Multicast > PIM-SM > Global Configuration**.

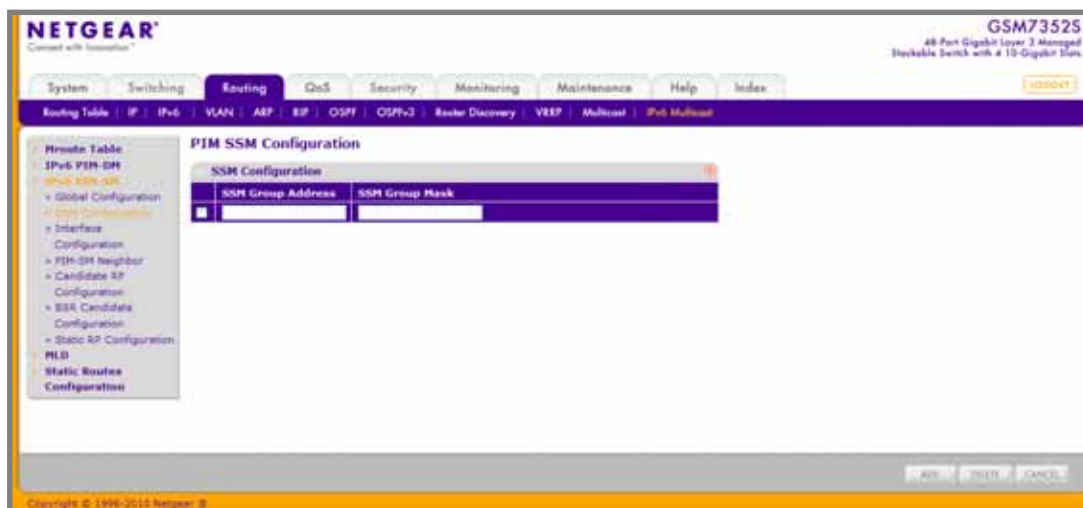


1. Use **Admin Mode** to set the administrative status of PIM-SM in the router. The default is disable.
2. Use **Data Threshold Rate(kbps)** to enter the rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree. The valid values are from 0 to 2000. The default value is 0.
3. Use **Register Threshold Rate(kbps)** to enter rate in K bits/second above which the Rendezvous Point router will switch to a source-specific shortest path tree. The valid values are from 0 to 2000. The default value is 0.

## PIM SSM Configuration

While PIM-SM employs a specially-configured RP router that serves as a meeting junction for multicast senders and listeners, Protocol-Independent Multicast Source Specific Multicast (PIM-SSM) does not use an RP. It supports only source route deliver trees. It is used between routers so that they can track which multicast packets to forward to each other and to their directly-connected LANs. The SSM service model can be implemented with a strict subset of the PIM-SM protocol mechanisms. Both regular IP Multicast and SSM semantics can coexist on a single router and both can be implemented using the PIM-SM protocol. A range of multicast addresses, currently FF3x::/96 in IPv6, is reserved for SSM.

To display the PIM SSM Configuration page, click **Routing > IPv6 Multicast > PIM-SM > SSM Configuration**.



1. Use **SSM Group Address** to enter the source-specific multicast group ip-address.
2. Use **SSM Group Mask** to enter the source-specific multicast IPv6 group prefix length.
3. Click **ADD** to add a new source-specific group.
4. Click **DELETE** to delete an extant source-specific group.
5. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

## PIM-SM Interface Configuration

To display the IPv6 PIM-SM Interface Configuration page, click **Routing > IPv6 Multicast > PIM-SM > Interface Configuration**.

**NETGEAR**  
GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Routing Table IP IPv6 VLAN ARP RIP OSPF OSPF3 Router Discovery VRRP Multicast IPv6 Multicast

**PIM-SM Interface Configuration**

Go To Interface

Interface	Admin Mode	Protocol State	IPv6 Prefix/Length	Hello Interval (secs)	Join/Prune Interval (secs)	BSR Border	DR Priority	Designated Router	Neighbor Count
<input type="checkbox"/> 1/0/1	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/2	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/3	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/4	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/5	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/6	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/7	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/8	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/9	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/10	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/11	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/12	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/13	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/14	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/15	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/16	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/17	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/> 1/0/18	Disable	Non-Operational		30	60	Disable	1		

Copyright © 1996-2012 Netgear, Inc.

1. **Interface** - The interface for which data is to be configured or to be displayed.
2. Use **Admin Mode** to set the administrative status of PIM-SM in the router. The default is disable.
3. Use **Hello Interval(secs)** to enter the time in seconds between the transmission of which PIM Hello messages on this interface. The valid values are from 0 to 18000. The default value is 30.
4. Use **Join/Prune Interval(secs)** to enter the frequency at which PIM Join/Prune messages are transmitted on this PIM interface. The valid values are from 0 to 18000. The default value is 60.
5. Use **BSR Border** to set BSR border status on the selected interface.
6. Use **DR Priority** to enter the DR priority for the selected interface. The valid values are from 0 to 2147483647. The default value is 1.

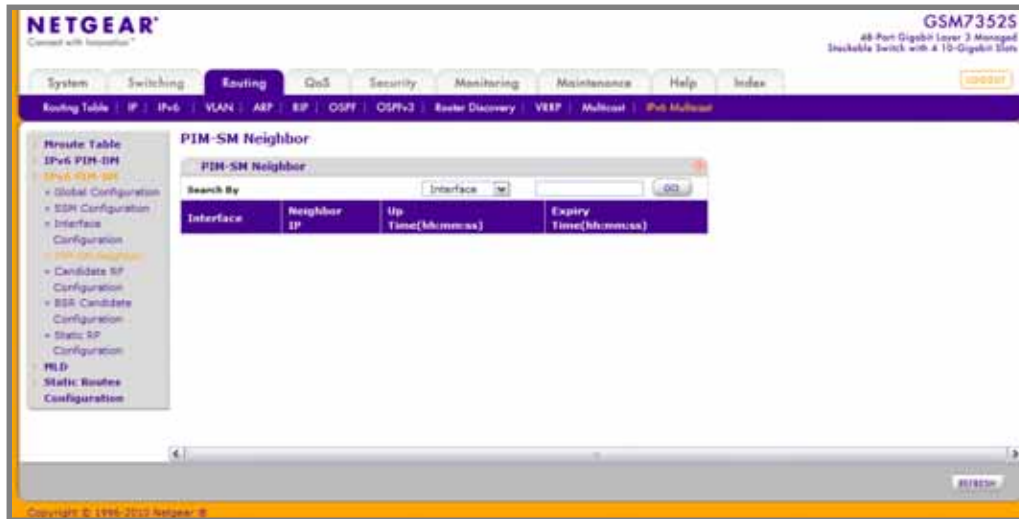
**Table 73.**

Field	Description
Protocol State	The state of PIM-SM in the router: either operational or non-operational.
IPv6 Prefix/Length	The IPv6 Address Prefix and the Length of the selected interface.
Designated Router	The Designated Router on the selected PIM interface.
Neighbor Count	The number of PIM neighbors on the selected interface.



## PIM-SM Neighbor

To display the IPv6 PIM-SM Neighbor page, click **Routing** > **IPv6 Multicast** > **PIM-SM** > **PIM-SM Neighbor**.



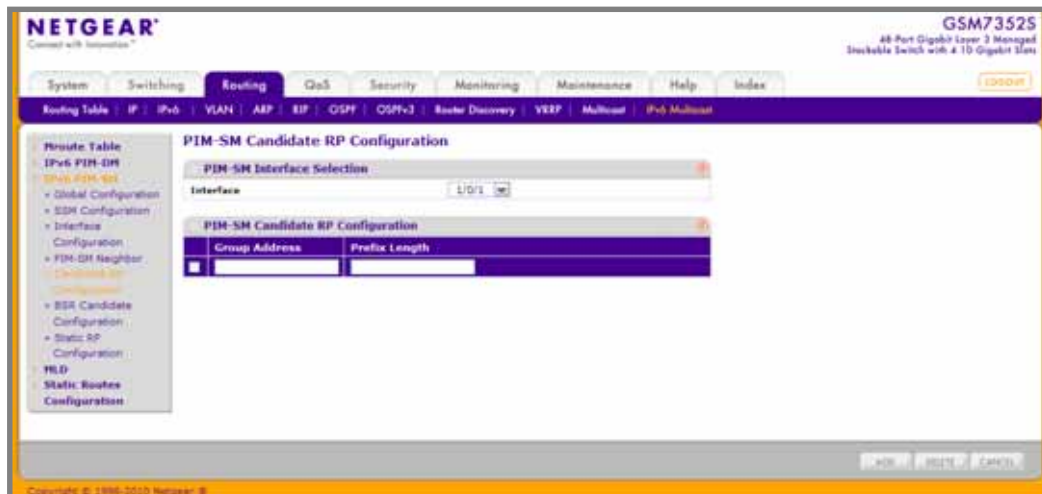
**Table 74.**

Field	Description
Interface	The interface on which neighbor is displayed.
Neighbor IP	The IP address of the PIM neighbor for this entry.
Up Time	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time	The minimum time remaining before this PIM neighbor will be aged out.

Click **REFRESH** to refresh the data on the screen with latest PIM-SM neighbor information.

## PIM-SM Candidate RP Configuration

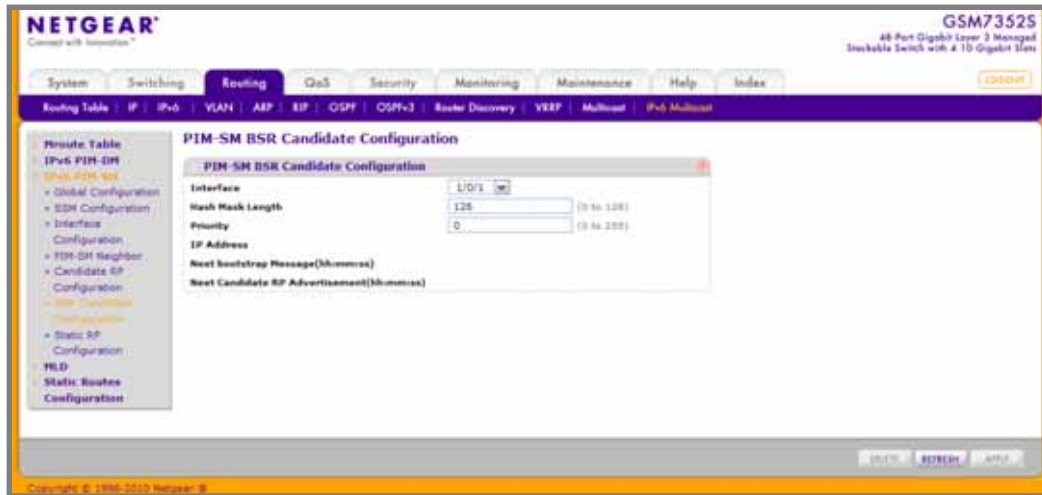
To display the IPv6 PIM-SM Candidate RP Configuration page, click **Routing > IPv6 Multicast > PIM-SM > Candidate RP Configuration**.



1. Use **Interface** to select the interface for which data is to be displayed.
2. Use **Group Address** to specify the group IPv6 address prefix transmitted in Candidate-RP-Advertisements.
3. Use **Prefix Length** to specify the group IPv6 Prefix Length transmitted in Candidate-RP-Advertisements.
4. Click **ADD** to add a new Candidate RP Address for the PIM-SM router.
5. Click **DELETE** to delete an extant Candidate RP Address for the PIM-SM router.

## PIM-SM BSR Candidate Configuration

To display the IPv6 PIM-SM BSR Candidate Configuration page, click **Routing > IPv6 Multicast > PIM-SM > BSR Candidate Configuration**.



1. Use **Interface** to select the interface for which data is to be configured.
2. Use **Priority** to enter the priority of C-BSR.
3. Use **Hash Mask Length** to enter the C-BSR hash mask length to be advertised in bootstrap messages. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid values are from 0 to 128. Default value is 126.

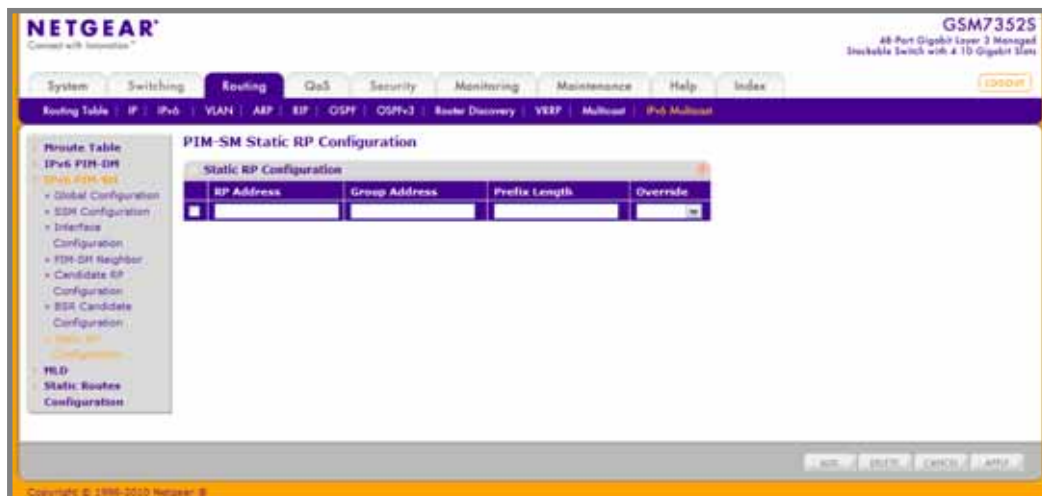
**Table 75.**

Field	Description
IP Address	Displays the IP address of the Elected BSR.
Next bootstrap Message	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP Advertisement	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

## PIM-SM Static RP Configuration

This page is used to statically configure the RP address for one or more multicast groups.

To display the IPv6 PIM-SM Static RP Configuration page, click **Routing** > **IPv6 Multicast** > **PIM-SM** > **Static RP Configuration**.



1. Use **RP Address** to specify the IP Address of the RP to be created or deleted.
2. Use **Group Address** to specify the Group Address of the RP to be created or deleted.
3. Use **Prefix Length** to specify the Group IPv6 Prefix Length of the RP to be created or deleted.
4. Use **Override** to indicate that if there is a conflict, the RP configured with this option prevails over the RP learned by BSR.
5. Click **ADD** to add a new static RP address for one or more multicast groups.
6. Click **DELETE** to delete the RP address selected.

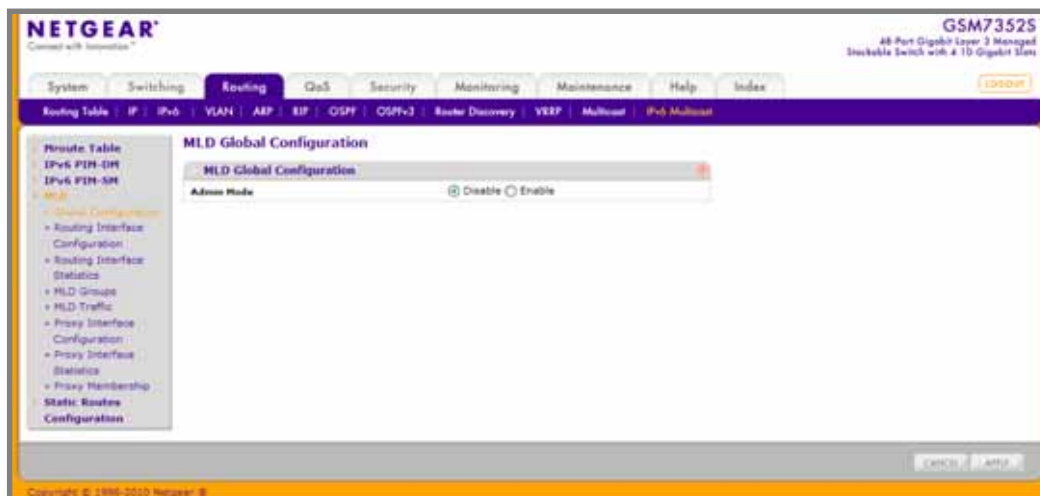
## MLD

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

- [MLD Global Configuration](#) on page 385
- [MLD Routing Interface Configuration](#) on page 386
- [MLD Routing Interface Statistics](#) on page 388
- [MLD Groups](#) on page 389
- [MLD Traffic](#) on page 390
- [MLD Proxy Interface Configuration](#) on page 392
- [MLD Proxy Interface Statistics](#) on page 394
- [MLD Proxy Membership](#) on page 395

### MLD Global Configuration

To display the MLD Global Configuration page, click **Routing > IPv6 Multicast > MLD > Global Configuration**.



1. Use **Admin Mode** to set the administrative status of MLD in the router to active or inactive. The default is disable.

## MLD Routing Interface Configuration

To display the MLD Routing Interface Configuration page, click **Routing > IPv6 Multicast > MLD > Routing Interface Configuration**.

MLD Routing Interface Configuration

MLD Routing Interface Configuration

Go To Interface

AR

Interface	Admin Mode	Operational Mode	Version	Redundancy	Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval	Last Member
<input type="checkbox"/> 1/0/1	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/2	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/3	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/4	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/5	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/6	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/7	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/8	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/9	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/10	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/11	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/12	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/13	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/14	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/15	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/16	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/17	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/18	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/19	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/20	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/21	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/22	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/23	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/24	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/25	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/26	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/27	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/28	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/29	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/30	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/31	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/32	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/33	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/34	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/35	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/36	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/37	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/38	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/39	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/40	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/41	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/42	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/43	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/44	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/45	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/46	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/47	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/48	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/49	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/50	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/51	Disable	Not In Service	V2	2	125	10000	31	2	1000	2
<input type="checkbox"/> 1/0/52	Disable	Not In Service	V2	2	125	10000	31	2	1000	2

AR

Go To Interface

1. Use **Interface** to select the interface for which data is to be configured or displayed.
2. Use **Admin Mode** to set the administrative status of MLD on the selected interface. The default value is disable.
3. Use **Version** to enter the version to be configured on the selected interface. Valid values are (1 to 2). The default value is 2.
4. Use **Query Interval** to enter the frequency in seconds at which MLD host-query packets are to be transmitted on this interface. Valid values are from 1 to 1800. The default value is 125.
5. Use **Query Max Response Time** to enter the maximum query response time to be advertised in MLDv2 queries on this interface, in milliseconds. Valid values are from 0 to 65535. The default value is 10000 milliseconds.
6. Use **Robustness** to specify the robustness parameter for the selected interface. This variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness variable may be increased. MLD is robust to (robustness variable-1) packet losses.
7. Use **Startup Query Interval** to specify the value that indicates the configured interval (in seconds) between General Queries sent by a Querier on startup.
8. Use **Startup Query Count** to specify the value that indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval.
9. Use **Last Member Query Interval** to enter the last member query interval in milliseconds. This is the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 65535. The default value is 1000 milliseconds.
10. Use **Last Member Query Count** to enter the number of queries to be sent on receiving a leave group report. Valid values are from 1 to 20. The default value is 2.

Table 76.

Field	Description
Operational Mode	The operational status of MLD on the Interface.

## MLD Routing Interface Statistics

To display the MLD Routing Interface Statistics page, click **Routing > IPv6 Multicast > MLD > Routing Interface Statistics**.

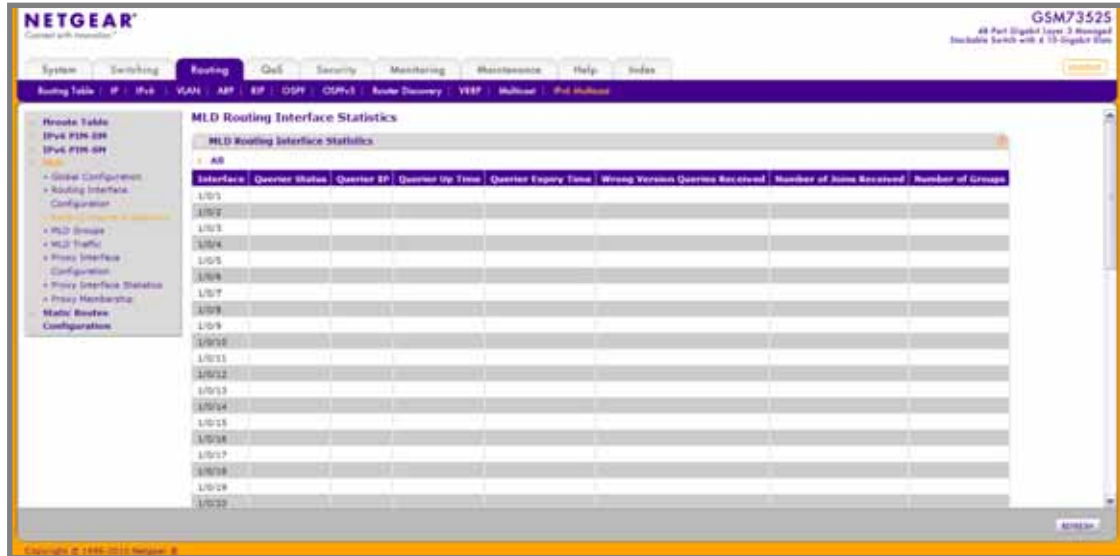


Table 77.

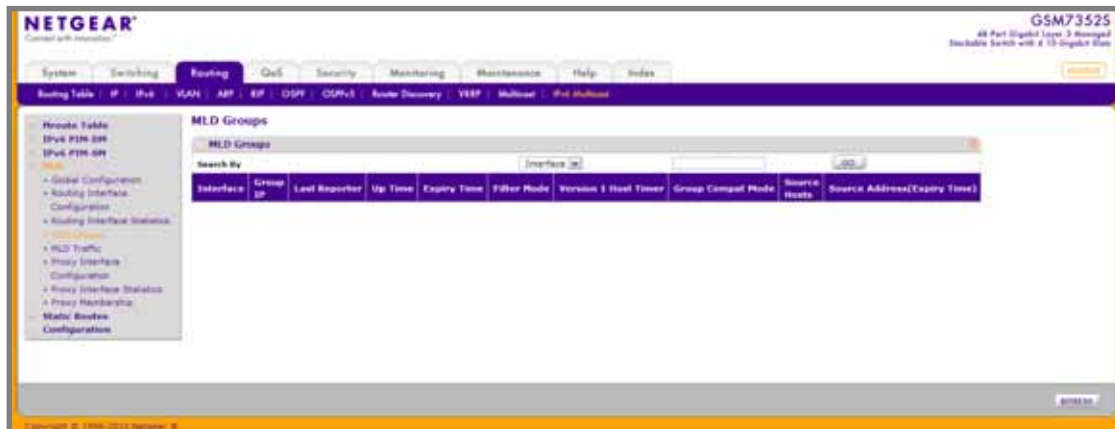
Field	Description
Interface	The interface for which data is to be displayed.
Querier Status	This value indicates whether the interface is a MLD querier or non-querier on the subnet it is associated with.
Querier IP	The address of the MLD querier on the IP subnet to which the selected interface is attached.
Querier Up Time	The time in seconds since the MLD interface querier was last changed.
Querier Expiry Time	The time in seconds remaining before the other querier present timer expires. If the local system is the querier, this will be zero.
Wrong Version Queries Received	Indicates the number of queries received whose MLD version does not match the MLD version of the interface.
Number of Joins Received	The number of times a group membership has been added on this interface.
Number of Groups	The current number of membership entries for the selected interface in the cache table.



Click **REFRESH** to refresh the data on the screen with the latest MLD routing interface statistics.

## MLD Groups

To display the MLD Groups page, click **Routing > IPv6 Multicast > MLD > MLD Groups**.



**Table 78.**

Field	Description
Interface	Indicates the interface on which data is displayed.
Group IP	Indicates the address of the Mgmnd members.
Last Reporter	The IP Address of the source of the last membership report received for this multicast group address on the interface.
Up Time	Time elapsed in seconds since the multicast group has been known.
Expiry Time	Time left in seconds before the entry is removed from the MLD membership table of this interface.
Filter Mode	The filter mode of the multicast group on this interface. The values it can take are INCLUDE and EXCLUDE.
Version1 Host Timer	The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.
Group Compat Mode	The compatibility mode of the multicast group on the interface. The values it can take are MLDv1 and MLDv2.

Table 78.

Field	Description
Source Hosts	This parameter shows source addresses which are members of this multicast address.
Source Address(Expiry Time)	This parameter shows expiry time interval against each source address which are members of this multicast group. This is the amount of time after which the specified source entry is aged out.

Click **REFRESH** to refresh the data on the screen with latest MLD groups information.

### MLD Traffic

To display the MLD Traffic page, click **Routing > IPv6 Multicast > MLD > MLD Traffic**.

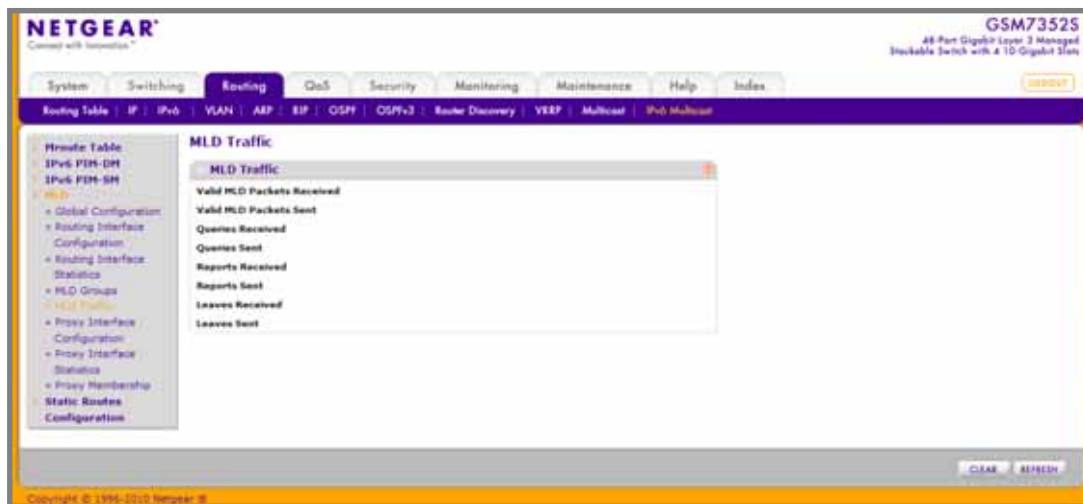


Table 79.

Field	Description
Valid MLD Packets Received	The number of valid MLD packets received by the router.
Valid MLD Packets Sent	The number of valid MLD packets sent by the router.
Queries Received	The number of valid MLD queries received by the router.
Queries Sent	The number of valid MLD queries sent by the router.
Reports Received	The number of valid MLD reports received by the router.
Reports Sent	The number of valid MLD reports sent by the router.

**Table 79.**

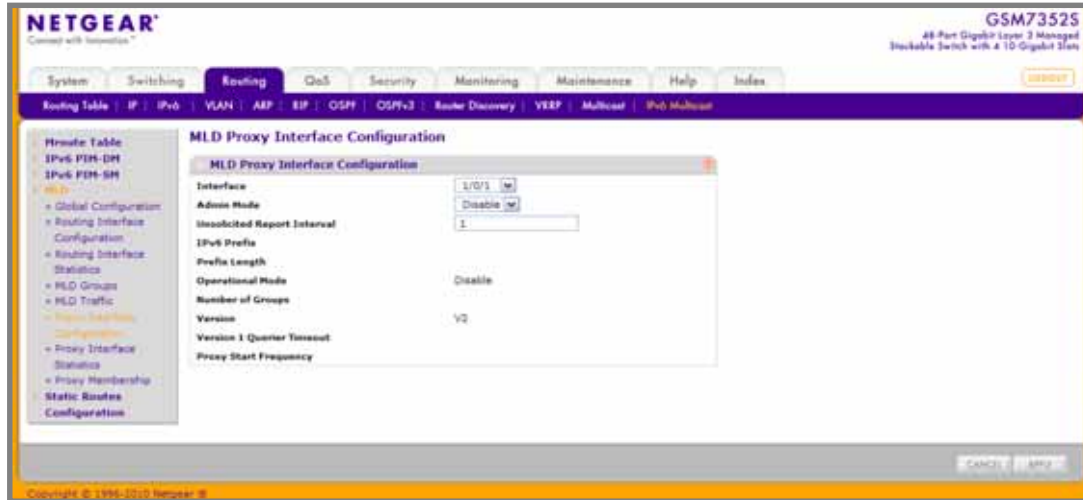
Field	Description
Leaves Received	The number of valid MLD leaves received by the router.
Leaves Sent	The number of valid MLD leaves sent by the router.

Click **REFRESH** to refresh the data on the screen with the latest MLD traffic.

Click **CLEAR** to clear all the MLD traffic.

## MLD Proxy Interface Configuration

To display the MLD Proxy Interface Configuration page, click **Routing > IPv6 Multicast > MLD > Proxy Interface Configuration**.



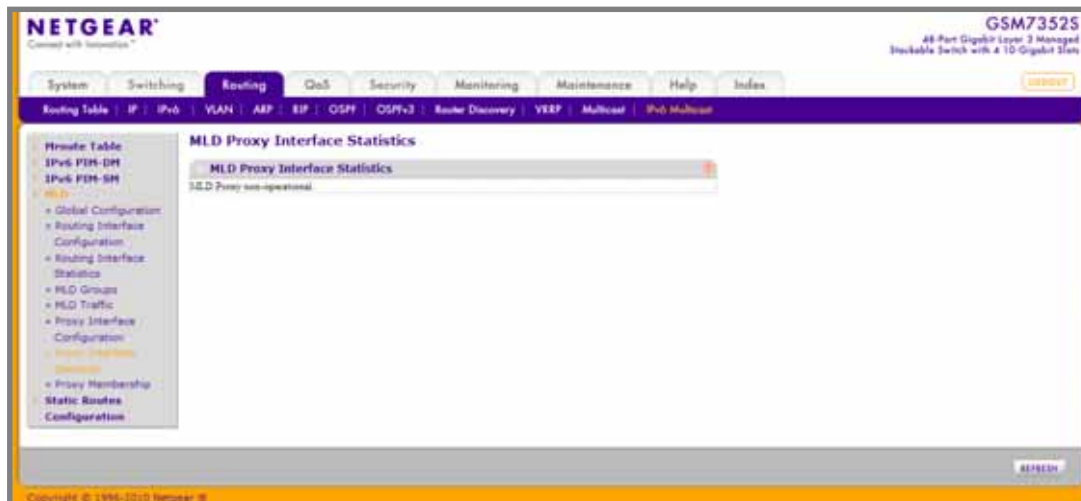
1. Use **Interface** to select the interface to be configured.
2. Use **Admin Mode** to set the administrative status of MLD Proxy on the selected interface. The default is disable. Routing, MLD and Multicast global admin modes should be enabled to enable MLD Proxy interface mode.
3. Use **Version** to enter the version of MLD you want to configure on the selected interface. Valid values are 1 to 2 and the default value is 3. This field is configurable only when MLD Proxy interface mode is enabled.
4. Use **Unsolicited Report Interval** to enter the unsolicited time interval value in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Valid values are from 1 to 260. The default value is 1.

**Table 80.**

Field	Description
IPv6 Prefix	The IPv6 address of the MLD Proxy interface.
Prefix Length	The prefix length for the IPv6 address of the MLD Proxy interface.
Operational Mode	The operational state of MLD Proxy interface.
Number of Groups	The current number of multicast group entries for the MLD Proxy interface in the cache table.
Version 1 Querier Timeout	The older MLD version 1 querier timeout value in seconds. The Older Version Querier Interval is the time-out for transitioning a host back to MLDv2 mode once an older version query is heard. When an older version query is received, hosts set their Older Version Querier Present Timer to Older Version Querier Interval.
Proxy Start Frequency	The number of times the proxy was brought up.

## MLD Proxy Interface Statistics

To display the MLD Proxy Interface Statistics page, click **Routing > IPv6 Multicast > MLD > Proxy Interface Statistics**.



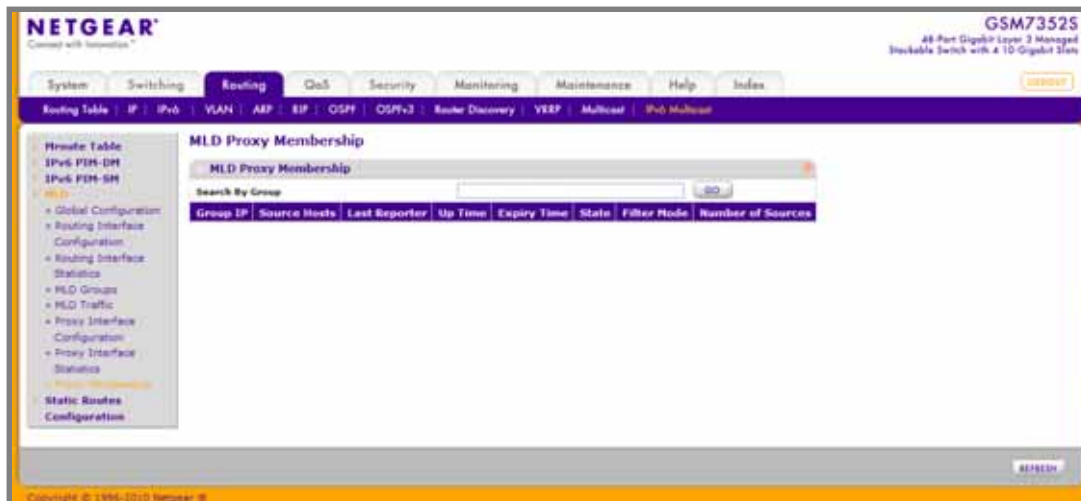
**Table 81.**

Field	Description
Proxy Interface	Displays the interface on which MLD Proxy packets received.
Version	The version of MLD Proxy packets received.
Queries Received	The number of MLD Proxy queries received.
Report Received	The number of MLD Proxy reports received.
Reports Sent	The number of MLD Proxy reports sent.
Leaves Received	The number of MLD Proxy leaves received.
Leaves Sent	The number of MLD Proxy leaves sent.

Click **REFRESH** to refresh the data on the screen with the latest MLD Proxy interface statistics.

## MLD Proxy Membership

To display the MLD Proxy Membership page, click **Routing** > **IPv6 Multicast** > **MLD** > **Proxy Membership**.



**Table 82.**

Field	Description
Group IP	The IPv6 multicast group address.
Source Hosts	This parameter shows source addresses which are members of this multicast address.
Last Reporter	The IPv6 address of the source of the last membership report received for the IPv6 Multicast group address on the MLD Proxy interface.
Up Time	The time elapsed since this entry was created.
Expiry Time	This parameter shows expiry time interval against each source address which is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.
State	The state of the host entry. A Host can be in one of the state. Non-member state - does not belong to the group on the interface. Delaying member state - host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. Idle member state - host belongs to the group on the interface and no report timer running.
Filter Mode	The group filter mode (Include/Exclude/None) for the specified group on the MLD Proxy interface.
Number of Sources	The number of source hosts present in the selected multicast group.

Click **REFRESH** to refresh the data on the screen with the latest MLD proxy membership information.



## Static Routes Configuration

To display the Static Routes Configuration page, click **Routing > IPv6 Multicast > Static Routes Configuration**.

The screenshot shows the Netgear web interface for a GSM7352S switch. The 'Routing' tab is selected, and the 'Static Routes Configuration' page is displayed. A table for configuring static routes is shown with the following columns: Source IP, Prefix Length, RPF Neighbor, Metric, and RPF Interface. The table is currently empty. At the bottom right, there are buttons for ADD, DELETE, CANCEL, and APPLY.

1. Use **Source IP** to enter the IP Address that identifies the multicast packet source for the entry you are creating.
2. Use **Prefix Length** to enter the Prefix Length to be applied to the Source IPv6 address.
3. Use **RPF Neighbor** to enter the IP address of the neighbor router on the path to the source.
4. Use **Metric** to enter the link state cost of the path to the multicast source. The range is 0 - 255 and the default is 1. You can change the metric for a configured route by selecting the static route and editing this field.
5. Use **RPF Interface** to select the interface number from the drop-down menu. This is the interface that connects to the neighbor router for the given source IP address.
6. Click **ADD** to add a new static route to the switch.
7. Click **DELETE** to delete the multicast static routes selected.

# 5 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 398
- [Differentiated Services](#) on page 407

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.

Eight queues per port are supported.

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

- [Basic](#) on page 399
- [Advanced](#) on page 401

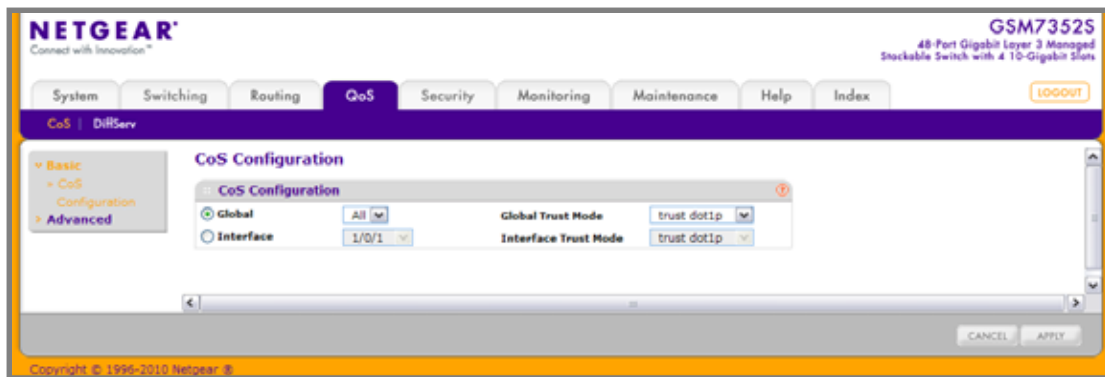
## Basic

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

- [CoS Configuration](#) on page 399

### CoS Configuration

To display the CoS Configuration page, click **QoS** > **CoS** > **Basic** > **CoS Configuration**.



Use the CoS 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 configure global CoS settings:

1. Use **Global** to specify all CoS configurable interfaces. The option "Global" represents the most recent global configuration settings.
2. Use **Interface** to specify CoS configuration settings based per-interface.
3. Use **Global Trust Mode** to specify whether to trust a particular packet marking at ingress. Global Trust Mode can only be one of the following. Default value is trust dot1p.
  - untrusted
  - trust dot1p
  - trust ip-dscp
4. Use **Interface Trust Mode** to specify whether to trust a particular packet marking at ingress. Interface Trust Mode can only be one of the following. Default value is untrusted.
  - untrusted
  - trust dot1p
  - trust ip-dscp
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.

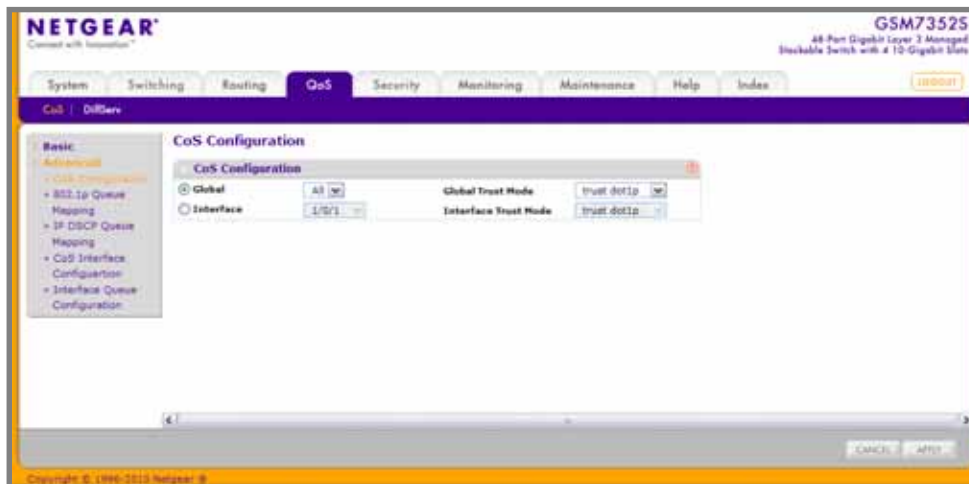
## Advanced

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

- [CoS Configuration](#) on page 401
- [802.1p to Queue Mapping](#) on page 402 (Advanced)
- [IP DSCP to Queue Mapping](#) on page 403 (Advanced)
- [CoS Interface Configuration](#) on page 404 (Advanced)
- [Interface Queue Configuration](#) on page 406 (Advanced)

## CoS Configuration

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



1. Use **Global** to specify all CoS configurable interfaces. The option “Global” represents the most recent global configuration settings.
2. Use **Interface** to specify CoS configuration settings based per-interface.
3. Use **Global Trust Mode** to specify whether to trust a particular packet marking at ingress. Global Trust Mode can only be one of the following. Default value is trust dot1p.
  - untrusted
  - trust dot1p
  - trust ip-dscp
4. Use **Interface Trust Mode** to specify whether to trust a particular packet marking at ingress. Interface Trust Mode can only be one of the following. Default value is untrusted.
  - untrusted
  - trust dot1p
  - trust ip-dscp

## 802.1p to Queue Mapping

The 802.1p to Queue Mapping page also displays the Current 802.1p Priority Mapping table.

To display the 802.1p to Queue Mapping page, click **QoS** > **CoS** > **Advanced** > **802.1p to Queue Mapping**.

The screenshot shows the Netgear web interface for a GSM7352S switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The QoS section is expanded, showing CoS and DiffServ. The 802.1p to Queue Mapping page is displayed, featuring an 'Interface Selection' dropdown set to '1/0/1'. Below this is a table titled '802.1p to Queue Mapping' with columns for 802.1p Priority (0-7) and Queue (1-3). The table shows the current mapping for each priority.

802.1p Priority	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

At the bottom of the page, there are 'CANCEL' and 'APPLY' buttons.

To map 802.1p priorities to queues:

1. Use **Interface** to specify CoS configuration settings based per-interface or specify all CoS configurable interfaces.
2. Specify which internal traffic class to map the corresponding 802.1p value. The queue number depends on the specific hardware.

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 (3). 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 3, 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.

## IP DSCP to Queue Mapping

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

To display the IP DSCP Queue Mapping page, click **QoS** > **CoS** > **Advanced** > **IP DSCP to Queue Mapping**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

CoS | DiffServ

> Basic  
▼ Advanced  
    > CoS Configuration  
    > 802.1p Queue Mapping  
    > IP DSCP Queue Mapping  
    > CoS Interface Configuration  
    > Interface Queue Configuration

**IP DSCP to Queue Mapping**

Interface Selection  
Interface: 1/0/1

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

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

To map DSCP values to queues:

1. Use **Interface** to specify CoS configuration settings based per-interface or specify all CoS configurable interfaces.
2. The **IP DSCP** field displays an IP DSCP value from 0 to 63.
3. For each DSCP value, specify which internal traffic class to map the corresponding IP DSCP value. The queue number depends on specific hardware.
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.

## 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 **QoS > CoS > Advanced > CoS Interface Configuration**.

**NETGEAR**  
Connected with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

CoS | DiffServ

Basic  
Advanced  
CoS Configuration  
802.1p Queue Mapping  
IP DSCP Queue Mapping  
**CoS Interface Configuration**  
Interface Queue Configuration

### CoS Interface Configuration

1 All Go To Interface  GO

Interface	Interface Trust Mode	Interface Shaping Rate
<input type="checkbox"/> 1/0/1	802.1p	0
<input type="checkbox"/> 1/0/2	802.1p	0
<input type="checkbox"/> 1/0/3	802.1p	0
<input type="checkbox"/> 1/0/4	802.1p	0
<input type="checkbox"/> 1/0/5	802.1p	0
<input type="checkbox"/> 1/0/6	802.1p	0
<input type="checkbox"/> 1/0/7	802.1p	0
<input type="checkbox"/> 1/0/8	802.1p	0
<input type="checkbox"/> 1/0/9	802.1p	0
<input type="checkbox"/> 1/0/10	802.1p	0
<input type="checkbox"/> 1/0/11	802.1p	0
<input type="checkbox"/> 1/0/12	802.1p	0
<input type="checkbox"/> 1/0/13	802.1p	0
<input type="checkbox"/> 1/0/14	802.1p	0
<input type="checkbox"/> 1/0/15	802.1p	0
<input type="checkbox"/> 1/0/16	802.1p	0
<input type="checkbox"/> 1/0/17	802.1p	0
<input type="checkbox"/> 1/0/18	802.1p	0
<input type="checkbox"/> 1/0/19	802.1p	0
<input type="checkbox"/> 1/0/20	802.1p	0
<input type="checkbox"/> 1/0/21	802.1p	0
<input type="checkbox"/> 1/0/22	802.1p	0
<input type="checkbox"/> 1/0/23	802.1p	0

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.



To configure CoS settings for an interface:

1. Use **Interface** to specify all CoS configurable interfaces.
2. Use **Interface Trust Mode** to specify whether to trust a particular packet marking at ingress. Interface Trust Mode can only be one of the following. Default value is trust dot1p.
  - untrusted
  - trust dot1p
  - trust ip-dscp
3. Use **Interface Shaping Rate** to specify the maximum bandwidth allowed, typically used to shape the outbound transmission rate. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. Default value is 0. Valid Range is 0 to 100 in increments of 1. The value 0 means maximum is unlimited.
4. Click **CANCEL** to cancel the configuration on the screen. Resets the data on the screen to the latest value of the switch.
5. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

## 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 > Advanced > Interface Queue Configuration**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

CoS | DiffServ

> Basic  
 > Advanced  
 > CoS Configuration  
 > 802.1p Queue Mapping  
 > IP DSCP Queue Mapping  
 > CoS Interface Configuration  
 > Interface Queue Configuration

### Interface Queue Configuration

1 All Go To Interface  GO

Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
<input type="checkbox"/> 1/0/1	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/2	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/3	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/4	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/5	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/6	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/7	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/8	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/9	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/10	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/11	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/12	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/13	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/14	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/15	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/16	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/17	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/18	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/19	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/20	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/21	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/22	0	0	Weighted	TailDrop

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

To configure CoS queue settings for an interface:

1. 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.
2. Configure any of the following settings:
  - **Queue ID** - Use the menu to select the queue to be configured (platform based).
  - Use **Minimum Bandwidth** to specify the minimum guaranteed bandwidth allotted to this queue. Setting this value higher than its corresponding Maximum Bandwidth automatically increases the maximum to the same value. Default value is 0. Valid Range is 0 to 100 in increments of 1. The value 0 means no guaranteed minimum. Sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum (100).
  - Use **Scheduler Type** to specify the type of scheduling used for this queue. 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.
3. **Queue Management Type** displays the Queue depth management technique used for queues on this interface. This is only used if device supports independent settings per-queue. Queue Management Type can only be taildrop. All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.
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.

## 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.

From the DiffServ link under the QoS tab, you can access the following pages:

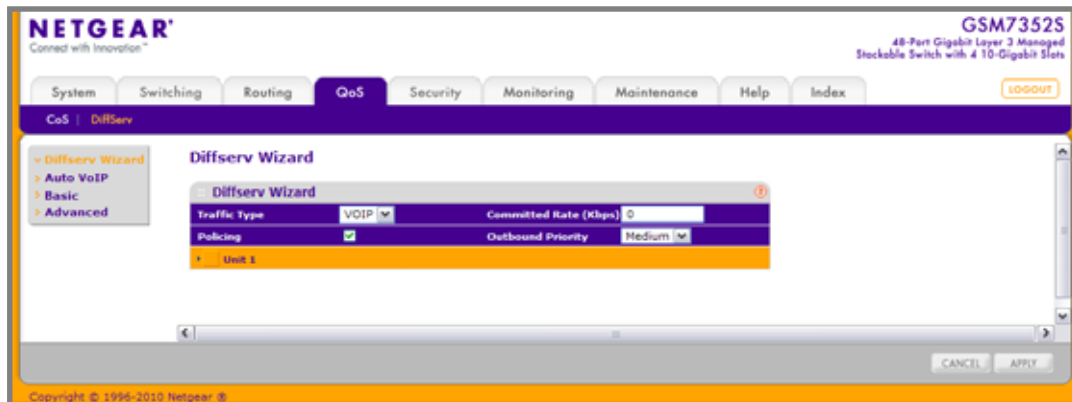
- [\*DiffServ Wizard\*](#) on page 409
- [\*Auto VoIP Configuration\*](#) on page 411
- [\*Basic\*](#) on page 412
- [\*Advanced\*](#) on page 414

## DiffServ Wizard

The DiffServ Wizard enables DiffServ on the switch by creating a traffic class, adding the traffic class to a policy, and then adding the policy to the ports selected on DiffServ Wizard page. The DiffServ Wizard will:

- Create a **DiffServ Class** and define match criteria used as a filter to determine if incoming traffic meets the requirements to be a member of the class.
- Set the **DiffServ Class** match criteria based on **Traffic Type** selection as below:
  - **VOIP** - sets match criteria to UDP protocol.
  - **HTTP** - sets match criteria to HTTP destination port.
  - **FTP** - sets match criteria to FTP destination port.
  - **Telnet** - sets match criteria to Telnet destination port.
  - **Every** - sets match criteria all traffic.
- Create a **Diffserv Policy** and add it to the **DiffServ Class** created.
- If **Policing** is set to **YES**, then **DiffServ Policy** style is set to **Simple**. Traffic which conforms to the **Class Match** criteria will be processed according to the **Outbound Priority** selection. **Outbound Priority** configures the handling of conforming traffic as below:
  - **High** - sets policing action to markdscp ef.
  - **Med** - sets policing action to markdscp af31.
  - **Low** - sets policing action to send.
- If **Policing** is set to **NO**, then all traffic will be marked as specified below:
  - **High** - sets policy mark ipdscp ef.
  - **Med** - sets policy mark ipdscp af31.
  - **Low** - sets policy mark ipdscp be.
- Each port selected will be added to the policy created.

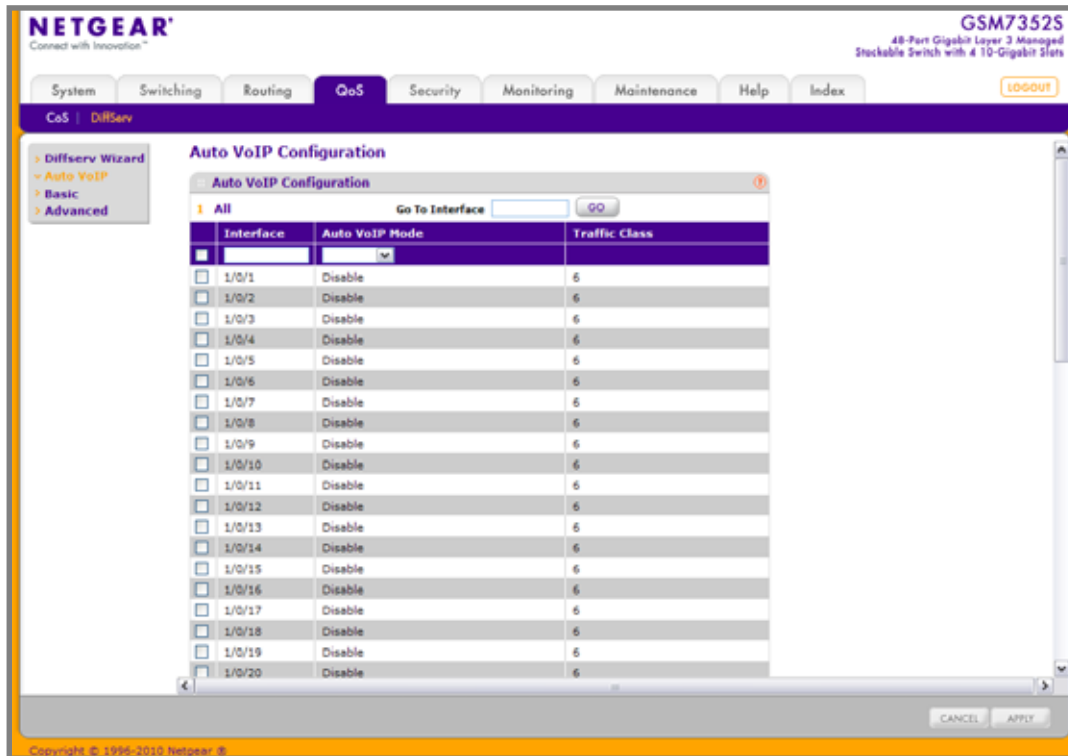
To display the DiffServ Wizard page, click **QoS > DiffServ > DiffServ Wizard**.



1. Use **Traffic Type** to define the **DiffServ Class**. Traffic type options: **VOIP**, **HTTP**, **FTP**, **Telnet**, and **Every**.
2. Ports displays the ports which can be configured to support a **DiffServ policy**. The **DiffServ policy** will be added to selected ports.
3. Use **Enable Policing** to add policing to the **DiffServ Policy**. The policing rate will be applied.
4. Committed Rate:
  - When **Policing** is enabled, the committed rate will be applied to the policy and the policing action is set to conform.
  - When **Policing** is disabled, the committed rate is not applied and the policy is set to markdscp.
5. Outbound Priority:
  - When **Policing** is enabled, **Outbound Priority** defines the type of policing conform action where: **High** sets action to markdscp ef, **Med** sets action to markdscp af31, and **Low** sets action to send.
  - When **Policing** is disabled, **Outbound Priority** defines the policy where: **High** sets policy to mark ipdscp ef, **Med** sets policy to mark ipdscp af31, **Low** set policy to mark ipdscp be.

## Auto VoIP Configuration

To display the Auto VoIP Configuration page, click **QoS > DiffServ > Auto VoIP**.



1. **Interface** - Specifies the Auto VoIP configurable interfaces.
2. Use **Auto VoIP Mode** to enable or disable the Auto VoIP mode. Auto VoIP Mode can only be one of the following:
  - Enable
  - Disable (Default)

Table 5-74.

Field	Description
Traffic Class	Displays the Traffic Class used for VoIP traffic.

## Basic

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

- [DiffServ Configuration](#) on page 412

### DiffServ Configuration

Packets are filtered and processed based on defined criteria. The filtering 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.

The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.

Packet processing begins by testing the match criteria for a packet. The 'all' class type option defines that each match criteria within a class must evaluate to true for a packet to match that class. The 'any' class type option defines that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

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

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

CaS | DiffServ

Diffserv Wizard  
Auto VoIP  
Basic  
DiffServ Configuration  
Advanced

### Diffserv Configuration

**Diffserv Config**

DiffServ Admin Mode ☐ Disable ☒ Enable

**Status**

MIB Table	Current Size	Max Size
Class Table	0	32
Class Rule table	0	192
Policy table	0	64
Policy Instance table	0	768
Policy Attributes table	0	2304
Service table	0	400

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.



Table 5-75.

Field	Description
DiffServ Admin Mode	The options mode for DiffServ. The default value is 'enable'. While disabled, the DiffServ configuration is retained when saved and can be changed, but it is not activated. When enabled, Diffserv services are activated.
Class table	Displays the number of configured DiffServ classes out of the total allowed on the switch.
Class Rule table	Displays the number of configured class rules out of the total allowed on the switch.
Policy table	Displays the number of configured policies out of the total allowed on the switch.
Policy Instance table	Displays the number of configured policy class instances out of the total allowed on the switch.
Policy Attributes table	Displays the number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
Service table	Displays the number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

## Advanced

- [Diffserv Configuration](#) on page 414
- [Class Configuration](#) on page 416
- [Policy Configuration](#) on page 420
- [Service Interface Configuration](#) on page 424
- [Service Statistics](#) on page 425

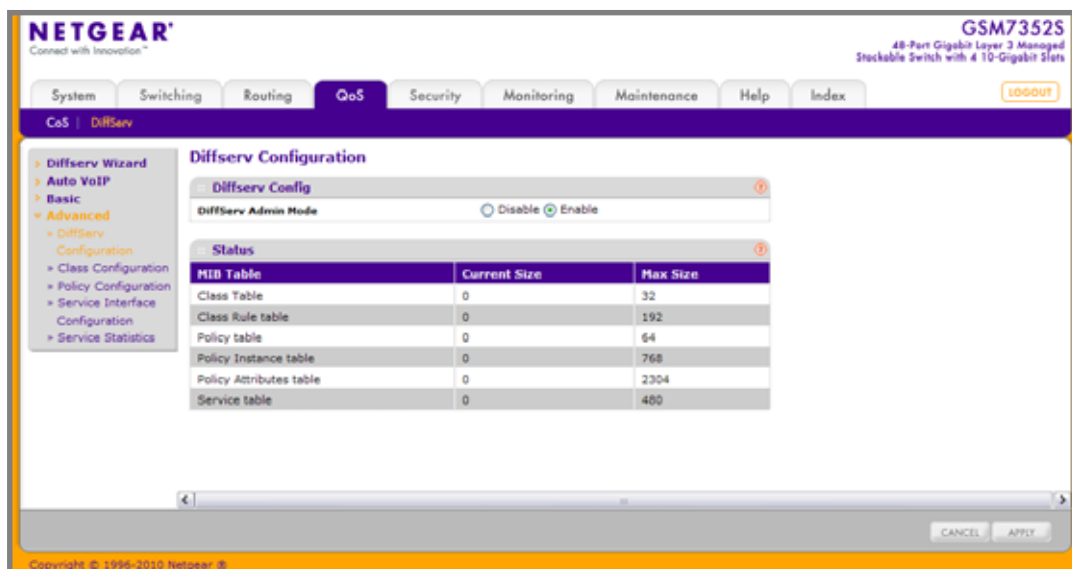
### Diffserv Configuration

Packets are filtered and processed based on defined criteria. The filtering 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.

The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.

Packet processing begins by testing the match criteria for a packet. The 'all' class type option defines that each match criteria within a class must evaluate to true for a packet to match that class. The 'any' class type option defines that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

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



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:

Table 5-76.

Field	Description
<b>Class table</b>	Displays the number of configured DiffServ classes out of the total allowed on the switch.
<b>Class Rule table</b>	Displays the number of configured class rules out of the total allowed on the switch.
<b>Policy table</b>	Displays the number of configured policies out of the total allowed on the switch.
<b>Policy Instance table</b>	Displays the number of configured policy class instances out of the total allowed on the switch.
<b>Policy Attributes table</b>	Displays the number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
<b>Service table</b>	Displays the number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

## 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:

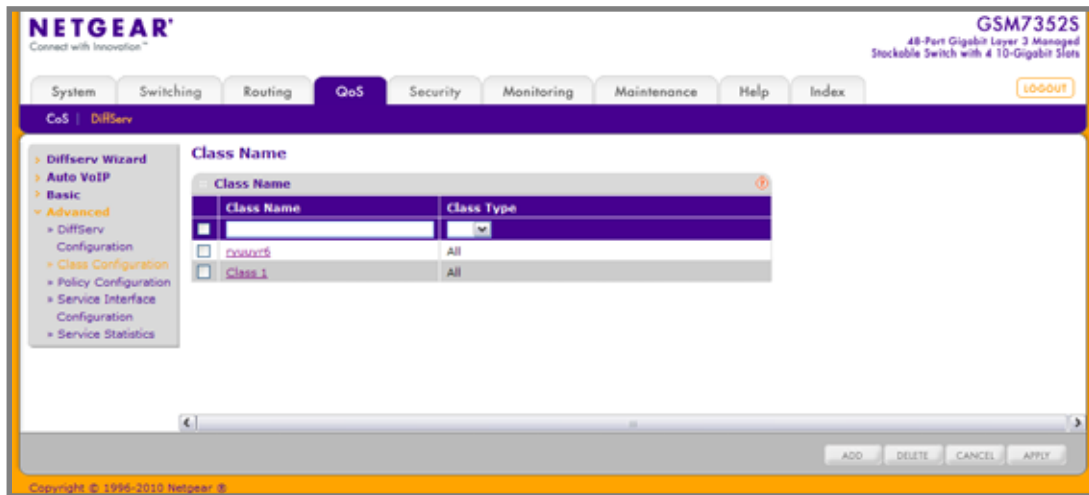
1. To create a new class, enter a **class name**, select the **class type**, and click **Add**. This field also lists all the existing DiffServ class names, from which one can be selected.

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. Only when a new class is created, this field is a selector field. After class creation this becomes a non-configurable field displaying the configured class type.

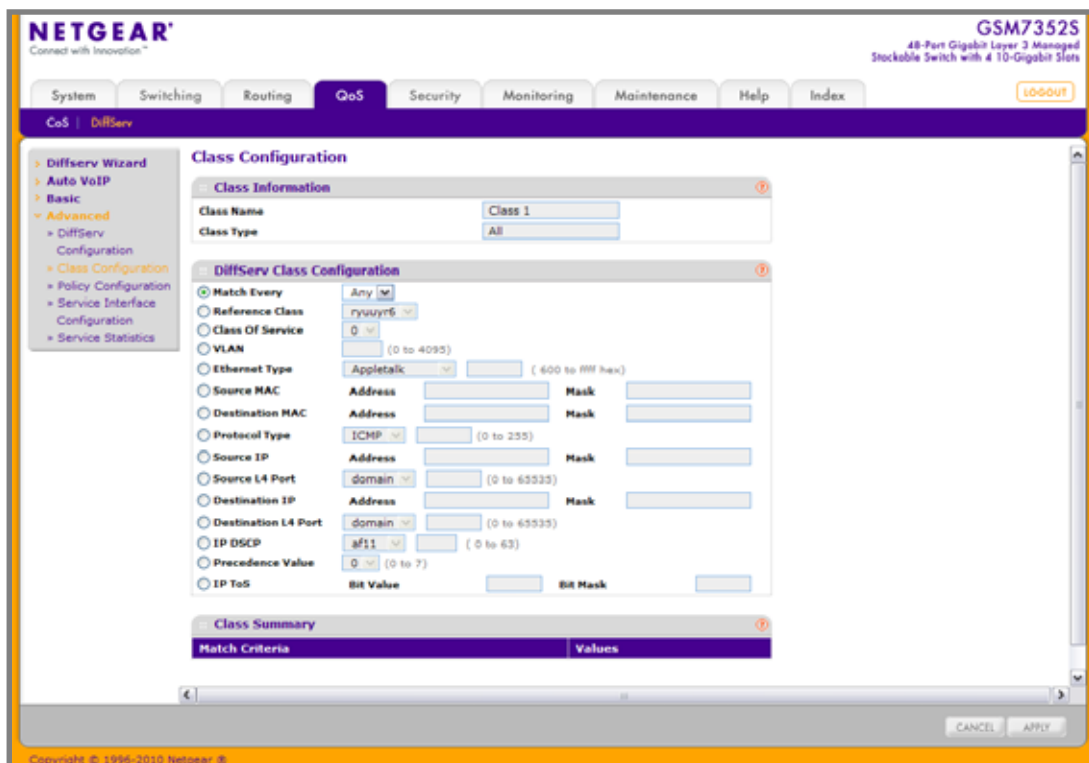
2. To rename an existing class, select the check box next to the configured class, update the name, and click **Apply**.
3. To remove a class, click the check box beside the Class Name, then click **Delete**.
4. Click **Refresh** to refresh the page with the most current data from the switch.
5. Click **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. **Class Name** - Displays the name for the configured DiffServ class.
3. **Class Type** - Displays the DiffServ class type. Options:

- All

Only when a new class is created, this field is a selector field. After class creation this becomes a non-configurable field displaying the configured class type.

4. 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.
  - **Reference Class** - This lists the class(es) that can be assigned as reference class(es) to the current class.
  - **Class of Service** - This lists all the values for the class of service match criterion in the range 0 to 7 from which one can be selected.
  - **VLAN** - This is a value in the range of 0-4095.
  - **Ethernet Type** - This lists the keywords for the Ethertype from which one can be selected.
  - **Source MAC Address** - This is the source MAC address specified as six, two-digit hexadecimal numbers separated by colons.
  - **Source MAC Mask** - This is a bit mask in the same format as MAC Address indicating which part(s) of the source MAC Address to use for matching against packet content.
  - **Destination MAC Address** - This is the destination MAC address specified as six, two-digit hexadecimal numbers separated by colons.
  - **Destination MAC Mask** - This is a bit mask in the same format as MAC Address indicating which part(s) of the destination MAC Address to use for matching against packet content.
  - **Protocol Type** - This lists the keywords for the layer 4 protocols from which one can be selected. The list includes 'other' as an option for the remaining values.
  - **Source IP Address** - This is a valid source IP address in the dotted decimal format.
  - **Source Mask** - This is a bit mask in IP dotted decimal format indicating which part(s) of the source IP Address to use for matching against packet content.
  - **Source L4 Port** - This lists the keywords for the known source layer 4 ports from which one can be selected. The list includes 'other' as an option for the unnamed ports.
  - **Destination IP Address** - This is a valid destination IP address in the dotted decimal format.
  - **DestinationMask** - This is a bit mask in IP dotted decimal format indicating which part(s) of the destination IP Address to use for matching against packet content.
  - **Destination L4 Port** - This lists the keywords for the known destination layer 4 ports from which one can be selected. The list includes 'other' as an option for the unnamed ports.
  - **IP DSCP** - This lists the keywords for the known DSCP values from which one can be selected. The list includes 'other' as an option for the remaining values.

- **Precedence Value** -This lists the keywords for the IP Precedence value in the range 0 to 7.
  - **IP ToS** - Configure the IP ToS field:
    - **ToS Bits** - This is the Type of Service octet value in the range 00 to ff to compare against.
    - **ToS Mask** - This indicates which ToS bits are subject to comparison against the Service Type value.
5. Click **CANCEL** to cancel the configuration on the screen. Resets 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.

## 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**.

The screenshot shows the Netgear web interface for a GSM7352S switch. The top navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The QoS section is expanded, showing CoS and DiffServ. The DiffServ section is further expanded to show Advanced, which includes DiffServ Wizard, Auto VoIP, Basic, and Advanced. The Advanced section is selected, showing a list of configuration options: DiffServ Configuration, Class Configuration, Policy Configuration (highlighted), Service Interface Configuration, and Service Statistics. The main content area is titled 'Policy Configuration' and contains a table with the following structure:

Policy Name	Policy Type	Member Class
<input type="text"/>	<input type="text"/>	<input type="text"/>

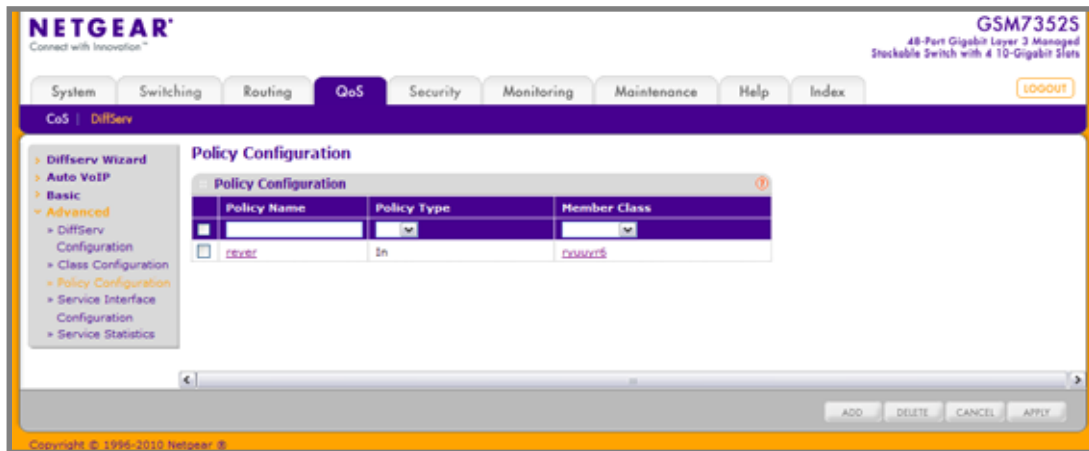
At the bottom of the page, there are buttons for ADD, DELETE, CANCEL, and APPLY. The footer indicates Copyright © 1996-2010 netgear.

1. Use **Policy Name** to uniquely identify a policy using a case-sensitive alphanumeric string from 1 to 31 characters.
2. **Member Class** - This lists all existing DiffServ classes currently defined as members of the specified Policy, from which one can be selected. This list is automatically updated as a new class is added to or removed from the policy. This field is a selector field only when an existing policy class instance is to be removed. After removal of the policy class instance this becomes a non-configurable field.
3. **Policy Type** - Indicates the type is specific to inbound traffic direction.
4. Click **ADD** to add a new policy to the switch.
5. Click **DELETE** to delete the currently selected policy from the switch.

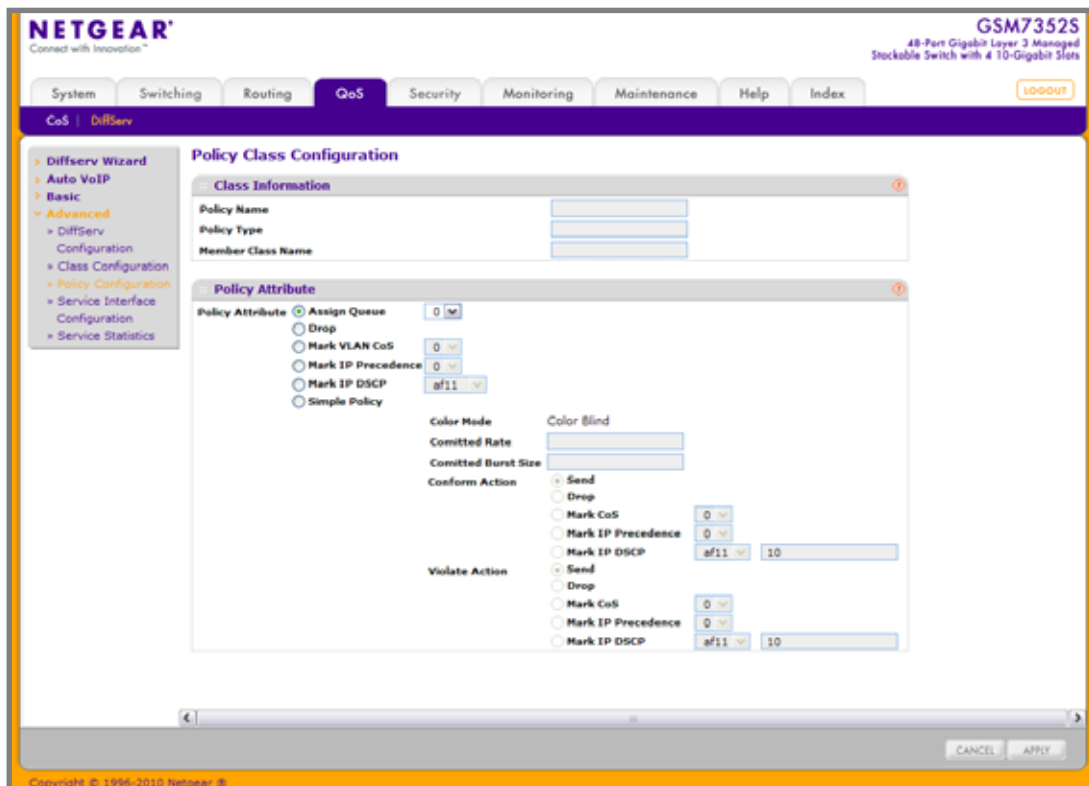


To configure the policy attributes:

1. Click the name of the policy.



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



2. Select the queue to which packets will of this policy-class will be assigned. This is an integer value in the range 0 to 7.
3. Configure the policy attributes:
  - **Drop** - Select the drop radio button. This flag indicates that the policy attribute is defined to drop every inbound packet.
  - **Mark VLAN CoS** - This is an integer value in the range from 0 to 7 for setting the VLAN priority.
  - **Mark IP Precedence** - This is an IP Precedence value in the range from 0 to 7.
  - **Mark IP DSCP** - This lists the keywords for the known DSCP values from which one can be selected. The list includes 'other' as an option for the remaining values.
  - **Simple Policy** - Use this attribute to establish the traffic policing style for the specified class. This command uses 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** - This lists the color mode. The default is 'Color Blind'.
    - **Color Blind**
    - **Color Aware**

**Color Aware** mode requires the existence of one or more color classes that are valid for use with this policy instance. A valid color class contains a single, non-excluded match criterion for one of the following fields (provided the field does not conflict with the classifier of the policy instance itself):

- **CoS**
- **IP DSCP**
- **IP Precedence**
- **Committed Rate** - This value is specified in the range 1 to 4294967295 kilobits-per-second (Kbps).
- **Committed Burst Size** - This value is specified in the range 1 to 128 KBytes. The committed burst size is used to determine the amount of conforming traffic allowed.
- **Conform Action** - This lists the actions to be taken on conforming packets per the policing metrics, from which one can be selected. The default is 'send'.
- **Violate Action** - This lists the actions to be taken on violating packets per the policing metrics, from which one can be selected. The default is 'send'.
- For each of the above Action Selectors one of the following actions can be taken:
  - **Drop** - These packets are immediately dropped.
  - **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.
  - **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.

- **Send** - These packets are presented unmodified by DiffServ to the system forwarding element.
  - **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.
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.

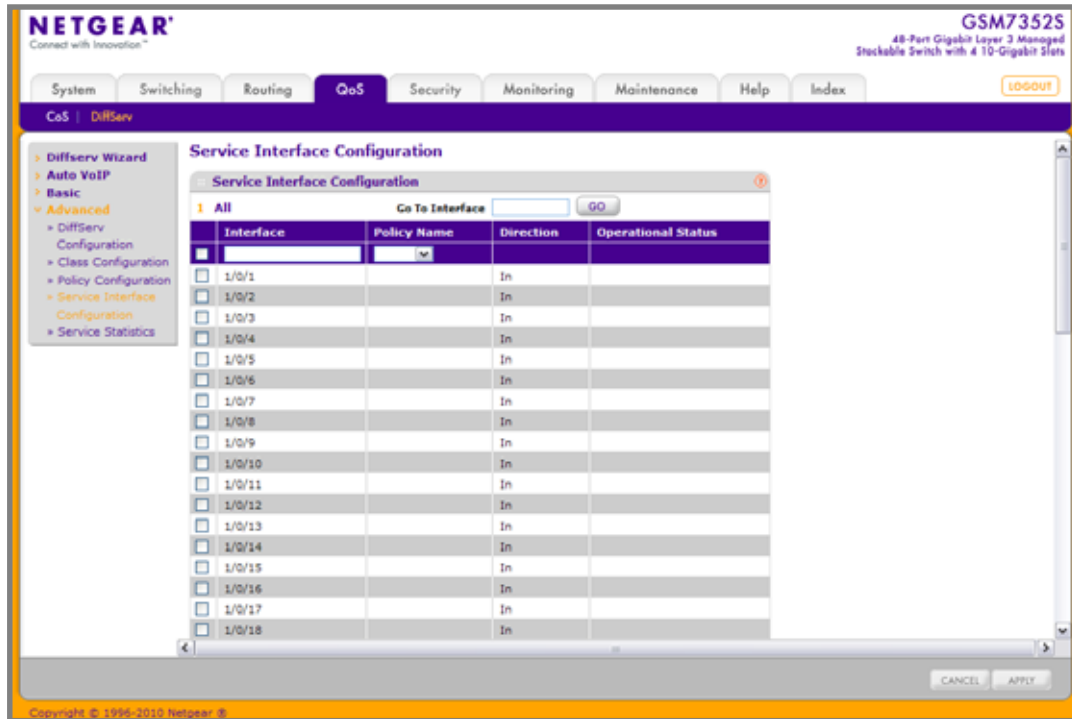
Table 5-77.

Field	Description
Policy Name	Displays name of the DiffServ policy.
Policy Type	Displays type of the policy as In
Member Class Name	Displays name of each class instance within the policy.

## Service Interface Configuration

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

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



To configure DiffServ policy settings on an interface:

1. Use **Interface** to select the interface on which you will configure the DiffServer service.
2. **Policy Name** - Lists all the policy names from which one can be selected. This field is not shown for Read/Write users where inbound service policy attachment is not supported by the platform.

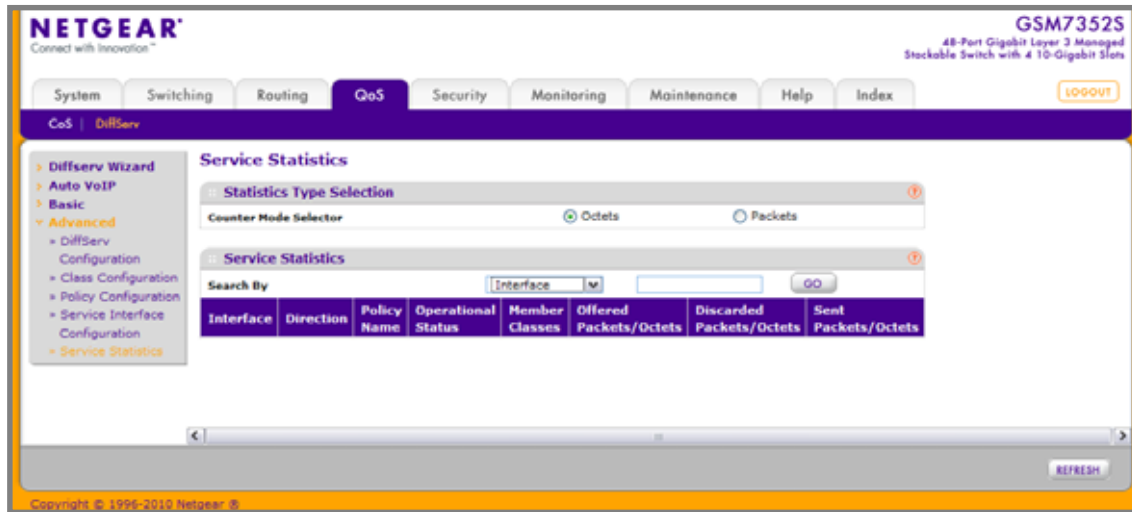
Table 5-78.

Field	Description
Direction	Shows that the traffic direction of this service interface is In.
Operational Status	Shows the operational status of this service interface, either Up or Down.

## Service Statistics

This screen displays class-oriented statistical information for the policy, which is specified by the interface and direction. The 'Member Classes' drop down list is populated on the basis of the specified interface and direction and hence the attached policy (if any). Highlighting a member class name displays the statistical information for the policy-class instance for the specified interface and direction.

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



The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual interface. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The QoS tab is selected, and the left sidebar shows the navigation menu with 'DiffServ' expanded, leading to 'Advanced' and then 'Service Statistics'.

The main content area is titled 'Service Statistics' and includes a 'Statistics Type Selection' section with a 'Counter Mode Selector' set to 'Octets'. Below this is a 'Service Statistics' table with columns for Interface, Direction, Policy Name, Operational Status, Member Classes, Offered Packets/Octets, Discarded Packets/Octets, and Sent Packets/Octets. A search bar is also present.

Interface	Direction	Policy Name	Operational Status	Member Classes	Offered Packets/Octets	Discarded Packets/Octets	Sent Packets/Octets
[Empty table body]							

**Counter Mode Selector** specifies the format of the displayed counter values, which must be either Octets or Packets. The default is 'Octets'.

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

**Table 5-79.**

Field	Description
Interface	List of all valid slot number and port number combinations in the system that have a DiffServ policy currently attached in In direction.
Direction	List of the traffic direction of interface as In. Only shows the direction(s) for which a DiffServ policy is currently attached.
Policy Name	Name of the policy currently attached to the specified interface and direction.
Operational Status	Operational status of the policy currently attached to the specified interface and direction. The value is either Up or Down.
Member Classes	List of all DiffServ classes currently defined as members of the selected Policy Name. Choose one member class name at a time to display its statistics. If no class is associated with the chosen policy then nothing will be populated in the list.
Offered Packets/Octets	A count of the total number of packets/octets offered to all class instances in this service policy before their defined DiffServ treatment is applied. This is the overall count per-interface, per-direction.
Discarded Packets/Octets	A count of the total number of packets/octets 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.
Sent Packets/Octets	A count of the total number of packets/octets forwarded for all class instances in this service policy after their defined DiffServ treatments were applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function of an outbound link transmission element. This is the overall count per-interface, per-direction.

# 6 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 427
- [Configuring Management Access](#) on page 450
- [Port Authentication](#) on page 466
- [Traffic Control](#) on page 481
- [Control](#) on page 496
- [Configuring Access Control Lists](#) on page 524

## 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:

- [Local User](#) on page 428
- [Enable Password Configuration](#) on page 431
- [Line Password Configuration](#) on page 432
- [RADIUS](#) on page 433
- [Configuring TACACS+](#) on page 440
- [Authentication List Configuration](#) on page 443
- [Login Sessions](#) on page 450

## Local User

From the Local User link, you can access the following pages:

- [User Management](#) on page 428
- [User Password Configuration](#) on page 430

### *User Management*

By default, two user accounts exist:

- admin, with 'Read/Write' privileges
- guest, with 'Read Only' privileges

By default, both of these accounts have blank passwords. The names are not case sensitive.

If you logon with a user account with 'Read/Write' privileges (i.e. as admin) you can use the User Accounts screen to assign passwords and set security parameters for the default accounts, and to add and delete accounts (other than admin) up to the maximum of six. Only a user with 'Read/Write' privileges may alter data on this screen, and only one account may be created with 'Read/Write' privileges.



To display the User Management page, click **Security > Management Security > Local User > User Management**.

1. Use **User Name** to enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) User names are up to eight characters in length and are not case sensitive. Valid characters include all the alphanumeric characters as well as the dash ('-') and underscore ('\_') characters. User name "default" is not valid. User names once created cannot be changed/modified.
2. Set the **Edit Password** field to "Enable" only when you want to change the password. The default value is "Disable".
3. Use **Password** to enter the optional new or changed password for the account. It will not display as it is typed, only asterisks(\*) will show. Passwords are up to eight alpha numeric characters in length, and are case sensitive.
4. Use **Confirm Password** to enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (\*).
5. **Access Mode** indicates the user's access mode. The admin account always has 'Read/Write' access, and all other accounts have 'Read Only' access.
6. Click **ADD** to add a user account with 'Read Only' access.
7. Click **DELETE** to delete the currently selected user account. This button is only visible when you have selected a user account with 'Read Only' access. You cannot delete the 'Read/Write' user.

**Table 6-80.**

Field	Description
Lockout Status	Indicates whether the user account is locked out (TRUE or FALSE).
Password Expiration Date	Indicates the current password expiration date in date format.

## User Password Configuration

To display the User Password Configuration page, click **Security** > **Management Security** > **Local User** > **User Password Configuration**.

The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual interface. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Security tab is selected, and the left sidebar shows the navigation path: Local User > User Management > User Password Configuration. The main content area is titled "Password Configuration" and contains a table with the following fields:

Password Configuration		
Password Minimum Length	<input type="text" value="8"/>	(0 to 64)
Password Aging (days)	<input type="text" value="0"/>	(1 to 365)
Password History	<input type="text" value="0"/>	(0 to 10)
Lockout Attempts	<input type="text" value="0"/>	(1 to 5)

At the bottom of the page, there are "CANCEL" and "APPLY" buttons. The footer indicates "Copyright © 1996-2010 Netgear Inc."

1. Use **Password Minimum Length** to specify the minimum character length of all new local user passwords.
2. Use **Password Aging (days)** to specify the maximum time that user passwords are valid, in days, from the time the password is set. Once a password expires, the user will be required to enter a new password following the first login after password expiration. A value of 0 indicates that passwords never expire.
3. Use **Password History** to specify the number of previous passwords to store for prevention of password reuse. This ensures that each user does not reuse passwords often. A value of 0 indicates that no previous passwords will be stored.
4. Use **Lockout Attempts** to specify the number of allowable failed local authentication attempts before the user's account is locked. A value of 0 indicates that user accounts will never be locked.

## Enable Password Configuration

This page prompts you to change the Privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case sensitive.

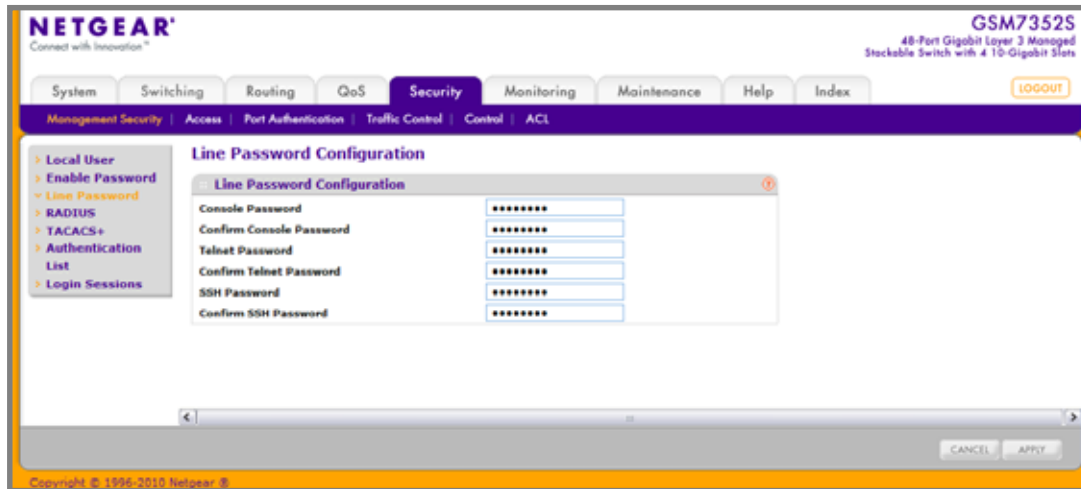
To display the Enable Password Configuration page, click **Security** > **Management Security** > **Enable Password**.

The screenshot shows the Netgear web interface for a GSM7352S switch. The navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under the Security tab, the sub-tabs are Management Security, Access, Port Authentication, Traffic Control, Control, and ACL. The left sidebar shows a tree view with 'Local User' expanded, containing 'Enable Password', 'Line Password', 'RADIUS', 'TACACS+', 'Authentication List', and 'Login Sessions'. The main content area is titled 'Enable Password Configuration' and contains a form with two fields: 'Password' and 'Confirm Password', both masked with asterisks. At the bottom right of the form are 'CANCEL' and 'APPLY' buttons. The footer of the page reads 'Copyright © 1996-2010 Netgear, Inc.'

1. Use **Password** to specify a password. Passwords are a maximum of 64 alphanumeric characters.
2. Use **Confirm Password** to enter the password again, to confirm that you entered it correctly.

## Line Password Configuration

To display the Line Password Configuration page, click **Security** > **Management Security** > **Line Password**.



1. Use **Console Password** to enter the Console password. Passwords are a maximum of 64 alphanumeric characters.
2. Use **Confirm Console Password** to enter the password again, to confirm that you entered it correctly.
3. Use **Telnet Password** to enter the Telnet password. Passwords are a maximum of 64 alphanumeric characters.
4. Use **Confirm Telnet Password** to enter the password again, to confirm that you entered it correctly.
  - The Encrypted option allows the administrator to transfer the privileged EXEC password between devices without having to know the password. The Password field must be exactly 128 hexadecimal characters.
5. Use **SSH Password** to enter the SSH password. Passwords are a maximum of 64 alphanumeric characters.
6. Use **Confirm SSH Password** to enter the password again, to confirm that you entered it correctly.
  - The Encrypted option allows the administrator to transfer the privileged EXEC password between devices without having to know the password. The Password field must be exactly 128 hexadecimal characters.

## RADIUS

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 433
- [\*RADIUS Server Configuration\*](#) on page 435
- [\*Accounting Server Configuration\*](#) on page 438

### 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** > **Radius Configuration**.

The screenshot displays the Netgear web interface for the RADIUS Configuration page. The interface has a top navigation bar with tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Security tab is active, and the left sidebar shows the navigation menu with 'RADIUS' expanded. The main content area is titled 'RADIUS Configuration' and contains a form with the following fields:

- Current Server Address: [Blank]
- Number of Configured Servers: [0]
- Max Number of Retransmits: [4] (1 to 15)
- Timeout Duration (secs): [5] (1 to 30)
- Accounting Mode: [Disable] (radio buttons for Disable and Enable)
- Radius Attribute 4 Mode: [Disable] (radio buttons for Disable and Enable)

At the bottom of the form are 'CANCEL' and 'APPLY' buttons. The footer of the page shows 'Copyright © 1996-2010 Netgear Inc.'

The Current Server IP Address field is blank if no servers are configured (see <pdf>“RADIUS Server Configuration” on page 6-435). 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. The value of the maximum number of times a request packet is retransmitted. The valid range is 1 - 15.

Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS time-out. 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 time-out 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 time-out) 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 time-out value, in seconds, for request retransmissions. The valid range is 1 - 30.

Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS time-out. 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 time-out 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 time-out) 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. Use **RADIUS Attribute 4** to enable or disable RADIUS attribute 4. Default value is Disable.

This is an optional field and can be seen only when RADIUS attribute 4 is enabled. It takes IP address value in the format (xx.xx.xx.xx).

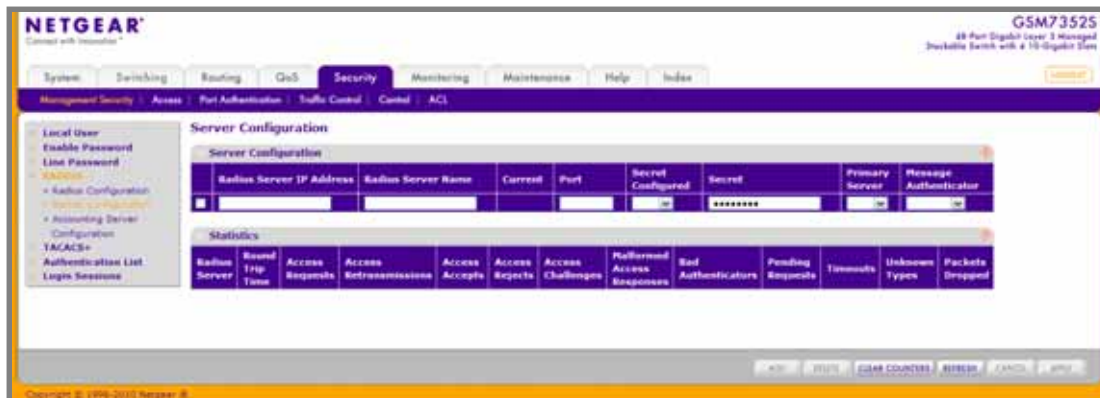
**Table 6-81.**

Field	Description
Current Server Address	The Address of the current server. This field is blank if no servers are configured.
Number of Configured Servers	The number of RADIUS servers that have been configured. This value will be in the range of 0 and 3.

## 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> 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 **Radius Server IP Address** field, specify the IP address of the RADIUS server to add.
  - In the **Radius Server Name** field, specify the Name of the server being added.
  - Use **Port** to specify the UDP port used by this server. The valid range is 0 - 65535.
  - Secret Configured** - The Secret will only be applied if this option is “yes”. If the option is “no”, anything entered in the Secret field will have no affect and will not be retained.
  - Use **Secret** to specify the shared secret for this server.
  - Use **Primary Server** to set the selected server to the Primary or Secondary server.
  - Use **Message Authenticator** to enable or disable the message authenticator attribute for the selected server.
- Click **ADD** to add a new server to the switch. This button is only available to READWRITE users. These changes will not be retained across a power cycle unless a save is performed.
- Click **DELETE** to remove the selected server from the configuration. This button is only available to READWRITE users. These changes will not be retained across a power cycle unless a save is performed.

Table 6-82.

Field	Description
Current	Indicates if this server is currently in use as the authentication server.

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

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.

**Table 6-83.**

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



Table 6-83.

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

## 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**.

The screenshot displays the 'Accounting Server Configuration' page in the Netgear web interface. The page has a purple header with the Netgear logo and a navigation menu. The main content area is titled 'Accounting Server Configuration' and contains a table for configuring RADIUS accounting servers. The table has columns for Accounting Server IP Address, Accounting Server Name, Port, Secret Configured, Secret, and Accounting Mode. Below the table is a 'Statistics' section with a table showing various metrics like Accounting Server, Round Trip Time, Accounting Requests, Accounting Retransmissions, Accounting Responses, Halfformed Accounting Responses, Bad Authenticators, Pending Requests, Timeouts, Unknown Types, and Packets Dropped. The bottom of the page shows a status bar with 'GSM73525' and '48 Port Gigabit Layer 3 Managed Stackable Switch with a 10-Gigabit SFP'.

To configure the RADIUS accounting server:

1. In the **Accounting Server IP Address** field, specify the IP address of the RADIUS accounting server to add.
2. In the **Accounting Server Name** field, enter the Name of the accounting server to add.
3. 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. If the user has READONLY access, the value is displayed but cannot be changed.
4. 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.
5. In the **Secret** field, type the shared secret to use with the specified accounting server.
6. From the **Accounting Mode** menu, enable or disable the RADIUS accounting mode.
7. To delete a configured RADIUS Accounting server, click **Delete**.

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

Click **CLEAR COUNTERS** to clear the accounting server statistics.

**Table 6-84.**

Field	Description
Accounting Server Address	Identifies the accounting server associated with the statistics.
Round Trip Time(secs)	Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Accounting Requests	Displays the number of RADIUS Accounting-Request packets sent not including retransmissions.
Accounting Retransmissions	Displays the number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting 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	Displays the number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	Displays the number of accounting timeouts to this server.
Unknown Types	Displays the number of RADIUS packets of unknown type that were received from this server on the accounting port.
Packets Dropped	Displays the number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

## 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.

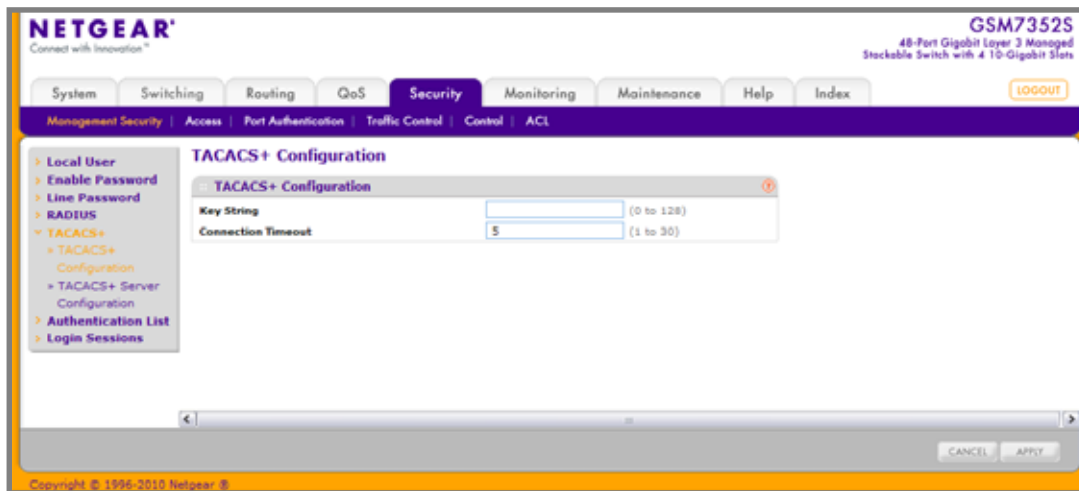
The TACACS+ folder contains links to the following features:

- [\*Configuring TACACS+\*](#) on page 440
- [\*TACACS+ Server Configuration\*](#) on page 442

## 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 > TACACS+ > TACACS+ Configuration**.



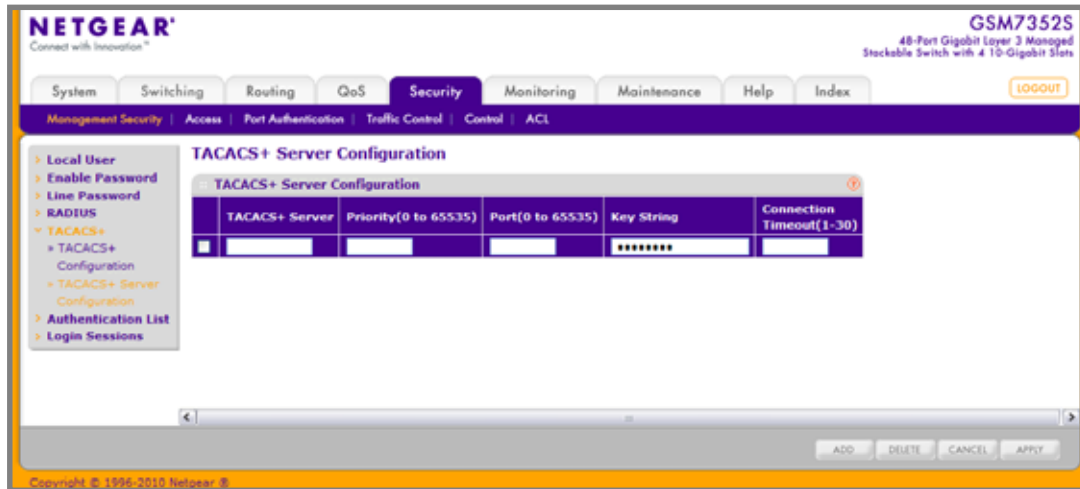
To configure global TACACS+ settings:

1. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the Managed Switch 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 Managed Switch and the TACACS+ server.
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** > **TACACS+** > **TACACS+ Server Configuration**.



To configure TACACS+ server settings:

1. Use **TACACS+ Server** to enter the configured TACACS+ server IP address.
2. Use **Priority** to specify the order in which the TACACS+ servers are used. It should be within the range 0-65535.
3. Use **Port** to specify the authentication port. It should be within the range 0-65535.
4. Use **Key String** to specify the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The valid range is 0-128 characters. The key must match the encryption used on the TACACS+ server.
5. Use **Connection Timeout** to specify the amount of time that passes before the connection between the device and the TACACS+ server time out. The range is between 1-30.
6. Click **ADD** to add a new server to the switch. This button is only available to READWRITE users. These changes will not be retained across a power cycle unless a save is performed.
7. Click **DELETE** to delete the selected server from the configuration.

## Authentication List Configuration

The Authentication List folder contains links to the following features:

- [Login Authentication List](#) on page 443
- [Enable Authentication List](#) on page 445
- [Dot1x Authentication List](#) on page 447
- [HTTP Authentication List](#) on page 448
- [HTTPS Authentication List](#) on page 449

### Login Authentication List

You use this page to configure login lists. A login list specifies the authentication method(s) you want to be used to validate switch or port access for the users associated with the list. The pre-configured users, admin and guest, are assigned to a pre-configured list named defaultList, which you may not delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list

To display the Login Authentication List page, click **Security > Management Security > Authentication List > Login Authentication List**.

**NETGEAR**  
Connected with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security Access Port Authentication Traffic Control Control ACL

Local User  
Enable Password  
Line Password  
RADIUS  
TACACS+  
Authentication List  
Login Authentication List  
Enable Authentication List  
Dot1x Authentication List  
HTTP Authentication List  
HTTPS Authentication List  
Login Sessions

### Login Authentication List

Login Authentication List

List Name	1	2	3	4	5	6
<input type="checkbox"/> defaultList	Local					
<input type="checkbox"/> networkList	Local					

ADD DELETE CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

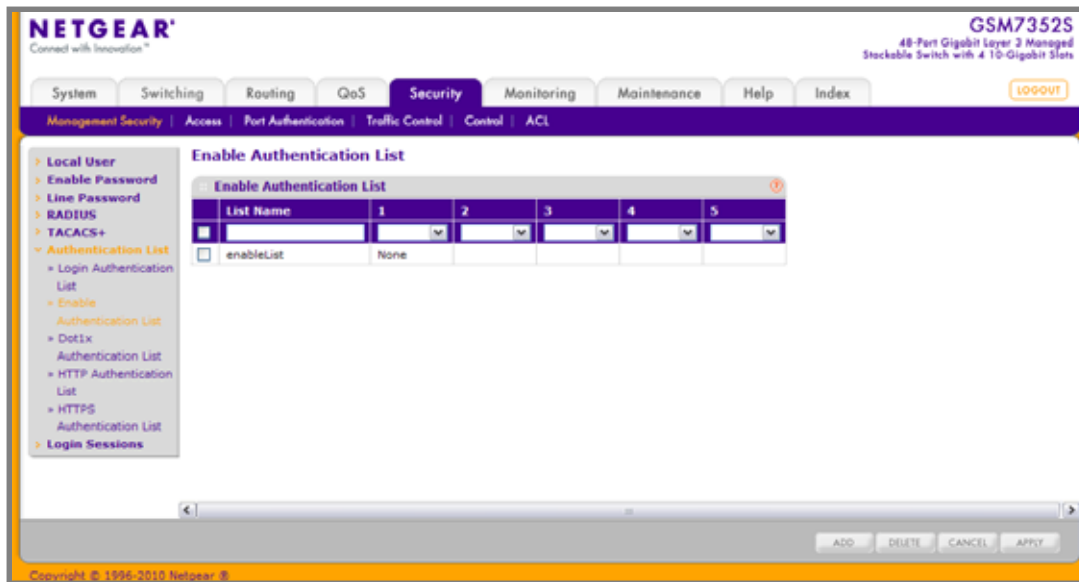
1. **List Name** - If you are creating a new login list, enter the name you want to assign. It can be up to 15 alphanumeric characters long and is not case sensitive.
2. Use the dropdown menu to select the method that should appear first in the selected authentication login list. If you select a method 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. The options are:
  - **Local** - The user's locally stored ID and password will be used for authentication.
  - **Radius** - The user's ID and password will be authenticated using the RADIUS server instead of locally.
  - **Line** - The line password will be used for authentication.
  - **Enable** - The privileged EXEC password will be used for authentication.
  - **Tacacs** - The user's ID and password will be authenticated using the TACACS+ server.
  - **None** - The user will not be authenticated.
3. Use the dropdown menu to select the method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. Note that this parameter will not appear when you first create a new login list.
4. Use the dropdown menu to select the method, if any, that should appear third in the selected authentication login list.
5. Use the dropdown menu to select the method, if any, that should appear forth in the selected authentication login list.
6. Use the dropdown menu to select the method, if any, that should appear fifth in the selected authentication login list.
7. Use the dropdown menu to select the method, if any, that should appear sixth in the selected authentication login list.
8. Click **ADD** to add a new login list to the switch.
9. Click **DELETE** to remove the selected authentication login list from the configuration. The delete will fail if the selected login list is assigned to any user (including the default user) for system login. You can only use this button if you have Read/Write access. The change will not be retained across a power cycle unless you perform a save.



## Enable Authentication List

You use this page to configure enable lists. An enable list specifies the authentication method(s) you want to be used to validate privileged EXEC access for the users associated with the list. The pre-configured users, admin and guest, are assigned to a pre-configured list named defaultList, which you may not delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list.

To display the Enable Authentication List page, click **Security > Management Security > Authentication List > Enable Authentication List**.



**NETGEAR**  
Connected with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security Access Port Authentication Traffic Control Control ACL

Local User  
Enable Password  
Line Password  
RADIUS  
TACACS+  
Authentication List  
Login Authentication List  
Enable Authentication List  
Dot1x Authentication List  
HTTP Authentication List  
HTTPS Authentication List  
Login Sessions

### Enable Authentication List

List Name	1	2	3	4	5
enableList	None				

ADD DELETE CANCEL APPLY

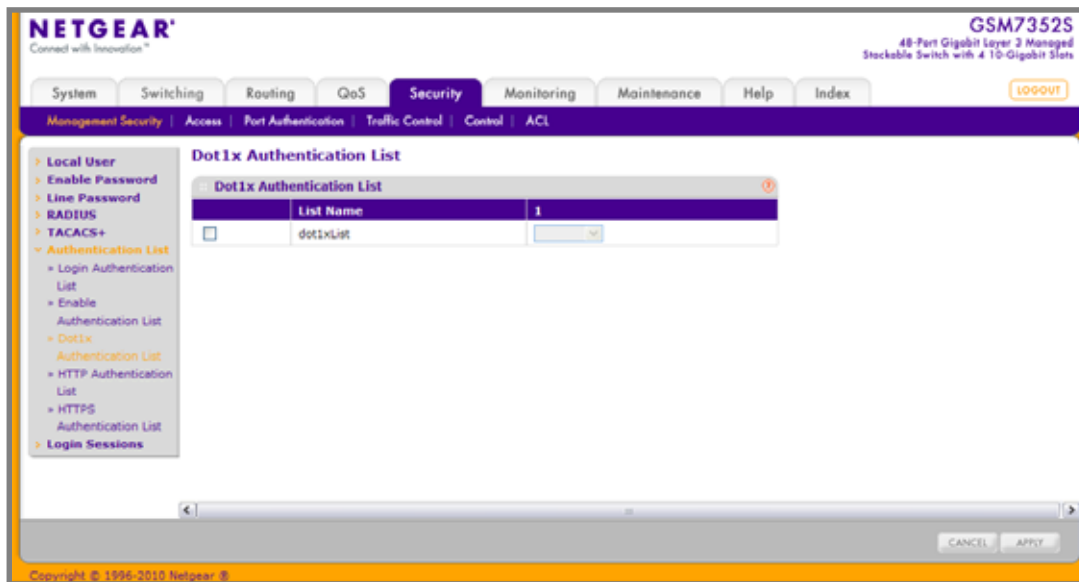
Copyright © 1996-2010 Netgear, Inc.

1. **List Name** - If you are creating a new enable list, enter the name you want to assign. It can be up to 15 alphanumeric characters long and is not case sensitive.
2. Use the dropdown menu to select the 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. The options are:
  - **Radius** - The user's ID and password will be authenticated using the RADIUS server instead of locally.
  - **Line** - The line password will be used for authentication.
  - **Enable** - The privileged EXEC password will be used for authentication.
  - **Tacacs** - The user's ID and password will be authenticated using the TACACS+ server.
  - **None** - The user will not be authenticated.
3. Use the dropdown menu to select the method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. Note that this parameter will not appear when you first create a new login list.
4. Use the dropdown menu to select the method, if any, that should appear third in the selected authentication login list.
5. Use the dropdown menu to select the method, if any, that should appear forth in the selected authentication login list.
6. Use the dropdown menu to select the method, if any, that should appear fifth in the selected authentication login list.
7. Click **ADD** to add a new login list to the switch.
8. Click **DELETE** to remove the selected authentication enable list from the configuration. You can only use this button if you have Read/Write access. The change will not be retained across a power cycle unless you perform a save.

## Dot1x Authentication List

You use this page to configure dot1x lists. A dot1x list specifies the authentication method(s) you want to be used to validate port access for the users associated with the list. Only one dot1x can be supported.

To display the Dot1x Authentication List page, click **Security > Management Security > Authentication List > Dot1x Authentication List**.



1. **List Name** - Select the dot1x list name for which you want to configure data.
2. Use the dropdown menu to select the method that should appear first in the selected authentication login list. The options are:
  - **Local** - The user's locally stored ID and password will be used for authentication.
  - **Radius** - The user's ID and password will be authenticated using the RADIUS server instead of locally.
  - **None** - The user will not be authenticated.

## HTTP Authentication List

You use this page to configure HTTP lists. A HTTP list specifies the authentication method(s) you want used to validate switch or port access through HTTP.

To display the HTTP Authentication List page, click **Security > Management Security > Authentication List > HTTP Authentication List**.

1. **List Name** - Select the HTTP list name for which you want to configure data.
2. Use the dropdown menu to select the 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. The options are:
  - **Local** - The user's locally stored ID and password will be used for authentication.
  - **Radius** - The user's ID and password will be authenticated using the RADIUS server instead of locally.
  - **Tacacs** - The user's ID and password will be authenticated using the TACACS+ server.
  - **None** - The user will not be authenticated.
3. Use the dropdown menu to select the method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. Note that this parameter will not appear when you first create a new login list.
4. Use the dropdown menu to select the method, if any, that should appear third in the selected authentication login list.
5. Use the dropdown menu to select the method, if any, that should appear forth in the selected authentication login list.

## HTTPS Authentication List

You use this page to configure HTTPS lists. A login list specifies the authentication method(s) you want used to validate switch or port access through HTTPS for the users associated with the list.

To display the HTTPS Authentication List page, click **Security > Management Security > Authentication List > HTTPS Authentication List**.

The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual. The main content area is titled "HTTPS Authentication List". It contains a table with the following structure:

List Name	1	2	3	4
<input type="checkbox"/> httpsList	Local			

The left sidebar shows the navigation menu with the following items:

- Local User
- Enable Password
- Line Password
- RADIUS
- TACACS+
- Authentication List
  - Login Authentication List
  - Enable Authentication List
  - Dot1x Authentication List
  - HTTP Authentication List
  - HTTPS Authentication List
- Login Sessions

The top navigation bar includes the following tabs: System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The top right corner shows the device model "GSM7352S" and a "LOGOUT" button.

1. **List Name** - Select the HTTPS list name for which you want to configure data.
2. Use the dropdown menu to select the 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. The options are:
  - **Local** - The user's locally stored ID and password will be used for authentication.
  - **Radius** - The user's ID and password will be authenticated using the RADIUS server instead of locally.
  - **Tacacs** - The user's ID and password will be authenticated using the TACACS+ server.
  - **None** - The user will not be authenticated.
3. Use the dropdown menu to select the method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. Note that this parameter will not appear when you first create a new login list.
4. Use the dropdown menu to select the method, if any, that should appear third in the selected authentication login list.
5. Use the dropdown menu to select the method, if any, that should appear forth in the selected authentication login list.

## Login Sessions

To display the Login Sessions page, click **Security** > **Management Security** > **Login Sessions**.

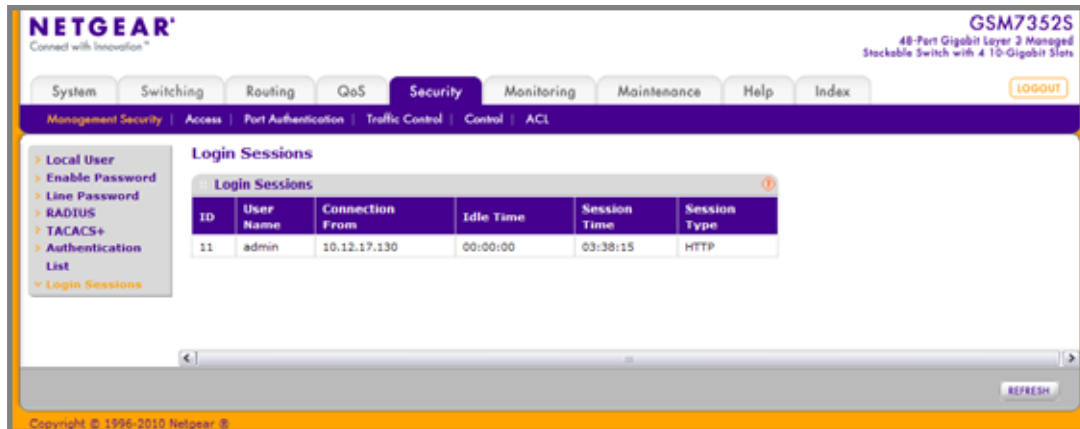


Table 6-85.

Field	Description
ID	Identifies the ID of this row.
User Name	Shows the user name of user made the session.
Connection From	Shows the user is connected from which machine.
Idle Time	Shows the idle session time.
Session Time	Shows the total session time.
Session Type	Shows the type of session: telnet, serial or SSH

## Configuring Management Access

From the Access page, you can configure HTTP and Secure HTTP access to the ProSafe® Managed Switches management interface.

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

- [HTTP](#) on page 451
- [HTTPS Configuration](#) on page 453
- [SSH](#) on page 458
- [Telnet](#) on page 462
- [Console Port](#) on page 464
- [Denial of Service](#) on page 465

## HTTP

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

- [HTTP Configuration](#) on page 451

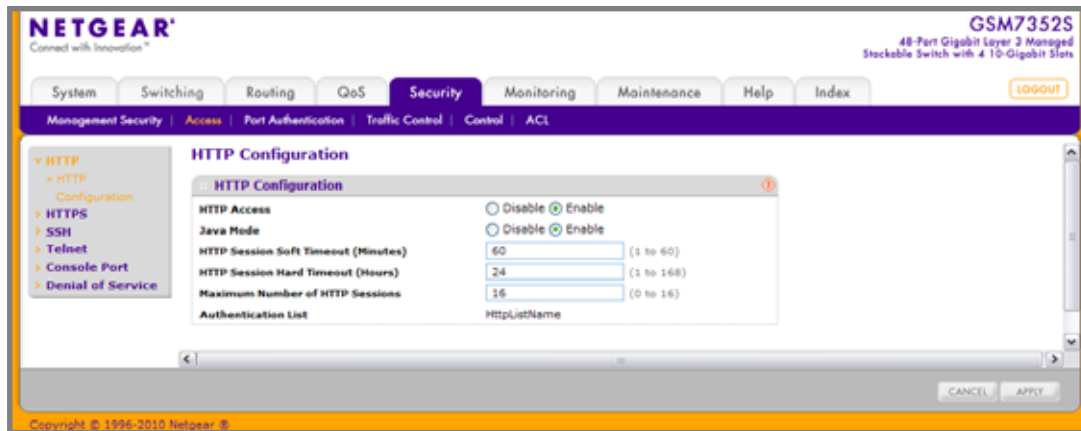
### *HTTP Configuration*

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

- BOOTP
- DHCP
- Terminal interface via the EIA-232 port

Once you have established in-band connectivity, you can change the IP information using a Web-based management.

To access the HTTP Configuration page, click **Security > Access > HTTP > HTTP Configuration**.



To configure the HTTP server settings:

1. Use **HTTP Access** to specify whether the switch may be accessed from a web browser. If you choose to enable web mode you will be able to manage the switch from a web browser. The factory default is enabled.
2. Use **Java Mode** to enable or disable the java applet that displays a picture of the switch at the top right of the screen. If you run the applet you will be able to click on the picture of the switch to select configuration screens instead of using the navigation tree at the left side of the screen. The factory default is disabled.
3. Use **HTTP Session Soft Timeout(Minutes)** to set the inactivity time-out for HTTP sessions. The value must be in the range of (1 to 60) minutes. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.
4. Use **HTTP Session Hard Timeout(Hours)** to set the hard time-out for HTTP sessions. This time-out is unaffected by the activity level of the session. The value must be in the range of (1 to 168) hours. The default value is 24 hours. The currently configured value is shown when the web page is displayed.
5. Use **Maximum Number of HTTP Sessions** to set the maximum allowable number of HTTP sessions. The value must be in the range of (0 to 16). The default value is 16. The currently configured value is shown when the web page is displayed.

Table 6-86.

Field	Description
Authentication List	Shows the authentication list which HTTP are using.



## HTTPS

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

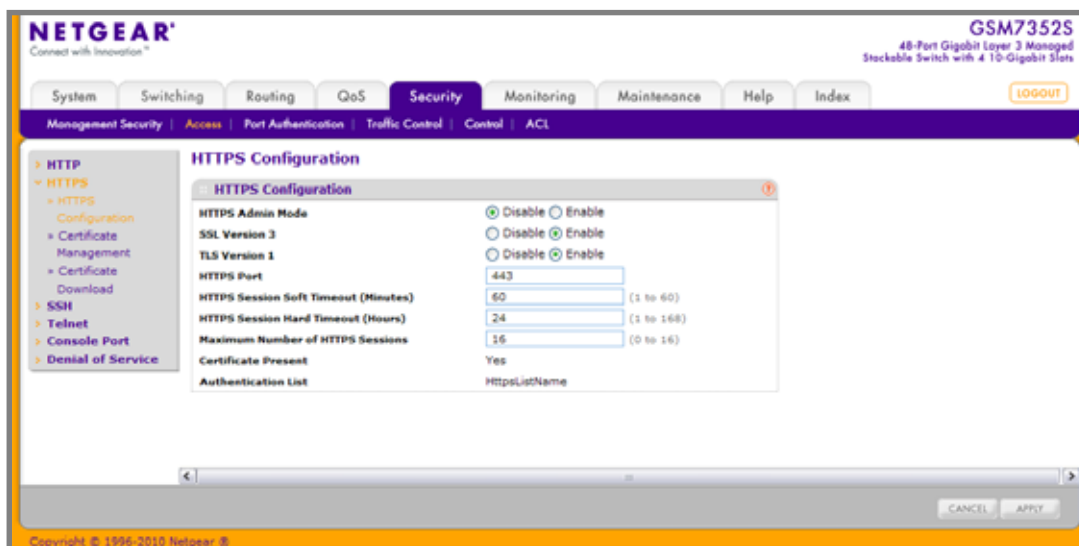
- [HTTPS Configuration](#) on page 453
- [Certificate Management](#) on page 455
- [Certificate Download](#) on page 456

### HTTPS 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 > HTTPS > HTTPS Configuration**.



To configure HTTPS settings:

1. Use **HTTPS Admin Mode** 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 **SSL Version 3** 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 **TLS Version 1** 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. Use **HTTPS Port** to set the HTTPS Port Number. The value must be in the range of 1 to 65535. Port 443 is the default value. The currently configured value is shown when the web page is displayed.
5. Use **HTTPS Session Soft Timeout(Minutes)** to set the inactivity time-out for HTTPS sessions. The value must be in the range of (1 to 60) minutes. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.
6. Use **HTTPS Session Hard Timeout(Hours)** to set the hard time-out for HTTPS sessions. This time-out is unaffected by the activity level of the session. The value must be in the range of (1 to 168) hours. The default value is 24 hours. The currently configured value is shown when the web page is displayed.
7. Use **Maximum Number of HTTPS Sessions** to set the maximum allowable number of HTTPS sessions. The value must be in the range of (0 to 16). The default value is 16. The currently configured value is shown when the web page is displayed.

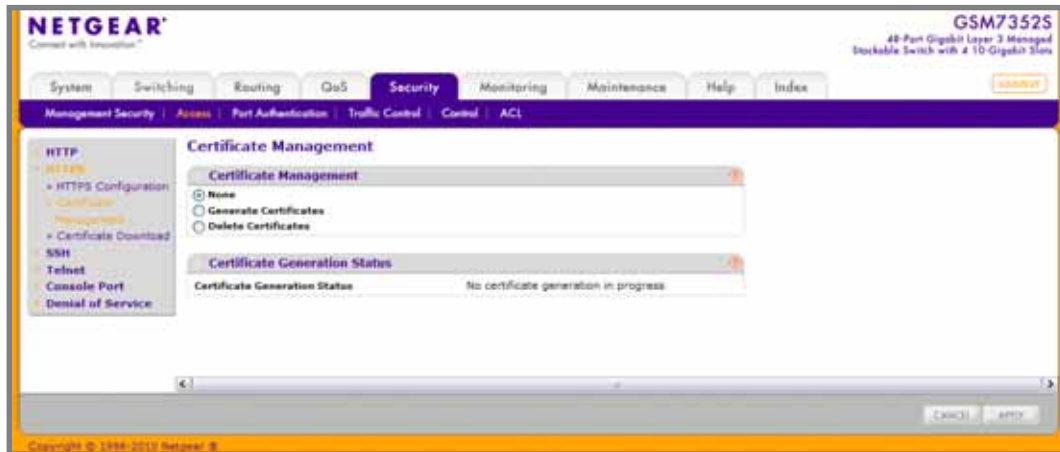
Table 6-87.

Field	Description
Certificate Present	Displays whether there is a certificate present on the device.
Authentication List	Displays authentication list for HTTPS.

## Certificate Management

Use this menu to generate or delete certificates.

To display the Certificate Management page, click **Security > Access > HTTPS > HTTPS Certificate Management**.



1. Use **None** to specify there is no certificate management. This is the default selection.
2. Use **Generate Certificates** to begin generating the Certificate files.
3. Use **Delete Certificates** to delete the corresponding Certificate files, if present.

Table 6-88.

Field	Description
Certificate Generation Status	Displays whether SSL certificate generation is in progress.

## Certificate Download

Use this menu to transfer a certificate file to the switch.

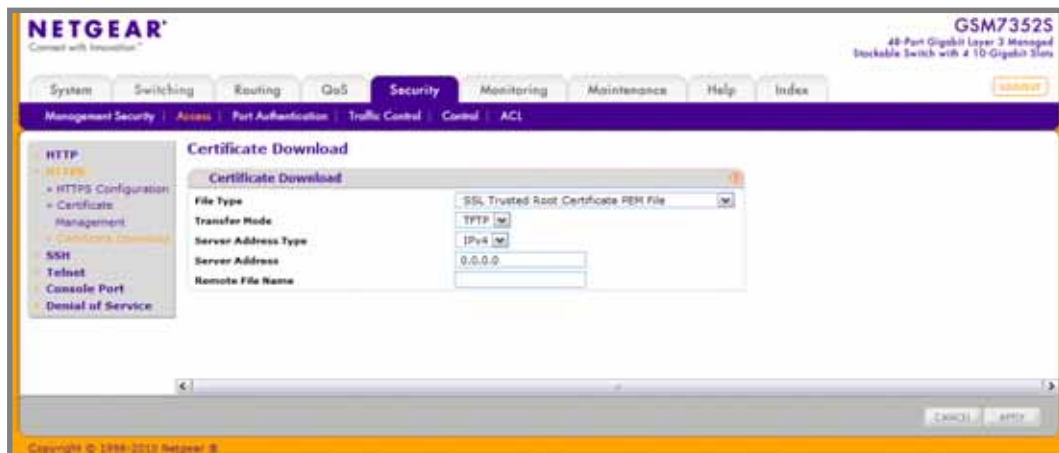
For the Web server on the switch to accept HTTPS connections from a management station, the Web server needs a public key certificate. You can generate a certificate externally (for example, off-line) and download it to the switch.

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

### 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. Use **File Type** to specify the type of file you want to transfer:
  - **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. Use **Transfer Mode** to specify the protocol to use to transfer the file:
  - **TFTP** - Trivial File Transfer Protocol
  - **SFTP** - Secure File Transfer Program
  - **SCP** - Secure Copy
3. Use **Server Address Type** to specify either IPv4 or IPv6 to indicate the format of the TFTP/SFTP/SCP Server Address field. The factory default is IPv4.
4. Use **Server Address** to enter the IP address of the server in accordance with the format indicated by the Server Address Type. The factory default is the IPv4 address 0.0.0.0.
5. Use **Remote File Name** to enter the name on the TFTP server of the file you want to download. You may enter up to 32 characters. The factory default is blank.

## SSH

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

- [SSH Configuration](#) on page 458
- [Host Keys Management](#) on page 460
- [Host Keys Download](#) on page 461

### SSH Configuration

To display the SSH Configuration page, click **Security > Access > SSH > SSH Configuration**.

The screenshot displays the Netgear web interface for a GSM7352S switch. The 'Security' tab is selected, and the 'SSH Configuration' page is shown. The left sidebar contains a navigation menu with options like HTTP, HTTPS, SSH, Telnet, and Denial of Service. The main content area shows the SSH Configuration settings:

- SSH Admin Mode:** Radio buttons for Disable and Enable (Enable is selected).
- SSH Version 1:** Radio buttons for Disable and Enable (Enable is selected).
- SSH Version 2:** Radio buttons for Disable and Enable (Enable is selected).
- SSH Session Timeout:** A text input field with the value '5' and a unit of 'minutes'.
- Maximum Number of SSH Sessions:** A text input field with the value '5'.
- Current Number of SSH Sessions:** A text input field with the value '0'.
- Keys Present:** A dropdown menu with 'Yes' selected.
- Login Authentication List:** A dropdown menu with 'networkList' selected.
- Enable Authentication List:** A dropdown menu with 'enableList' selected.

At the bottom of the page, there are buttons for 'REFRESH', 'CANCEL', and 'APPLY'. The footer indicates 'Copyright © 1996-2010 Netgear, Inc.'.

1. Use **SSH Admin Mode** to Enable or Disable the administrative mode of SSH. The currently configured value is shown when the web page is displayed. The default value is Disable.
2. Use **SSH Version 1** to Enable or Disable Protocol Level 1 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.
3. Use **SSH Version 2** to Enable or Disable Protocol Level 2 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.
4. Use **SSH Session Timeout** to configure the inactivity time-out value for incoming SSH sessions to the switch. The acceptable range for this value is (1-160) minutes.
5. Use **Maximum Number of SSH Sessions** to configure the maximum number of inbound SSH sessions allowed on the switch. The currently configured value is shown when the web page is displayed. The range of acceptable values for this field is (0-5).
6. Use **Login Authentication List** to select an authentication list from the pull down menu. This list is used to authenticate users who try to login the switch.
7. Use **Enable Authentication List** to select an authentication list from the pull down menu. This list is used to authenticate users who try to get “enable” level privilege.
8. Click **REFRESH** to refresh the web page to show the latest SSH Sessions.

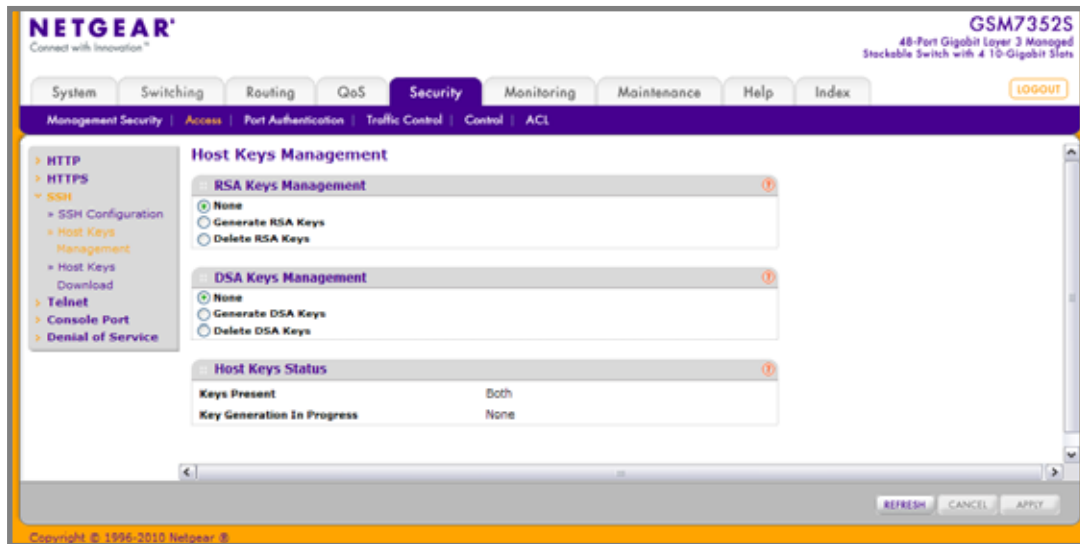
Table 6-89.

Field	Description
Current Number of SSH Sessions	Displays the number of SSH connections currently in use in the system.
Keys Present	Displays which keys, RSA, DSA or both, are present (if any).

## Host Keys Management

Use this menu to generate or delete RSA and DSA keys.

To display the Host Keys Management page, click **Security > Access > SSH > Host Keys Management**.



1. **Host Keys Management** - None is the default selection.
2. Use **Generate RSA Keys** to begin generating the RSA host keys. Note that to generate SSH key files SSH must be administratively disabled and there can be no active SSH sessions.
3. Use **Delete RSA Keys** to delete the corresponding RSA key file, if it is present.
4. **DSA Keys Management** - None is the default selection.
5. Use **Generate DSA Keys** to begin generating the DSA host keys. Note that to generate SSH key files SSH must be administratively disabled and there can be no active SSH sessions.
6. Use **Delete DSA Keys** to delete the corresponding DSA key file, if it is present.
7. Click **APPLY** to start to download the Host Key file. Note that to download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.
8. Click **REFRESH** to refresh the web page to show the latest SSH Sessions.

Table 6-90.

Field	Description
Keys Present	Displays which keys, RSA, DSA or both, are present (if any).
Key Generation In Progress	Displays which key is being generated (if any), RSA, DSA or None.



## Host Keys Download

Use this menu to transfer a file to or from the switch.

To display the Host Keys Download page, click **Security > Access > SSH > Host Keys Download**.

The screenshot shows the Netgear ProSafe Gigabit L3 Managed Stackable Switches Software Administration Manual. The main menu is at the top, with 'Security' selected. The 'Host Keys Download' page is displayed, showing a form with the following fields:

- File Type:** SSH-1 RSA Key File (dropdown menu)
- Transfer Mode:** TFTP (dropdown menu)
- Server Address Type:** IPv4 (dropdown menu)
- Server Address:** 0.0.0.0 (text input)
- Remote File Name:** (empty text input)

The page also includes a sidebar with navigation links and a footer with copyright information.

1. Use **File Type** to specify the type of file you want to transfer:
  - **SSH-1 RSA Key File** - SSH-1 Rivest-Shamir-Adleman (RSA) Key File
  - **SSH-2 RSA Key PEM File** - SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded)
  - **SSH-2 DSA Key PEM File** - SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded)
2. Use **Transfer Mode** to specify the protocol to use to transfer the file:
  - **TFTP** - Trivial File Transfer Protocol
  - **SFTP** - Secure File Transfer Program
  - **SCP** - Secure Copy
3. Use **Server Address Type** to specify either IPv4 or IPv6 to indicate the format of the TFTP/SFTP/SCP Server Address field. The factory default is IPv4.
4. Use **Server Address** to enter the IP address of the server in accordance with the format indicated by the Server Address Type. The factory default is the IPv4 address 0.0.0.0.
5. Use **Remote File Name** to enter the name on the TFTP server of the file you want to download. You may enter up to 32 characters. The factory default is blank.
6. Click **APPLY** to start to download the Host Key file. Note that to download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

## Telnet

To display the Telnet page, click **Security > Access > Telnet**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security | Access | Port Authentication | Traffic Control | Control | ACL

LOGOUT

**TELNET**

**Authentication List**

Login Authentication List: networkList

Enable Authentication List: enableList

**Inbound Telnet**

Allow new telnet sessions: ☒ Disable ☒ Enable

Session Timeout: 5 minutes

Maximum Number of Sessions: 5

Current Number of Sessions: 0

**Outbound Telnet**

Allow new telnet sessions: ☒ Disable ☒ Enable

Session Timeout: 5 minutes

Maximum Number of Sessions: 5

Current Number of Sessions: 0

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

### Telnet Authentication List

This page allows you to select the login and enable authentication list available. The login list specifies the authentication method(s) you want used to validate switch or port access for the users associated with the list. The enable list specifies the authentication method(s) you want used to validate privileged EXEC access for the users associated with the list. These list can be created by Authentication List page under Management Security.

1. Use **Login Authentication List** to specify which authentication list to use when you login through telnet. The default value is networkList.
2. Use **Enable Authentication List** to specify which authentication list you are using when going into the privileged EXEC mode. The default value is enableList.

### *Inbound Telnet Configuration*

This page regulates new telnet sessions. If Allow New Telnet Sessions are enabled, new inbound telnet sessions can be established until there are no more sessions available. If Allow New Telnet Sessions are disabled, no new inbound telnet sessions are established. An established session remains active until the session is ended or an abnormal network error ends the session.

1. Use **Allow New Telnet Sessions** to specify whether the new Inbound Telnet session is Enabled or Disabled. Default value is Enabled.
2. Use **Session Timeout** to specify how many minutes of inactivity should occur on a telnet session before the session is logged off. You may enter any number from 1 to 160. The factory default is 5.
3. Use **Maximum Number of Sessions** to select how many simultaneous telnet sessions will be allowed. The maximum is 5, which is also the factory default.
4. **Current Number of Sessions** - Displays the number of current sessions.

### *Outbound Telnet Client Configuration*

This page regulates new outbound telnet connections. If Allow New Telnet Sessions are enabled, new outbound telnet sessions can be established until there are no more sessions available. If Allow New Telnet Sessions are disabled, no new outbound telnet sessions are established. An established session remains active until the session is ended or an abnormal network error ends the session.

1. Use **Allow New Telnet Sessions** to specify whether the new Outbound Telnet Session is Enabled or Disabled. Default value is Enabled.
2. Use **Maximum Number of Sessions** to specify the maximum number of Outbound Telnet Sessions allowed. Default value is 5. Valid Range is (0 to 5).
3. Use **Session Timeout** to specify the Outbound Telnet login inactivity time-out. Default value is 5. Valid Range is (1 to 160).
4. **Current Number of Sessions** - Displays the number of current sessions.

## Console Port

To display the Console Port page, click **Security > Access > Console Port**.

The screenshot shows the Netgear web interface for the Console Port configuration. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Security tab is selected, and the left sidebar shows a tree view with options like HTTP, HTTPS, SSH, Telnet, Console Port, and Denial of Service. The main content area is titled 'Console Port' and contains a form with the following fields:

- Serial Port Login Timeout (minutes):** A text input field with the value '5' and a range '(0 to 160)'.
- Baud Rate (bps):** A pull-down menu with '9600' selected.
- Character Size (bits):** A text input field with the value '8'.
- Flow Control:** A pull-down menu with 'Disable' selected.
- Stop Bits:** A text input field with the value '1'.
- Parity:** A pull-down menu with 'None' selected.
- Login Authentication List:** A pull-down menu with 'defaultList' selected.
- Enable Authentication List:** A pull-down menu with 'enableList' selected.

At the bottom of the form are 'CANCEL' and 'APPLY' buttons. The footer of the page reads 'Copyright © 1996-2010 Netgear, Inc.'.

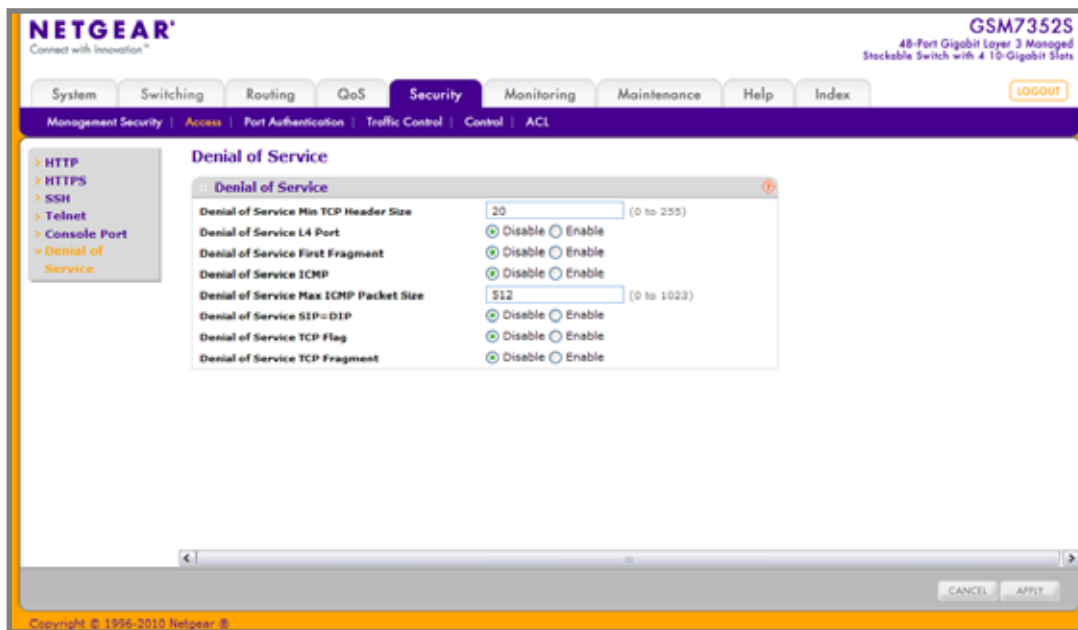
1. Use **Serial Port Login Timeout (minutes)** to specify how many minutes of inactivity should occur on a serial port connection before the switch closes the connection. Enter a number between 0 and 160: the factory default is 5. Entering 0 disables the time-out.
2. Use **Baud Rate (bps)** to select the default baud rate for the serial port connection from the pull-down menu. You may choose from 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory default is 9600 baud.
3. Use **Login Authentication List** to specify which authentication list to use when you login through Telnet. The default value is defaultList.
4. Use **Enable Authentication List** to specify which authentication list you are using when going into the privileged EXEC mode. The default value is enableList.

Table 6-91.

Field	Description
Character Size (bits)	The number of bits in a character. This is always 8.
Flow Control	Whether hardware flow control is enabled or disabled. It is always disabled.
Stop Bits	The number of stop bits per character. Its is always 1.
Parity	The parity method used on the serial port. It is always None.

## Denial of Service

To display the Denial of Service page, click **Security** > **Access** > **Denial of Service**.



1. Use **Denial of Service Min TCP Header Size** to specify the Min TCP Hdr Size allowed. If DoS TCP Fragment is enabled, the switch will drop these packets:
  - **First TCP fragments that has a TCP payload** -  $IP\_Payload\_Length - IP\_Header\_Size < Min\_TCP\_Header\_Size$ .

The factory default is disabled.

2. Use **Denial of Service L4 Port** to enable L4 Port DoS prevention causing the switch to drop packets having source TCP/UDP port number equal to destination TCP/UDP port number. The factory default is disabled.
3. Use **Denial of Service First Fragment** to enable First Fragment DoS prevention causing the switch to check DoS options on first fragment IP packets when switch are receiving fragmented IP packets. Otherwise, switch ignores the first fragment IP packages. The factory default is disabled.
4. Use **Denial of Service ICMP** to enable ICMP DoS prevention causing the switch to drop ICMP packets that have a type set to ECHO\_REQ (ping) and a size greater than the configured ICMP Pkt Size. The factory default is disabled.
5. Use **Denial of Service Max ICMP Packet Size** to specify the Max ICMP Packet Size allowed (This includes the ICMP header size of 8 bytes). If ICMP DoS prevention is enabled, the switch will drop ICMP ping packets that have a size greater then this configured Max ICMP Packet Size minus the ICMP header size of 8 bytes. The factory default is 512.
6. Use **Denial of Service SIP=DIP** to enable SIP=DIP DoS prevention causing the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
7. Use **Denial of Service TCP FLAG** to enable TCP Flag DoS prevention causing the switch to drop these packets:
  - TCP SYN flag=1 & source port < 1024
  - TCP control flag =0 & sequence number = 0
  - TCP FIN,URG,PSH bits set & sequence number = 0
  - TCP SYN & FIN bits set

The factory default is disabled.

8. Use **Denial of Service TCP Fragment** to enable TCP Fragment DoS prevention causing the switch to drop packets:
  - **First TCP fragments that has a TCP payload** -  $IP\_Payload\_Length - IP\_Header\_Size < Min\_TCP\_Header\_Size$ .

The factory default is disabled.

## 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](#) on page 467
- [Advanced](#) on page 470

## Basic

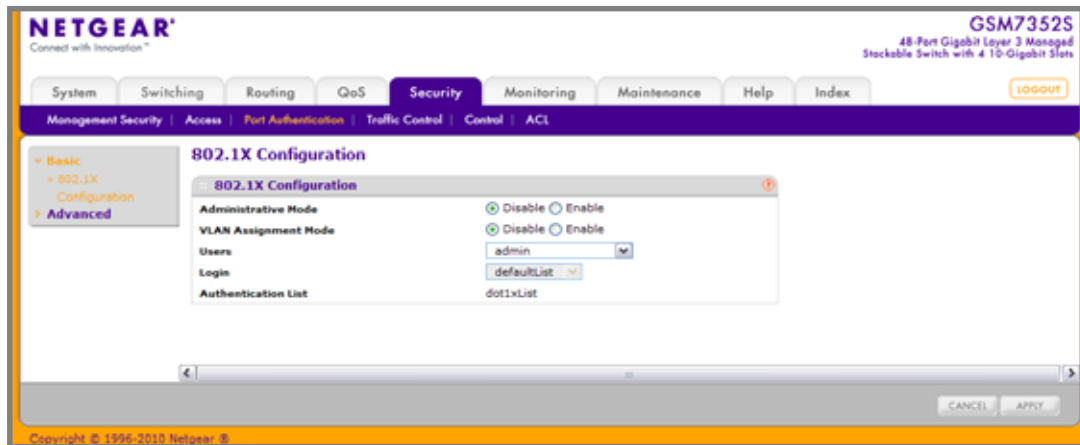
From the Basic link, you can access the following pages:

- [802.1X Configuration](#) on page 468

## 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 > Authentication List** and select RADIUS as method 1 for defaultList. For more information, see <pdf>“Authentication List Configuration” on page 6-443.

---

- **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. Default value.
2. Use **VLAN Assignment Mode** to select one of options for VLAN Assignment mode: enable and disable. The default value is disable.
  3. Use **Users** to select the user name that will use the selected login list for 802.1x port security.
  4. Use **Login** to select the login to apply to the specified user. All configured logins are displayed.

**Table 6-92.**

Field	Description
Authentication List	Displays the authentication list which is used by 802.1X.

## Advanced

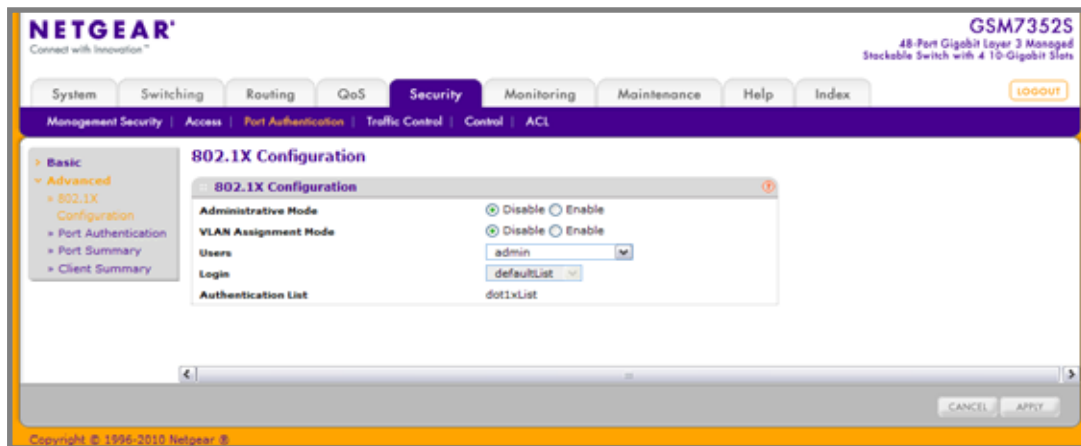
From the Advanced link, you can access the following pages:

- [802.1X Configuration](#) on page 470
- [Port Authentication](#) on page 471
- [Port Summary](#) on page 476

### 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** > **Advanced** > **802.1X Configuration**.



1. Use **Administrative Mode** to select one of the options for administrative mode: enable and disable. The default value is disable.
2. Use **VLAN Assignment Mode** to select one of the options for VLAN Assignment mode: enable and disable. The default value is disable.
3. Use **Users** to select the user name that will use the selected login list for 802.1x port security.
4. Use **Login** to select the login to apply to the specified user. All configured logins are displayed.

**Table 6-93.**

Field	Description
Authentication List	Displays the authentication list which is used by 802.1X.

### *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 > Advanced > Port Authentication**.

---

**Note:** Use the horizontal scroll bar at the bottom of the browser to view all the fields on the Port Authentication page.

---

**Port Authentication**

Port Authentication

1 All Go To Port

	Port	Control Mode	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID	Supplicant Timeout	Server Timeout
<input type="checkbox"/>									
<input type="checkbox"/>	1/0/1	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/2	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/3	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/4	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/5	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/6	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/7	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/8	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/9	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/10	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/11	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/12	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/13	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/14	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/15	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/16	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/17	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/18	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/19	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/20	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/21	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/22	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/23	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/24	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/25	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/26	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/27	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/28	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/29	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/30	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/31	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/32	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/33	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/34	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/35	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/36	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/37	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/38	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/39	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/40	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/41	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/42	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/43	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/44	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/45	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/46	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/47	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/48	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/49	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/50	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/51	Auto	60	30	0	90	0	30	30
<input type="checkbox"/>	1/0/52	Auto	60	30	0	90	0	30	30

1 All Go To Port

The screenshot shows a web-based configuration interface for 802.1X settings. At the top, there is a 'Go To Port' search bar with a 'GO' button. Below this is a table with 11 columns: Guest VLAN ID, Guest VLAN Period, Unauthenticated VLAN ID, Supplicant Timeout, Server Timeout, Maximum Requests, PAE Capabilities, Periodic Reauthentication, Reauthentication Period, User Privileges, and Max Users. The table contains 24 rows of data, all with identical values: Guest VLAN ID is 90, Guest VLAN Period is 0, Unauthenticated VLAN ID is 0, Supplicant Timeout is 30, Server Timeout is 30, Maximum Requests is 2, PAE Capabilities is Authenticator, Periodic Reauthentication is Disable, Reauthentication Period is 3600, User Privileges is admin,guest, and Max Users is 16. At the bottom of the table, there is another 'Go To Port' search bar with a 'GO' button.

Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID	Supplicant Timeout	Server Timeout	Maximum Requests	PAE Capabilities	Periodic Reauthentication	Reauthentication Period	User Privileges	Max Users
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16
90	0	0	30	30	2	Authenticator	Disable	3600	admin,guest,	16

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:
  - **Control Mode** - This selector lists the options for control mode. The control mode is only set if the link status of the port is link up. The options are:
    - **force unauthorized** - The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized
    - **force authorized** - The authenticator PAE unconditionally sets the controlled port to authorized.
    - **auto** - The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.
    - **mac based** - The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.
  - **Quiet Period** - This input field allows the user to configure the quiet period for the selected port. This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet period is the period for which the authenticator does not attempt to acquire a supplicant after a failed authentication exchange with the supplicant. The quiet period must be a number in the range of 0

and 65535. A quiet period value of 0 means that the authenticator state machine will never acquire a supplicant. The default value is 60. Changing the value will not change the configuration until the APPLY button is pressed.

- **Transmit Period** - This input field allows the user 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/Identity frame to the supplicant. The transmit period must be a number in the range of 1 and 65535. The default value is 30. Changing the value will not change the configuration until the APPLY button is pressed.
- **GuestVLAN Id** - This field allows the user to configure Guest Vlan Id on the interface. The valid range is 0-3965. The default value is 0. Changing the value will not change the configuration until the Apply button is pressed. Enter 0 to clear the Guest Vlan Id on the interface.
- **Guest VLAN Period** - This input field allows the user to enter the guest Vlan period for the selected port. The guest Vlan period is the value, in seconds, of the timer used by the GuestVlan Authentication. The guest Vlan time-out must be a value in the range of 1 and 300. The default value is 90. Changing the value will not change the configuration until the Apply button is pressed.
- **Unauthenticated VLAN id** - This input field allows the user to enter the Unauthenticated Vlan Id for the selected port. The valid range is 0-3965. The default value is 0. Changing the value will not change the configuration until the Submit button is pressed. Enter 0 to clear the Unauthenticated Vlan Id on the interface.
- **Supplicant Timeout** - This input field allows the user to enter the supplicant time-out for the selected port. The supplicant time-out is the value, in seconds, of the timer used by the authenticator state machine on this port to time-out the supplicant. The supplicant time-out must be a value in the range of 1 and 65535. The default value is 30. Changing the value will not change the configuration until the Apply button is pressed.
- **Server Timeout** - This input field allows the user to enter the server time-out for the selected port. The server time-out is the value, in seconds, of the timer used by the authenticator on this port to time-out the authentication server. The server time-out must be a value in the range of 1 and 65535. The default value is 30. Changing the value will not change the configuration until the APPLY button is pressed.
- **Maximum Requests** - This input field allows the user to enter the maximum requests for the selected port. The maximum requests value is the maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The maximum requests value must be in the range of 1 and 10. The default value is 2. Changing the value will not change the configuration until the APPLY button is pressed.
- **PAE Capabilities** - This field selects the port access entity (PAE) functionality of the selected port. Possible values are "Authenticator" or "Supplicant".
- **Periodic Reauthentication** - This select field allows the user to enable or disable reauthentication of the supplicant for the specified port. The selectable values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise,

reauthentication will not be allowed. The default value is false. Changing the selection will not change the configuration until the APPLY button is pressed.

- **Reauthentication Period** - This input field allows the user to enter the reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthentication period must be a value in the range of 1 and 65535. The default value is 3600. Changing the value will not change the configuration until the APPLY button is pressed.
  - **User Privileges** - This select field allows the user to add the specified user to the list of users with access to the specified port or all ports.
  - **Max Users** - This field allows the user to enter the limit to the number of supplicants on the specified interface.
3. Click **INITIALIZE** to begin the initialization sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the APPLY button for the action to occur.
  4. Click **REAUTHENTICATE** to begin the reauthentication sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the APPLY button for the action to occur.





Table 6-94.

Field	Description
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"> <li>• ForceUnauthorized</li> <li>• ForceAuthorized</li> <li>• Auto</li> <li>• N/A: If the port is in detached state it cannot participate in port access control.</li> </ul>
Reauthentication Enabled	<p>This field shows whether reauthentication of the supplicant for the specified port is allowed. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.</p>
Control Direction	<p>This displays the control direction for the specified port. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator. This affects whether the unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames) or just in the incoming direction (disabling only the reception of incoming frames). This field is not configurable on some platforms.</p>
Protocol Version	<p>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.</p>
PAE Capabilities	<p>This field displays the port access entity (PAE) functionality of the selected port. Possible values are "Authenticator" or "Supplicant". This field is not configurable.</p>
Authenticator PAE State	<p>This field displays the current state of the authenticator PAE state machine. Possible values are:</p> <ul style="list-style-type: none"> <li>• "Initialize"</li> <li>• "Disconnected"</li> <li>• "Connecting"</li> <li>• "Authenticating"</li> <li>• "Authenticated"</li> <li>• "Aborting"</li> <li>• "Held"</li> <li>• "ForceAuthorized"</li> <li>• "ForceUnauthorized".</li> </ul>

Table 6-94.

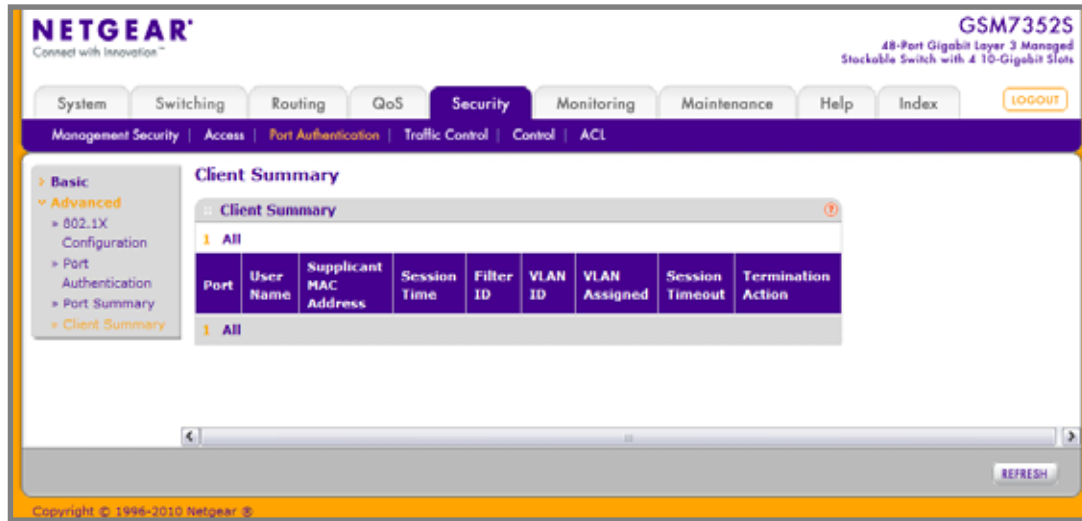
Field	Description
Backend State	<p>This field displays the current state of the backend authentication state machine. Possible values are:</p> <ul style="list-style-type: none"> <li>• “Request”</li> <li>• “Response”</li> <li>• “Success”</li> <li>• “Fail”</li> <li>• “Timeout”</li> <li>• “Initialize”</li> <li>• “Idle”</li> </ul>
Vlan Assigned	<p>This field displays the vlan id assigned to the selected interface by the Authenticator. This field is displayed only when the port control mode of the selected interface is not mac-based. This field is not configurable.</p>
Vlan Assigned Reason	<p>This field displays reason for the vlan id assigned by the authenticator to the selected interface. This field is displayed only when the port control mode of the selected interface is not mac-based. This field is not configurable. Possible values are:</p> <ul style="list-style-type: none"> <li>• “Radius”</li> <li>• “Unauth”</li> <li>• “Default”</li> <li>• “Not Assigned”</li> </ul>
Key Transmission Enabled	<p>This field displays if key transmission is enabled on the selected port. This is not a configurable field. The possible values are 'true' and 'false'. If the value is 'false' key transmission will not occur. Otherwise Key transmission is supported on the selected port.</p>
Session Timeout	<p>This field displays Session Timeout set by the Radius Server for the selected port. This field is displayed only when the port control mode of the selected port is not mac-based.</p>
Session Termination Action	<p>This field displays Termination Action set by the Radius Server for the selected port. This field is displayed only when the port control mode of the selected port is not mac-based. Possible values are:</p> <ul style="list-style-type: none"> <li>• “Default”</li> <li>• “Reauthenticate”</li> </ul> <p>If the termination action is 'default' then at the end of the session, the client details are initialized. Otherwise re-authentication is attempted.</p>

Table 6-94.

Field	Description
Port Status	This field shows the authorization status of the specified port. The possible values are 'Authorized', 'Unauthorized' and 'N/A'. If the port is in detached state, the value will be 'N/A' since the port cannot participate in port access control.
Port Method	This field shows the authorization mode of the specified port. The possible values are 'Mac based', 'Port based'.

## Client Summary

To access the Client Summary page, click **Security > Port Authentication > Advanced > Client Summary**.



**Table 6-95.**

Field	Description
Port	The port to be displayed.
User Name	This field displays the User Name representing the identity of the supplicant device.
Supplicant Mac Address	This field displays supplicant's device Mac Address.
Session Time	This field displays the time since the supplicant as logged in seconds.
Filter ID	This field displays policy filter id assigned by the authenticator to the supplicant device.
Vlan ID	This field displays vlan id assigned by the authenticator to the supplicant device.
Vlan Assigned	This field displays reason for the vlan id assigned by the authenticator to the supplicant device.
Session Timeout	This field displays Session Timeout set by the Radius Server to the supplicant device.
Termination Action	This field displays Termination Action set by the Radius Server to the supplicant device.

## 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](#) on page 481
- [Port Security](#) on page 484
- [Private Group](#) on page 490
- [Protected Ports Configuration](#) on page 492
- [Storm Control](#) on page 493

## MAC Filter

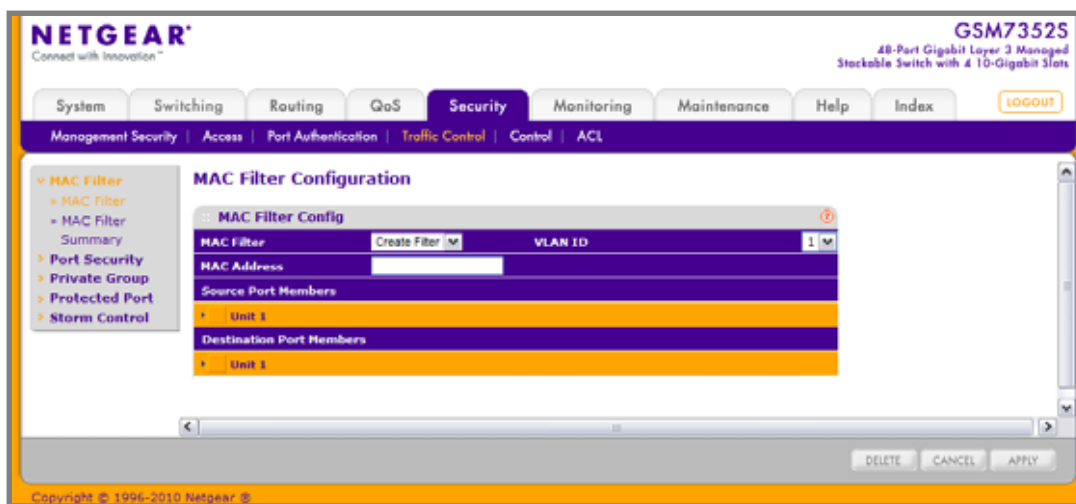
The MAC Filter folder contains links to the following features:

- [MAC Filter Configuration](#) on page 481
- [MAC Filter Summary](#) on page 483

### 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. Select Create Filter from the **MAC Filter** menu.
  - a. This is the list of MAC address and VLAN ID pairings for all configured filters. To change the port mask(s) for an existing filter, select the entry you want to change. To add a new filter, select “Create Filter” from the top of the list.
  - 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.

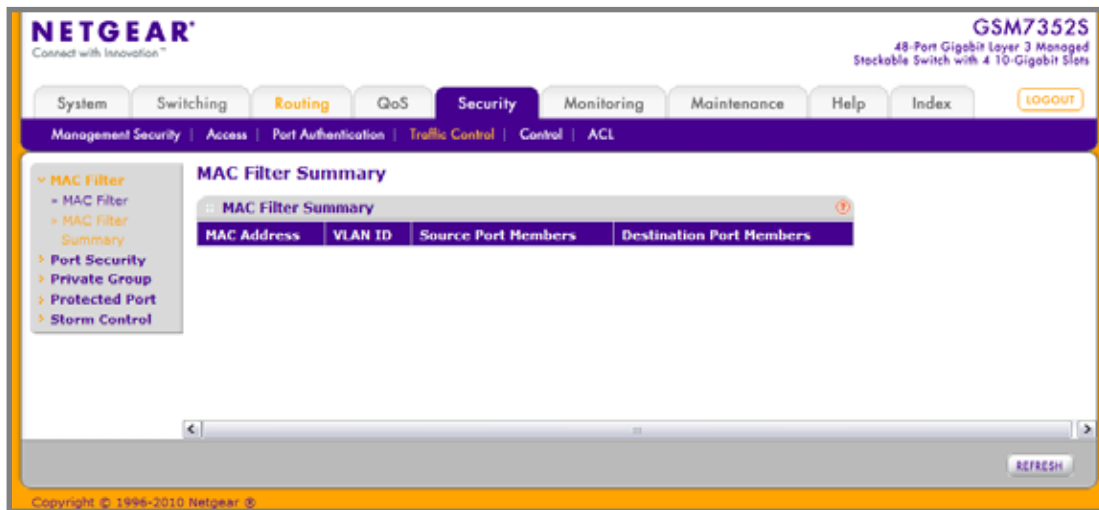
You cannot define filters for the following MAC addresses:

  - 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.
  - 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

## 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 > MAC Filter > MAC Filter Summary**.



The following table describes the information displayed on the page:

**Table 6-96.**

Field	Description
MAC Address	The MAC address of the filter in the format 00:01:1A:B2:53:4D.
VLAN ID	The VLAN ID associated with the filter.
Source Port Members	A list of ports to be used for filtering inbound packets.

## Port Security

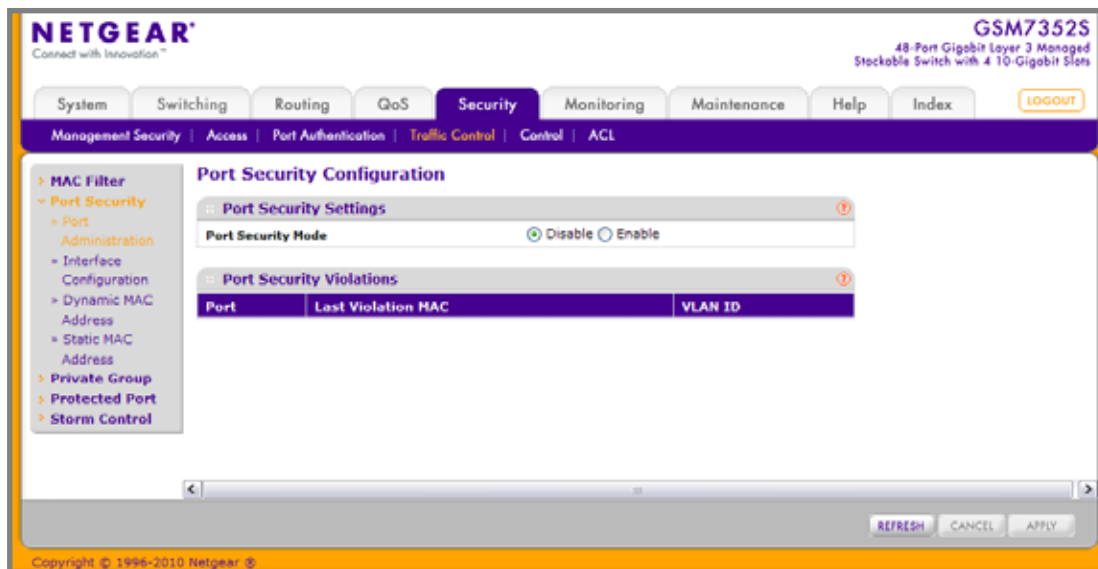
The Port Security folder contains links to the following features:

- [Port Security Configuration](#) on page 484
- [Port Security Interface Configuration](#) on page 486
- [Dynamic MAC Address](#) on page 488
- [Static MAC Address](#) on page 489

### 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 > Port Security > Port Administration**.



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.



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.

**Table 6-97.**

Field	Description
Port	Displays the physical interface for which you want to display data.
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.

## 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 > Port Security > Interface Configuration**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Management Security Access Port Authentication Traffic Control Control ACL

**Port Security Interface Configuration**

Interface Configuration

Go To Port  **GO**

	Port	Security Mode	Max Allowed Dynamically Learned MAC	Max Allowed Statically Locked MAC	Violation Trap
<input type="checkbox"/>	1/0/1	Disable	600	48	Disable
<input type="checkbox"/>	1/0/2	Disable	600	48	Disable
<input type="checkbox"/>	1/0/3	Disable	600	48	Disable
<input type="checkbox"/>	1/0/4	Disable	600	48	Disable
<input type="checkbox"/>	1/0/5	Disable	600	48	Disable
<input type="checkbox"/>	1/0/6	Disable	600	48	Disable
<input type="checkbox"/>	1/0/7	Disable	600	48	Disable
<input type="checkbox"/>	1/0/8	Disable	600	48	Disable
<input type="checkbox"/>	1/0/9	Disable	600	48	Disable
<input type="checkbox"/>	1/0/10	Disable	600	48	Disable
<input type="checkbox"/>	1/0/11	Disable	600	48	Disable
<input type="checkbox"/>	1/0/12	Disable	600	48	Disable
<input type="checkbox"/>	1/0/13	Disable	600	48	Disable
<input type="checkbox"/>	1/0/14	Disable	600	48	Disable
<input type="checkbox"/>	1/0/15	Disable	600	48	Disable

**CANCEL** **APPLY**

Copyright © 1996-2010 Netgear ©

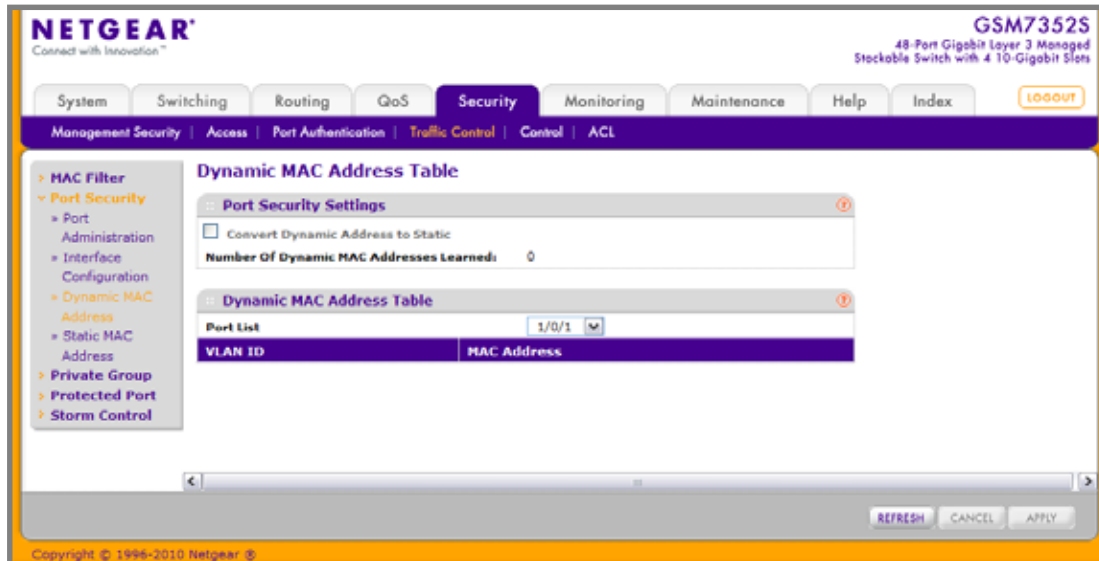
To configure port security settings:

1. **Port** - Selects the interface to be configured.
2. 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.
3. Specify the following settings:
  - **Security Mode** - Enables or disables the Port Security feature for the selected interface.
  - **Max Allowed Dynamically Learned MAC** - Sets the maximum number of dynamically learned MAC addresses on the selected interface.
  - **Max Allowed Statically Locked MAC** - Sets the maximum number of statically locked MAC addresses on the selected interface.
  - **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.

## Dynamic MAC Address

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

To display the Dynamic MAC Address page, click **Security > Traffic Control > Port Security > Dynamic MAC Address**.



To convert learned MAC addresses:

1. **Port List** - Select the physical interface for which you want to display data.
2. Use **Convert Dynamic Address to Static** to convert a dynamically learned MAC address to a statically locked address. The Dynamic MAC address entries are converted to Static MAC address entries in a numerically ascending order until the Static limit is reached.
3. Click **REFRESH** to refresh the web page to show the latest MAC address learned on a specific port.

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.

**Table 6-98.**

Field	Description
Number of Dynamic MAC Addresses Learned	Displays the number of dynamically learned MAC addresses on a specific port.
VLAN ID	Displays the VLAN ID corresponding to the MAC address.
MAC Address	Displays the MAC addresses learned on a specific port.

## Static MAC Address

To display the Static MAC Address page, click **Security > Traffic Control > Port Security > Static MAC Address**.

The screenshot displays the Netgear web interface for a GSM7352S switch. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The 'Security' tab is active, and the breadcrumb trail shows 'Management Security > Access > Port Authentication > Traffic Control > Control > ACL'. The left sidebar contains a tree view with 'MAC Filter' expanded, showing 'Port Security' and its sub-items: 'Port Administration', 'Interface Configuration', 'Dynamic MAC Address', 'Static MAC Address', 'Private Group', 'Protected Port', and 'Storm Control'. The main panel is titled 'Static MAC Address Configuration'. It features a 'Port List' section with an 'Interface' dropdown set to '1/0/1'. Below this is a 'Static MAC Address Table' with two columns: 'Static MAC Address' and 'VLAN ID'. The table is currently empty. At the bottom right of the table area are 'ADD', 'DELETE', and 'CANCEL' buttons. The footer indicates 'Copyright © 1996-2010 Netgear Inc.'

1. **Interface** - Select the physical interface for which you want to display data.
2. **Static MAC Address** - Accepts user input for the MAC address to be deleted.
3. Use **VLAN ID** to select the VLAN ID corresponding to the MAC address being added.
4. Click **ADD** to add a new static MAC address to the switch.
5. Click **DELETE** to delete a existing static MAC address from the switch.

## Private Group

The Private Group folder contains links to the following features:

- [Private Group Configuration](#) on page 490
- [Private Group Membership](#) on page 491

### Private Group Configuration

To display the Private Group Configuration page, click **Security > Traffic Control > Private Group > Private Group Configuration**.

The screenshot shows the Netgear web interface for a GSM7352S switch. The navigation menu includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Under Security, there are sub-menus for Management Security, Access, Port Authentication, Traffic Control, Control, and ACL. The left sidebar shows a tree view with 'Private Group Configuration' selected. The main content area is titled 'Private Group Configuration' and contains a table with the following structure:

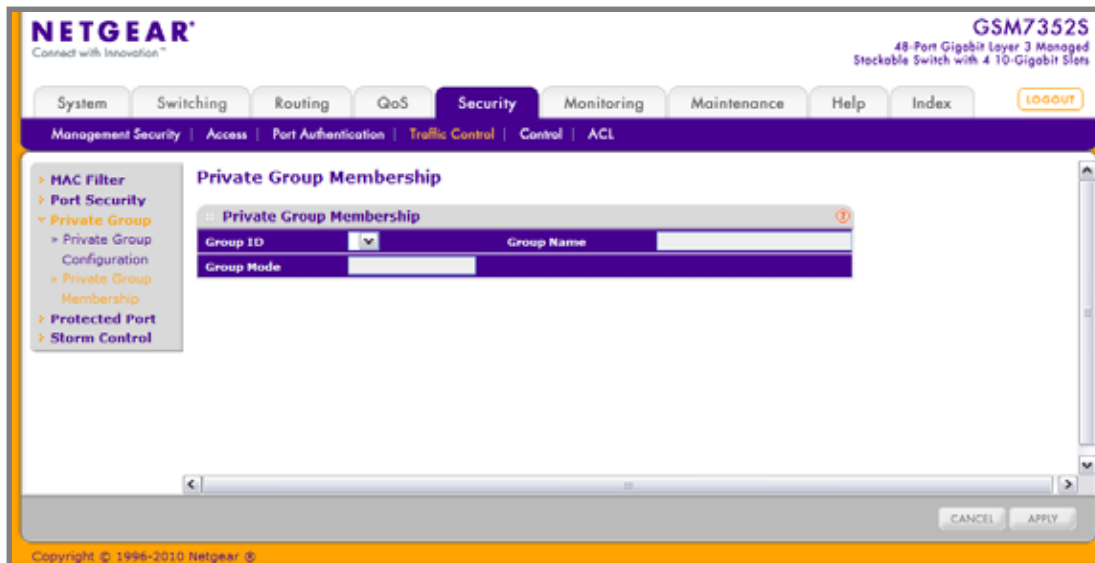
	Group Name	Group ID	Group Mode
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

At the bottom of the table are buttons for ADD, DELETE, and CANCEL. The footer of the page indicates 'Copyright © 1996-2010 Netgear'.

1. Use **Group Name** to enter the Private Group name to be configured. The name string can be up to 24 bytes of non-blank characters.
2. Use the optional **Group ID** field to specify the private group identifier. If not specified, a group id not used will be assigned automatically. The range of group id is (1 to 192).
3. Use **Group Mode** to configure the mode of private group. The group mode can be either "isolated" or "community". When in "isolated" mode, the member port in the group cannot forward its egress traffic to any other members in the same group. By default, the mode is "community" mode that each member port can forward traffic to other members in the same group, but not to members in other groups.
4. Click **ADD** to create a new private group in the switch.
5. Click **DELETE** to delete a selected private group from the switch.

## Private Group Membership

To display the Private Group Membership page, click **Security > Traffic Control > Private Group > Private Group Membership**.



1. Use **Group ID** to select the Group ID for which you want to display or configure data.
2. Use **Port List** to add the ports you selected to this private group.

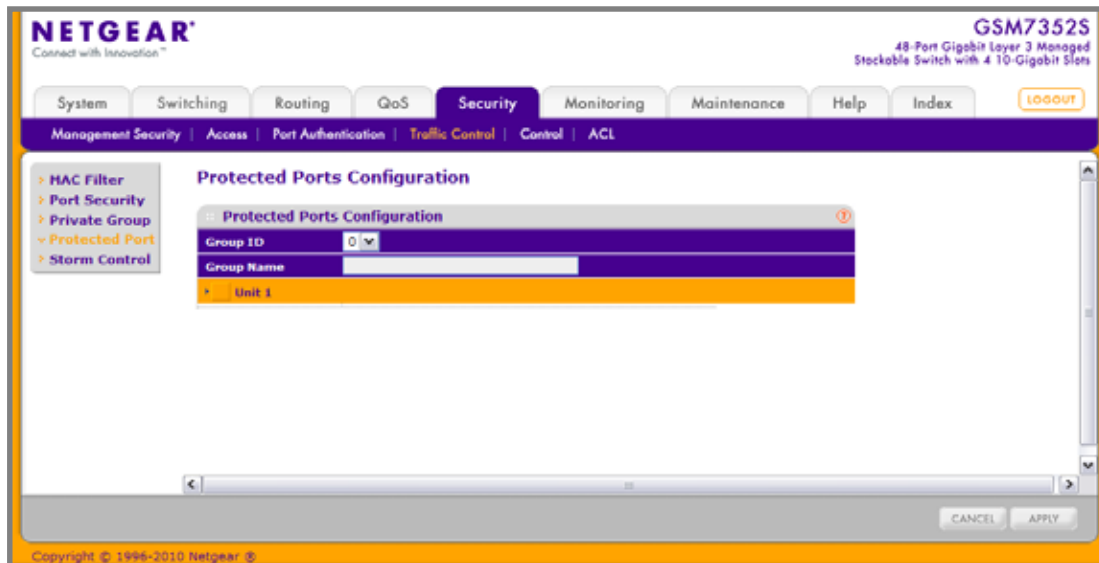
Table 6-99.

Field	Description
Group Name	This field identifies the name for the Private Group you selected. It can be up to 24 non-blank characters long.
Group Mode	<p>This field identifies the mode of the Private Group you selected. The modes are:</p> <ul style="list-style-type: none"> <li>• community</li> <li>• isolated</li> </ul> <p>The group mode can be either “isolated” or “community”. When in “isolated” mode, the member port in the group cannot forward its egress traffic to any other members in the same group. By default, the mode is “community” mode that each member port can forward traffic to other members in the same group, but not to members in other groups.</p>

## Protected Ports Configuration

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 Configuration page to configure the ports as protected or unprotected. You need read-write access privileges to modify the configuration.

To display the Protected Ports Configuration page, click the **Security > Traffic Control > Protected Ports**.



To configure protected ports:

1. Use **Group ID** to identify a group of protected ports that can be combined into a logical group. Traffic can flow between protected ports belonging to different groups, but not within the same group. The selection box lists all the possible protected port Group IDs supported for the current platform. The valid range of the Group ID is 0 to 2.
2. Use the optional **Group Name** field to associate a name with the protected ports group (used for identification purposes). It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
3. Click the orange bar to display the available ports.
4. Click the box below each port to configure as a protected port. The selection list consists of physical ports, protected as well as unprotected. The protected ports are tick-marked to differentiate between them. No traffic forwarding is possible between two protected ports. If left unconfigured, the default state is unprotected. No traffic forwarding is possible between two protected ports.
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.
7. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.



## 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.

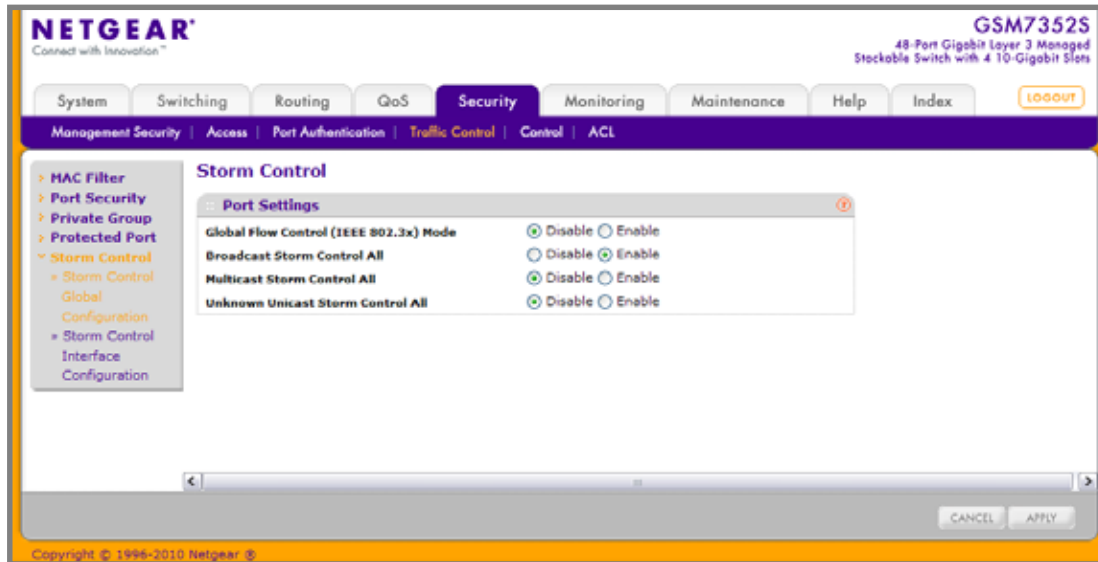
The switch measures the incoming broadcast/multicast/unknown unicast packet rate per port and discards packets when the rate exceeds the defined value. Storm control is enabled per interface, by defining the packet type and the rate at which the packets are transmitted.

The Storm Control folder contains links to the following features:

- [Storm Control Global Configuration](#) on page 494
- [Storm Control Interface Configuration](#) on page 495

## Storm Control Global Configuration

To display the Storm Control Global Configuration page, click **Security > Traffic Control > Storm Control > Storm Control Global Configuration**.



The following four control radio buttons provide an easy way to enable or disable each type of packets be rate-limited on every port in a global fashion. The effective storm control state of each port can be viewed by going to the port configuration page.

- **Global Flow Control (IEEE 802.3x) Mode** - Enable or disable this option by selecting the corresponding line on the radio button. The factory default is disabled.
- **Broadcast Storm Control All** - Enable or disable the Broadcast Storm Recovery mode on all ports by clicking the corresponding radio button. When you specify Enable for Broadcast Storm Recovery and the broadcast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. The factory default is enabled.
- **Multicast Storm Control All** - Enable or disable the Multicast Storm Recovery mode on all ports by clicking the corresponding radio button. When you specify Enable for Multicast Storm Recovery and the multicast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. The factory default is disabled.
- **Unknown Unicast Storm Control All** - Enable or disable the Unicast Storm Recovery mode on all ports by clicking the corresponding radio button. When you specify Enable for Unicast Storm Recovery and the Unicast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. The factory default is disabled.

## Storm Control Interface Configuration

To display the Storm Control Interface Configuration page, click **Security > Traffic Control > Storm Control > Storm Control Interface Configuration**.

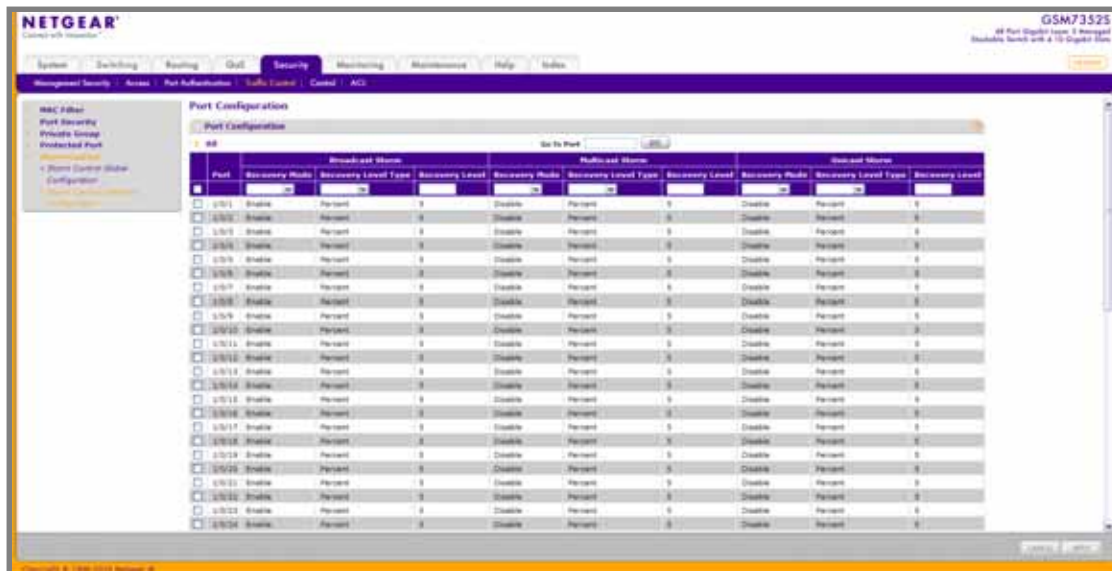


Table 6-100.

Field	Description
Broadcast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the pull-down entry field. When you specify Enable for Broadcast Storm Recovery and the broadcast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. The factory default is disabled.
Broadcast Storm Recovery Level Type	Specify the Broadcast Storm Recovery Level as a percentage of link speed or as packages per second.
Broadcast Storm Recovery Level	Specify the threshold at which storm control activates. The factory default is 5 percent of port speed for pps type.
Multicast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the pull-down entry field. When you specify Enable for Multicast Storm Recovery and the multicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. The factory default is disabled.
Multicast Storm Recovery Level Type	Specify the Multicast Storm Recovery Level as a percentage of link speed or as packages per second.
Multicast Storm Recovery Level	Specify the threshold at which storm control activates. The factory default is 5 percent of port speed for pps type.
Unicast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the pull-down entry field. When you specify Enable for Unicast Storm Recovery and the unicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. The factory default is disabled.
Unicast Storm Recovery Level Type	Specify the Unicast Storm Recovery Level as a percentage of link speed or as packages per second.
Unicast Storm Recovery Level	Specify the threshold at which storm control activates. The factory default is 5 percent of port speed for pps type.

## Control

To display the page, click the **Security > Control** tab.

The Control folder contains links to the following features:

- [\*DHCP Snooping\*](#) on page 497
- [\*IP Source Guard\*](#) on page 503
- [\*Dynamic ARP Inspection\*](#) on page 505
- [\*Captive Portal\*](#) on page 512

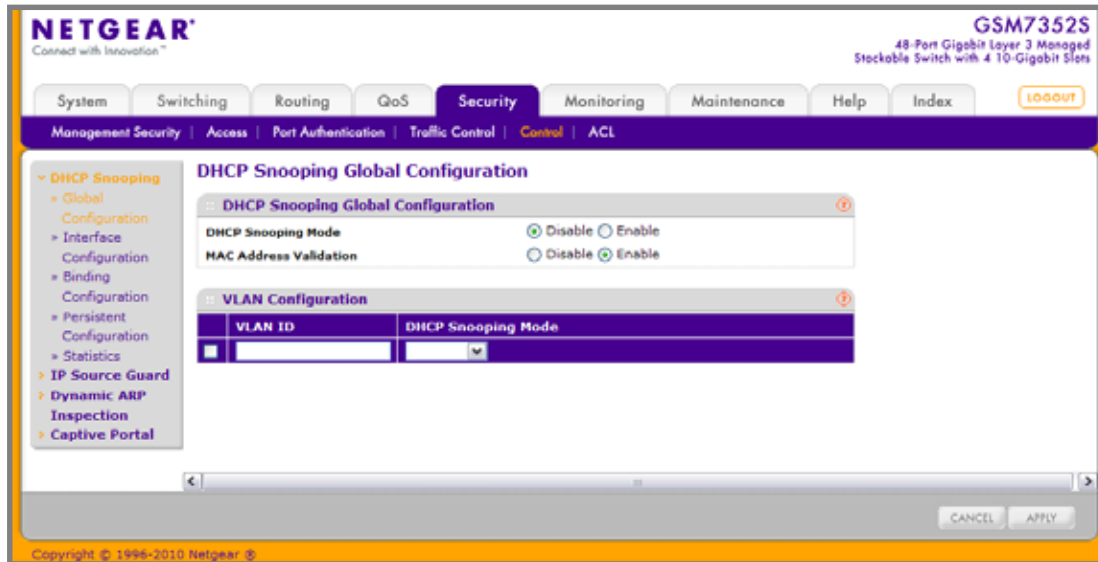
## DHCP Snooping

The DHCP Snooping folder contains links to the following features:

- [\*DHCP Snooping Global Configuration\*](#) on page 498
- [\*DHCP Snooping Interface Configuration\*](#) on page 499
- [\*DHCP Snooping Binding Configuration\*](#) on page 500
- [\*DHCP Snooping Persistent Configuration\*](#) on page 501
- [\*DHCP Snooping Statistics\*](#) on page 502

## DHCP Snooping Global Configuration

To display the DHCP Snooping Global Configuration page, click **Security > Control > DHCP Snooping > Global Configuration**.



## DHCP Snooping Configuration

1. Use **DHCP Snooping Mode** to enable or disable the DHCP Snooping feature. The factory default is disabled.
2. Use **MAC Address Validation** to enable or disable the validation of sender MAC Address for DHCP Snooping. The factory default is enabled.

## DHCP Snooping VLAN Configuration

1. Use **VLAN ID** to enter the VLAN for which the DHCP Snooping Mode is to be enabled.
2. Use **DHCP Snooping Mode** to enable or disable the DHCP Snooping feature for entered VLAN. The factory default is disabled.
3. Click **APPLY** to apply the new configuration and cause the changes to take effect. These changes will not be retained across a power cycle unless a save configuration is performed.

## DHCP Snooping Interface Configuration

To display the DHCP Snooping Interface Configuration page, click **Security > Control > DHCP Snooping > Interface Configuration**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security Access Port Authentication Traffic Control **Control** ACL

**DHCP Snooping**

- Global Configuration
- Interface Configuration
- Binding Configuration
- Persistent Configuration
- Statistics
- IP Source Guard
- Dynamic ARP Inspection
- Captive Portal

### DHCP Snooping Interface Configuration

1 All Go To Interface  GO

Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
<input type="checkbox"/> 1/0/1	Disable	Disable	15	1
<input type="checkbox"/> 1/0/2	Disable	Disable	15	1
<input type="checkbox"/> 1/0/3	Disable	Disable	15	1
<input type="checkbox"/> 1/0/4	Disable	Disable	15	1
<input type="checkbox"/> 1/0/5	Disable	Disable	15	1
<input type="checkbox"/> 1/0/6	Disable	Disable	15	1
<input type="checkbox"/> 1/0/7	Disable	Disable	15	1
<input type="checkbox"/> 1/0/8	Disable	Disable	15	1
<input type="checkbox"/> 1/0/9	Disable	Disable	15	1
<input type="checkbox"/> 1/0/10	Disable	Disable	15	1
<input type="checkbox"/> 1/0/11	Disable	Disable	15	1
<input type="checkbox"/> 1/0/12	Disable	Disable	15	1
<input type="checkbox"/> 1/0/13	Disable	Disable	15	1
<input type="checkbox"/> 1/0/14	Disable	Disable	15	1
<input type="checkbox"/> 1/0/15	Disable	Disable	15	1
<input type="checkbox"/> 1/0/16	Disable	Disable	15	1
<input type="checkbox"/> 1/0/17	Disable	Disable	15	1
<input type="checkbox"/> 1/0/18	Disable	Disable	15	1
<input type="checkbox"/> 1/0/19	Disable	Disable	15	1

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

1. **Interface** - Selects the interface for which data is to be configured.
2. If **Trust Mode** is enabled, DHCP snooping application considers as port trusted. The factory default is disabled.
3. If **Logging Invalid Packets** is enabled, DHCP snooping application logs invalid packets on this interface. The factory default is disabled.
4. Use **Rate Limit(pps)** to specify 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 None there is no limit. The factory default is 15pps (packets per second). The range of Rate Limit is (0 to 300).
5. Use **Burst Interval(secs)** to specify the burst interval value for rate limiting purpose on this interface. If the rate limit is None burst interval has no meaning shows it as N/A. The factory default is 1 second. The range of Burst Interval is 1 to 15).

## DHCP Snooping Binding Configuration

To display the DHCP Snooping Binding Configuration page, click **Security > Control > DHCP Snooping > Binding Configuration**.

### Static Binding Configuration

1. **Interface** - Selects the interface to add a binding into the DHCP snooping database.
2. Use **MAC Address** to specify the MAC address for the binding to be added. This is the Key to the binding database.
3. Use **VLAN ID** to select the VLAN from the list for the binding rule. The range of the VLAN ID is (1 to 4093).
4. Use **IP Address** to specify valid IP Address for the binding rule.
5. Click **ADD** to add DHCP snooping binding entry into the database.
6. Click **DELETE** to delete selected static entries from the database.

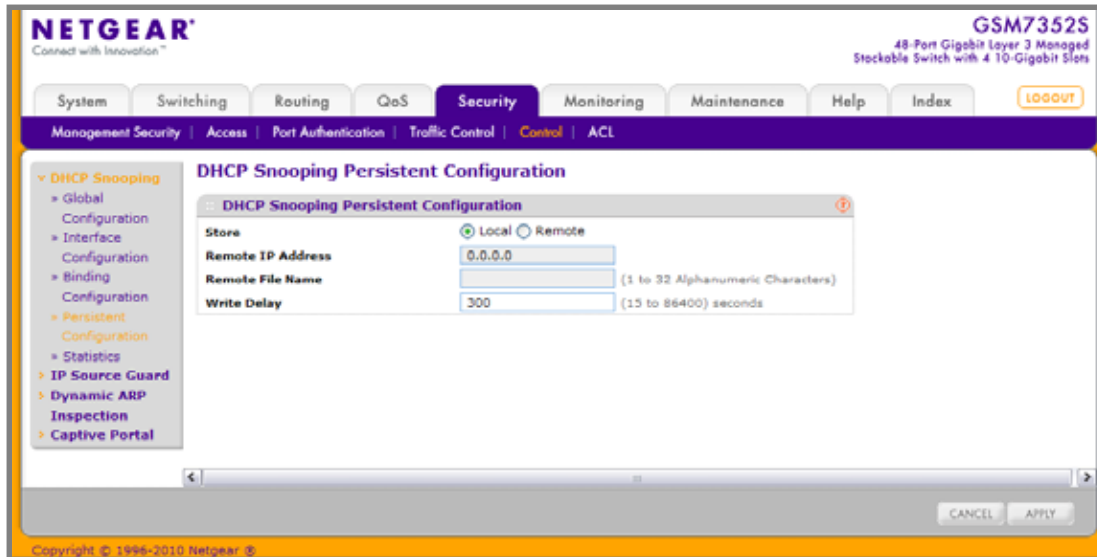
### Dynamic Binding Configuration

1. **Interface** - Displays the interface to which a binding entry in the DHCP snooping database.
2. Use **MAC Address** to display the MAC address for the binding in the binding database.
3. Use **VLAN ID** to display the VLAN for the binding entry in the binding database. The range of the VLAN ID is (1 to 4093).
4. **IP Address** - Displays IP Address for the binding entry in the binding database.
5. **Lease Time** - Displays the remaining Lease time for the Dynamic entries
6. Click **CLEAR** to delete all DHCP Snooping binding entries.



## DHCP Snooping Persistent Configuration

To display the DHCP Snooping Persistent Configuration page, click **Security > Control > DHCP Snooping > Persistent Configuration**.



1. Use **Store** to select the local store or remote store. Local selection disable the Remote objects like Remote File Name and Remote IP address.
2. Use **Remote IP Address** to configure Remote IP Address on which the snooping database will be stored when Remote is selected.
3. Use **Remote File Name** to configure Remote file name to store the database when Remote is selected.
4. Use **Write Delay** to configure the maximum write time to write the database into local or remote. The range of Write Delay is 15 to 86400.

## DHCP Snooping Statistics

To display the DHCP Snooping Statistics page, click **Security** > **Control** > **DHCP Snooping** > **Statistics**.

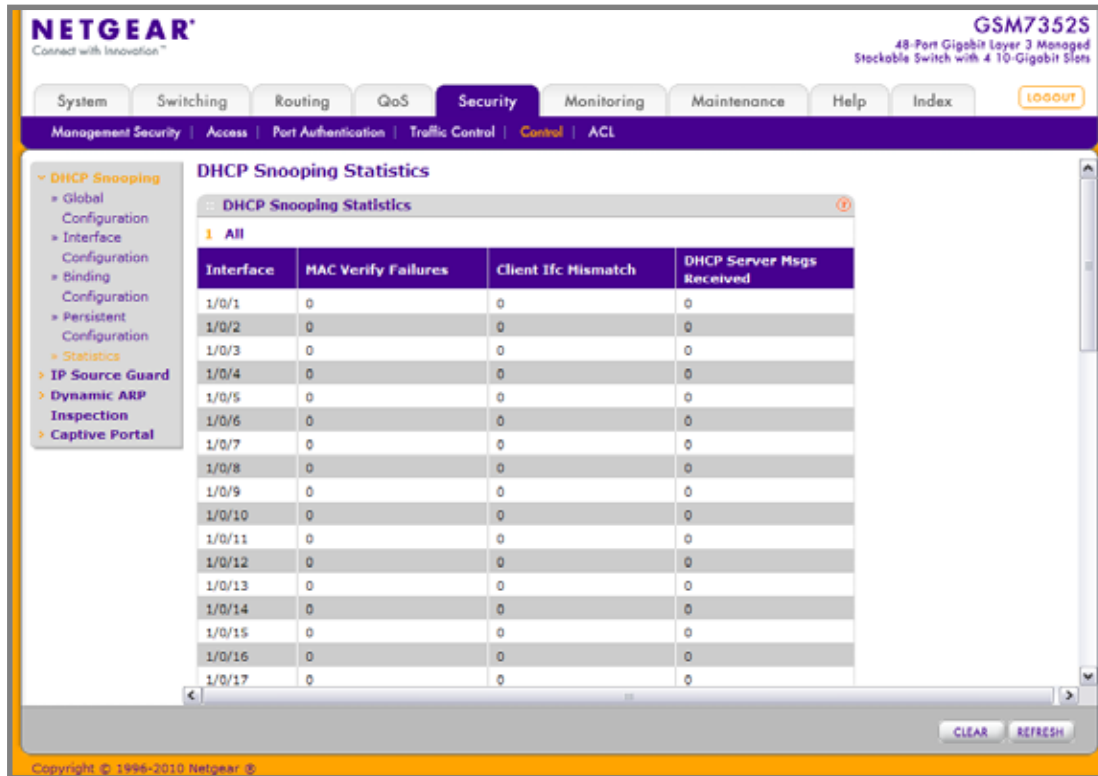


Table 6-101.

Field	Description
Interface	The untrusted and snooping enabled interface for which statistics to be displayed.
MAC Verify Failures	Number of packets that were dropped by DHCP Snooping as there is no matching DHCP Snooping binding entry found.
Client Ifc Mismatch	The number of DHCP messages that are dropped based on source MAC address and client HW address verification.
DHCP Server Msgs Received	The number of Server messages that are dropped on an un trusted port.

Click **CLEAR** to clear all interfaces statistics.

Click **REFRESH** to refresh the data on the screen with the latest statistics.

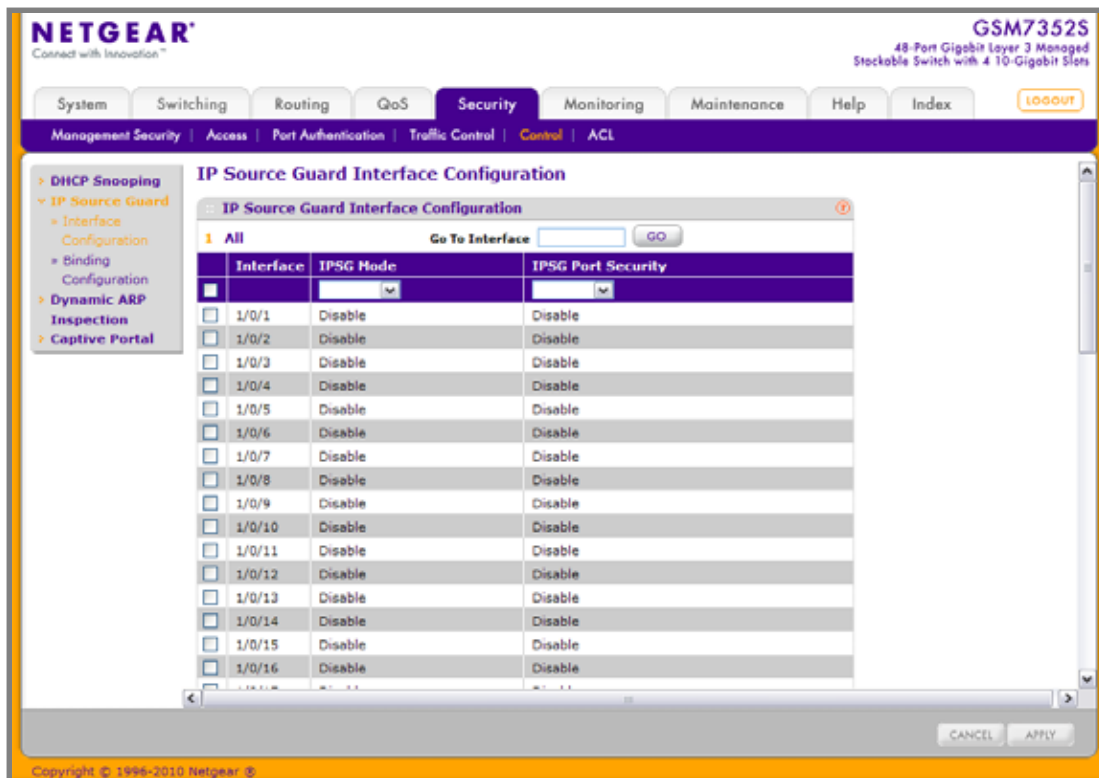
## IP Source Guard

The IP Source Guard folder contains links to the following features:

- [IP Source Guard Interface Configuration](#) on page 503
- [IP Source Guard Binding Configuration](#) on page 504

### IP Source Guard Interface Configuration

To display the IP Source Guard Interface Configuration page, click **Security > Control > IP Source Guard > Interface Configuration**.



1. **Interface** - Selects the interface to enable IPSG.
2. Use **IPSG Mode** to enable or disable validation of Sender IP Address on this interface. If IPSG is Enabled Packets will not be forwarded if Sender IP Address is not in DHCP Snooping Binding database. The factory default is disabled.
3. Use **IPSG Port Security** to enable or disables the IPSG Port Security on the selected interface. If IPSG Port Security is enabled then the packets will not be forwarded if the sender MAC Address is not in FDB table and it is not in DHCP snooping binding database. To enforce filtering based on MAC address other required configurations are:
  - Enable port-security Globally.
  - Enable port-security on the interface level.

IPSG Port Security can't be Enabled if IPSG is Disabled. The factory default is disabled.

## IP Source Guard Binding Configuration

To display the IP Source Guard Binding Configuration page, click **Security > Control > IP Source Guard > Binding Configuration**.

The screenshot shows the Netgear web interface for a GSM7352S switch. The 'Security' tab is selected, and the 'IP Source Guard' configuration page is displayed. The 'Binding Configuration' section is active, showing two tables for static and dynamic bindings. The static binding table has columns for Interface, MAC Address, VLAN ID, IP Address, and Filter Type. The dynamic binding table has the same columns. At the bottom, there are buttons for ADD, DELETE, CLEAR, and CANCEL.

### Static Binding Configuration

1. **Interface** - Selects the interface to add a binding into the IPSG database.
2. Use **MAC Address** to specify the MAC address for the binding.
3. Use **VLAN ID** to select the VLAN from the list for the binding rule.
4. Use **IP Address** to specify valid IP Address for the binding rule.
5. Click **ADD** to add IPSG static binding entry into the database.
6. Click **DELETE** to delete selected static entries from the database.

Table 6-102.

Field	Description
Interface	Displays the interface to add a binding into the IPSG database.
MAC Address	Displays the MAC address for the binding entry.
VLAN ID	Displays the VLAN from the list for the binding entry.
IP Address	Displays valid IP Address for the binding entry.
Filter Type	Filter Type using on the interface. one is source IP address filter type, the other is source IP address and MAC address filter type.

Click **CLEAR** to clear all the dynamic binding entries.

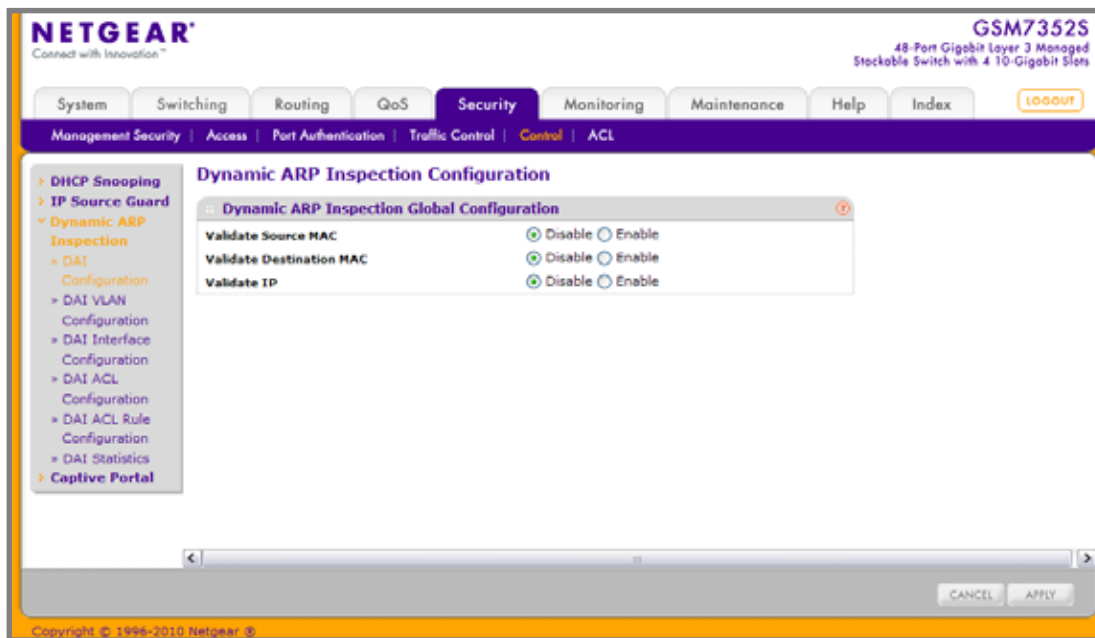
## Dynamic ARP Inspection

The Dynamic ARP Inspection (DAI) folder contains links to the following features:

- [DAI Configuration](#) on page 505
- [DAI VLAN Configuration](#) on page 506
- [DAI Interface Configuration](#) on page 507
- [DAI ACL Configuration](#) on page 508
- [DAI ACL Rule Configuration](#) on page 509
- [DAI Statistics](#) on page 510

### DAI Configuration

To display the DAI Configuration page, click **Security > Control > Dynamic ARP Inspection > DAI Configuration**.



1. Use **Validate Source MAC** to choose the DAI Source MAC Validation Mode for the switch by selecting Enable or Disable radio button. If you select Enable, Sender MAC validation for the ARP packets will be enabled. The factory default is disable.
2. Use **Validate Destination MAC** to choose the DAI Destination MAC Validation Mode for the switch by selecting Enable or Disable radio button. If you select Enable, Destination MAC validation for the ARP Response packets will be enabled. The factory default is disable.
3. Use **Validate IP** to choose the DAI IP Validation Mode for the switch by selecting Enable or Disable radio button. If you select Enable, IP Address validation for the ARP packets will be enabled. The factory default is disable.

## DAI VLAN Configuration

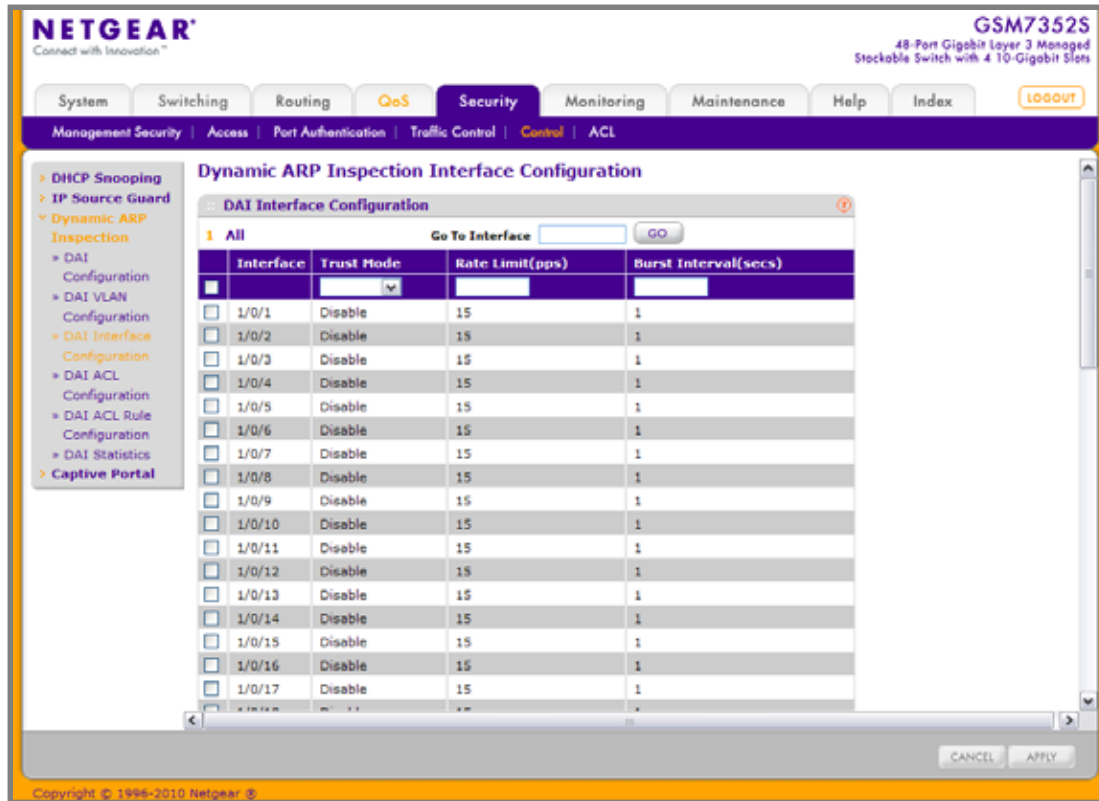
To display the DAI VLAN Configuration page, click **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**.

VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
1	Disable	Enable		Disable

1. **VLAN ID** - Select the DAI Capable VLANs for which information has to be displayed or configured.
2. Use **Dynamic ARP Inspection** to indicate whether the Dynamic ARP Inspection is enabled on this VLAN. If this object is set to 'Enable' Dynamic ARP Inspection is enabled. If this object is set to 'Disable', Dynamic ARP Inspection is disabled.
3. Use **Logging Invalid Packets** to indicate whether the Dynamic ARP Inspection logging is enabled on this VLAN. If this object is set to 'Enable' it will log the Invalid ARP Packets information. If this object is set to 'Disable', Dynamic ARP Inspection logging is disabled.
4. Use **ARP ACL Name** to specify a name for the ARP Access list. A vlan can be configured to use this ARP ACL containing rules as the filter for ARP packet validation. The name can contain up to <1-31> alphanumeric characters.
5. Use **Static Flag** to determine whether the ARP packet needs validation using the DHCP snooping database in case ARP ACL rules don't match. If the flag is enabled then the ARP Packet will be validated by the ARP ACL Rules only. If the flag is disabled then the ARP Packet needs further validation by using the DHCP Snooping entries. The factory default is disable.

## DAI Interface Configuration

To display the DAI Interface Configuration page, click **Security > Control > Dynamic ARP Inspection > DAI Interface Configuration**.

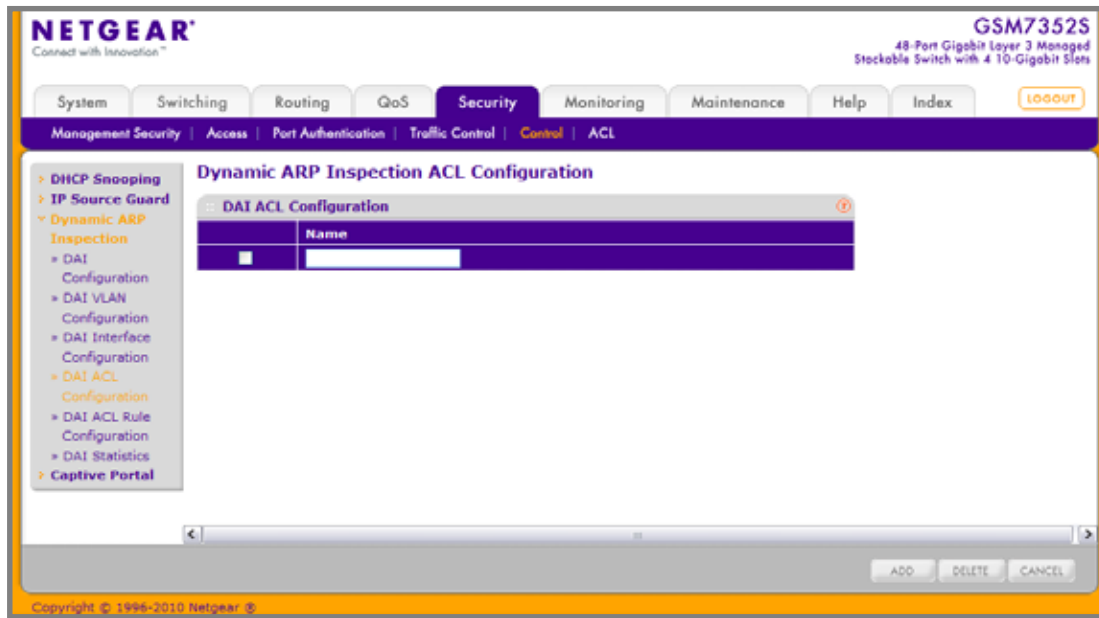


1. **Interface** - Selects the physical interface for which data is to be configured.
2. Use **Trusted State** to indicate whether the interface is trusted for Dynamic ARP Inspection purpose. If this object is set to 'Enable', the interface is trusted. ARP packets coming to this interface will be forwarded without checking. If this object is set to 'Disable', the interface is not trusted. ARP packets coming to this interface will be subjected to ARP inspection. The factory default is disable.
3. Use **Rate Limit(pps)** to specify rate limit value for Dynamic ARP Inspection purpose. If the incoming rate of ARP packets exceeds the value of this object for consecutively burst interval seconds, ARP packets will be dropped. If this value is None there is no limit. The factory default is 15pps (packets per second).
4. Use **Burst Interval(secs)** to specify the burst interval value for rate limiting purpose on this interface. If the rate limit is None burst interval has no meaning shows it as N/A. The factory default is 1 second.

## DAI ACL Configuration

This screen shows the ARP ACLs configured.

To display the DAI ACL Configuration page, click **Security > Control > Dynamic ARP Inspection > DAI ACL Configuration**.



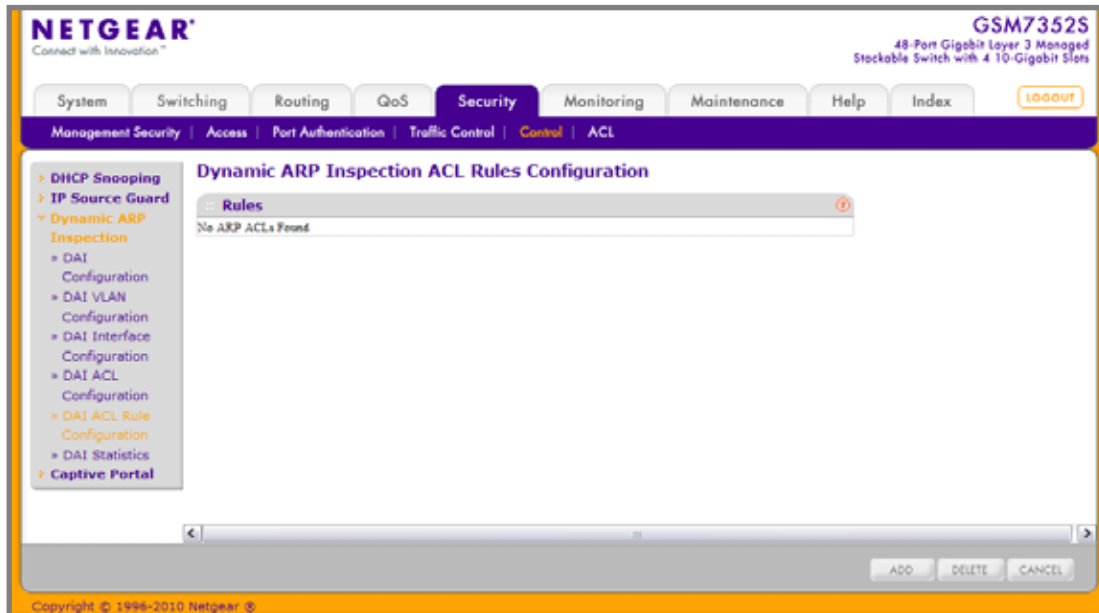
1. Use **Name** to create New ARP ACL for DAI.
2. Click **ADD** to add a new DAI ACL to the switch configuration.
3. Click **DELETE** to remove the currently selected DAI ACL from the switch configuration.



## DAI ACL Rule Configuration

This screen shows the Rules for selected DAI ARP ACL.

To display the DAI ACL Rule Configuration page, click **Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration**.



1. **ACL Name** - Selects the DAI ARP ACL for which information want to be displayed or configured.
2. Click **ADD** to add a new Rule to the selected ACL.
3. Click **DELETE** to remove the currently selected Rule from the selected ACL.

Table 6-103.

Field	Description
Source IP Address	This indicates Sender IP address match value for the DAI ARP ACL.
Source MAC Address	This indicates Sender MAC address match value for the DAI ARP ACL.

## DAI Statistics

This screen shows the Statistics per VLAN.

To display the DAI Statistics page, click **Security > Control > Dynamic ARP Inspection > DAI Statistics**.

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Management Security Access Port Authentication Traffic Control **Control** ACL

**Dynamic ARP Inspection Statistics**

**DAI Statistics**

VLAN	DHCP Drops	DHCP Permits	ACL Drops	ACL Permits	Bad Source MAC	Bad Dest MAC	Invalid IP	Forwarded	Dropped
1	0	0	0	0	0	0	0	0	0

CLEAR REFRESH

Copyright © 1996-2010 Netgear, Inc.

Table 6-104.

Field	Description
VLAN	The enabled VLAN ID for which statistics to be displayed.
DHCP Drops	Number of ARP packets that were dropped by DAI as there is no matching DHCP Snooping binding entry found.
DHCP Permits	Number of ARP packets that were forwarded by DAI as there is a matching DHCP Snooping binding entry found.
ACL Drops	Number of ARP packets that were dropped by DAI as there is no matching ARP ACL rule found for this VLAN and the static flag is set on this VLAN.
ACL Permits	Number of ARP packets that were permitted by DAI as there is a matching ARP ACL rule found for this VLAN.
Bad Source MAC	Number of ARP packets that were dropped by DAI as the sender MAC address in ARP packet didn't match the source MAC in ethernet header.
Bad Dest MAC	Number of ARP packets that were dropped by DAI as the target MAC address in ARP reply packet didn't match the destination MAC in ethernet header.
Invalid IP	Number of ARP packets that were dropped by DAI as the sender IP address in ARP packet or target IP address in ARP reply packet is invalid. Invalid addresses include 0.0.0.0, 255.255.255.255, IP multicast addresses, class E addresses (240.0.0.0/4), loopback addresses (127.0.0.0/8).
Forwarded	Number of valid ARP packets forwarded by DAI.
Dropped	Number of invalid ARP packets dropped by DAI.

Click **CLEAR** to clear the DAI statistics.

Click **REFRESH** to refresh the data on the screen with the latest DAI statistics.

## Captive Portal

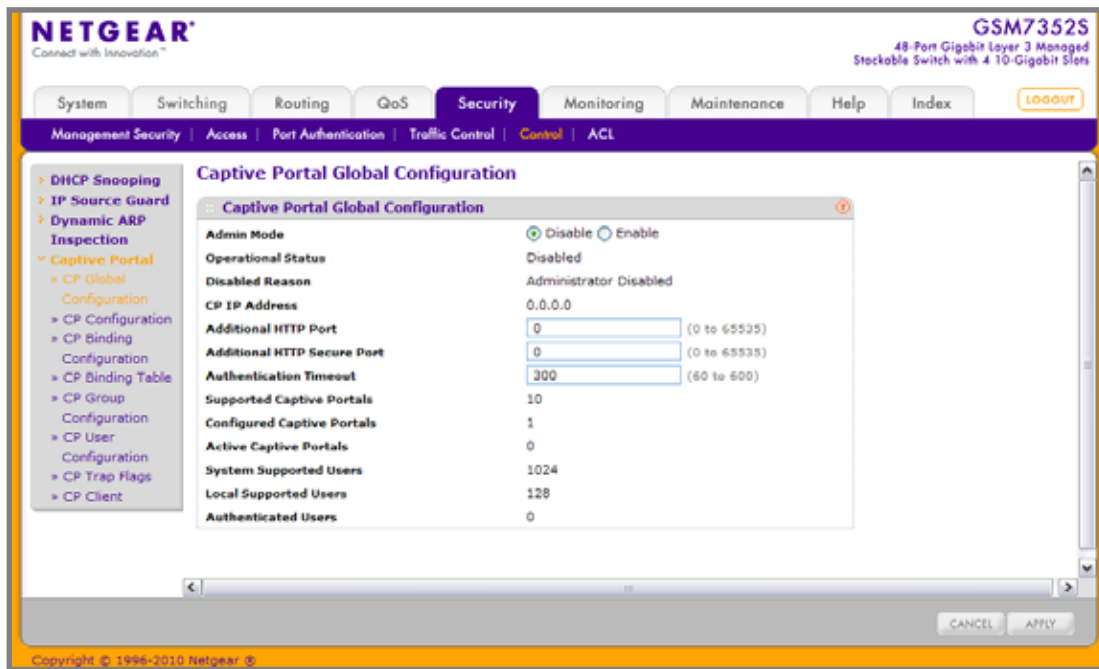
The Captive Portal folder contains links to the following features:

- [\*Captive Portal Global Configuration\*](#) on page 513
- [\*Captive Portal Configuration\*](#) on page 515
- [\*Captive Portal Binding Configuration\*](#) on page 517
- [\*Captive Portal Binding Table\*](#) on page 518
- [\*Captive Portal Group Configuration\*](#) on page 519
- [\*Captive Portal User Configuration\*](#) on page 520
- [\*Captive Portal Trap Flags\*](#) on page 522
- [\*Captive Portal Client\*](#) on page 523

## Captive Portal Global Configuration

Using the Captive Portal Global Configuration page, you can control the administrative state of the CP feature and configure global settings that affect all captive portals configured on the switch.

To display the Captive Portal Global Configuration page, click **Security > Control > Captive Portal > CP Global Configuration**.



1. Use **Admin Mode** to enable or disable Captive Portal feature. By default, the Captive Portal feature is disabled.
2. Use **Additional HTTP Port** to configure an additional port for HTTP traffic (HTTP traffic uses port 80), but you can configure an additional port for HTTP traffic. Enter a port number between 0-65535 (excluding port 80). Enter 0 to unconfigure the Additional HTTP Port. Default is 0.
3. Use **Additional HTTP Secure Port** to configure an additional port for HTTP Secure traffic (HTTP Secure traffic uses port 443). Enter a port number between 0-65535 (excluding port 443). Enter 0 to unconfigure the Additional HTTP Secure Port. Default is 0.
4. Use **Authentication Timeout** to specify the number of seconds to keep the authentication session open with the client. To access the network through a portal, the client must first enter authentication information on an authentication Web page. When the time-out expires, the switch disconnects any active TCP or SSL connection with the client. The valid range is 60 to 600 seconds. Default Authentication Timeout is 300 seconds.

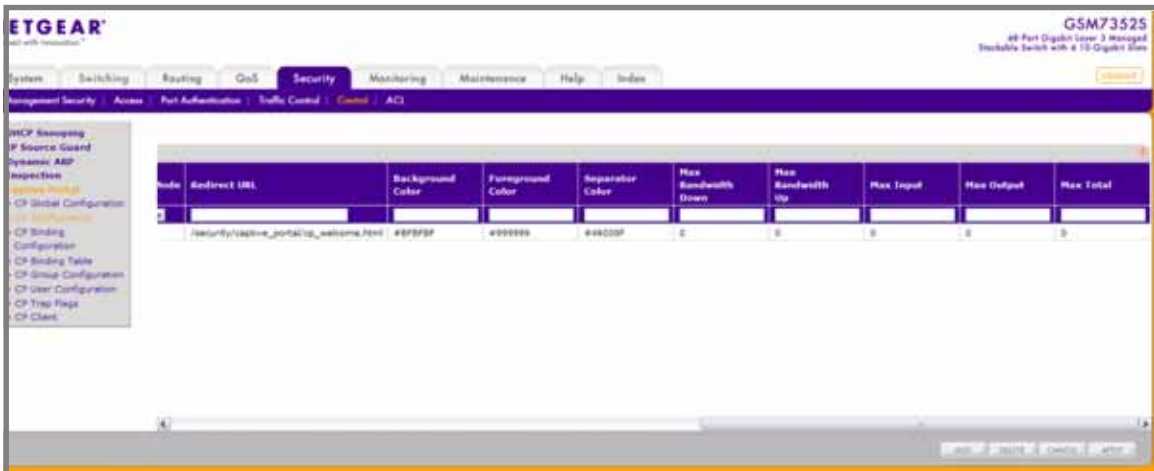
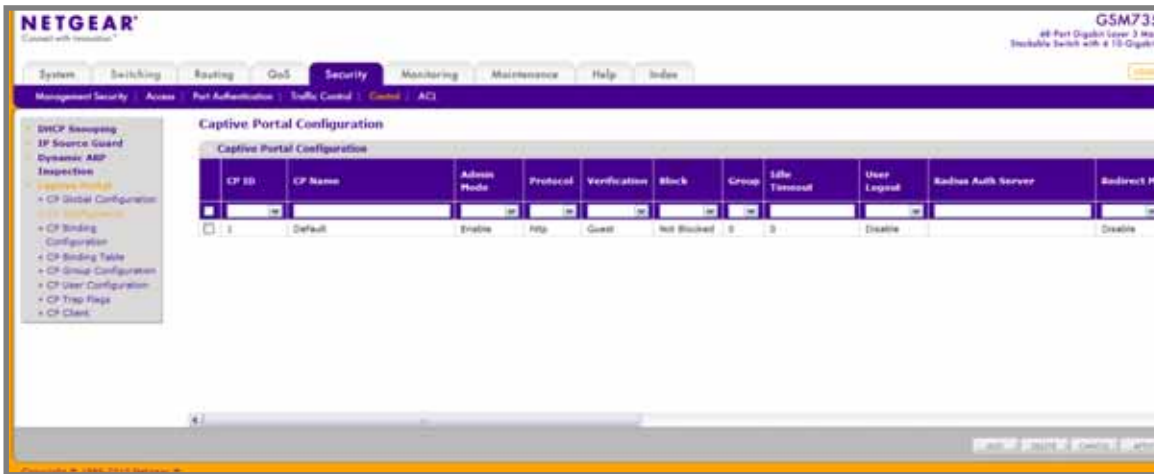
**Table 6-105.**

Field	Description
Operational Status	Shows whether the CP feature is Enabled or Disabled. Default is Disabled.
Disabled Reason	If CP is disabled, this field displays the reason, which can be one of the following: <ul style="list-style-type: none"> <li>• Administrator Disabled.</li> <li>• IP Address Not Configured.</li> <li>• No IP Routing Interface.</li> <li>• Routing Disabled.</li> </ul>
CP IP Address	Shows the captive portal IP address.
Supported Captive Portals	Shows the number of supported captive portals in the system.
Configured Captive Portals	Shows the number of captive portals configured on the switch.
Active Captive Portals	Shows the number of captive portal instances that are operationally enabled.
System Supported Users	Shows the number of authenticated users that the system can support.
Local Supported Users	Shows the number of entries that the Local User database supports.
Authenticated Users	Shows the number of users currently authenticated to all captive portal instances on this switch.

## Captive Portal Configuration

By default, the switch has one captive portal. You can change the settings for that captive portal, and you can also create and configure up to nine additional portals.

To display the Captive Portal Configuration page, click **Security > Control > Captive Portal > CP Configuration**. (Shown in two figures below.)



1. Use the **CP ID** pull-down menu to select the CP ID for which to create or update.
2. Use **CP Name** to enter the name of the configuration. Name can contain 1 to 31 alphanumeric characters.
3. Use **Admin Mode** to enable or disable this CP instance.
4. Use **Protocol** to choose whether to use HTTP or HTTPS as the protocol for the portal to use during the verification process:
  - **HTTP** - Does not use encryption during verification.
  - **HTTPS** - Uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption. The certificate is presented to the user at connection time.

5. Use **Verification** to select the mode for the CP to use to verify clients:
  - **Guest** - The user does not need to be authenticated by a database.
  - **Local** - The switch uses a local database to authenticated users.
  - **RADIUS** - The switch uses a database on a remote RADIUS server to authenticate users.
6. Use **Block** to control the blocked status. If the CP is blocked, users cannot gain access to the network through the CP. Use this function to temporarily protect the network during unexpected events, such as denial of service attacks.
7. If the **Verification Mode** is Local or RADIUS, use Group to assign an existing User Group to the captive portal. All users who belong to the group are permitted to access the network through this portal. The User Group list is the same for all CP configurations on the switch.
8. Use **Idle Timeout** to enter the number of seconds to wait before terminating a session. A user is logged out once the idle time-out is reached. If the value is set to 0 then the time-out is not enforced. The valid range is 0 to 86400 seconds and the default value is 0.
9. Use **User Logout** to allow the authenticated client to deauthenticate from the network.
10. Use **Radius Auth Server** to enter the IP address of the RADIUS server used for client authentications. The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the clients.
11. Use **Redirect URL** to specify the URL to which the newly authenticated client is redirected. The max length for the URL is 512 alphanumeric characters.
12. Use **Background Color** to specify the value of the background color. Example: #BFBFBF.
13. Use **Foreground Color** to specify the value of the foreground color. Example: #999999.
14. Use **Separator Color** to specify the value of the separator color. Example: #46008F.
15. Use **Max Bandwidth Down** to specify the maximum rate (Rate in bytes per seconds) at which a client can receive data from the network. 0 indicates limit not enforced (Range: 0 – 536870911).
16. Use **Max Bandwidth Up** to specify the maximum rate (Rate in bytes per seconds) at which a client can send data into the network. 0 indicates limit not enforced (Range: 0 – 536870911).
17. Use **Max Input** to specify the maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. 0 indicates limit not enforced (Range: 0 – 4294967295).
18. Use **Max Output** to specify the maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. 0 indicates limit not enforced (Range: 0 – 4294967295).
19. Use **Max Total** to specify the maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. 0 indicates limit not enforced (Range: 0 – 4294967295).
20. Click **ADD** to add a new CP instance.
21. Click **DELETE** to remove the currently selected CP instance.



## Captive Portal Binding Configuration

You can associate a configured captive portal with a specific network (SSID). The CP feature only runs on the interfaces you specify. A CP can have multiple interfaces associated with it, but an interface can be associated to only one CP at a time.

To display the Captive Portal Global Configuration page, click **Security > Control > Captive Portal > CP Binding Configuration**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security Access Port Authentication Traffic Control **Control** ACL

**Captive Portal Binding Configuration**

CP ID: 1 CP Name: Default

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																				

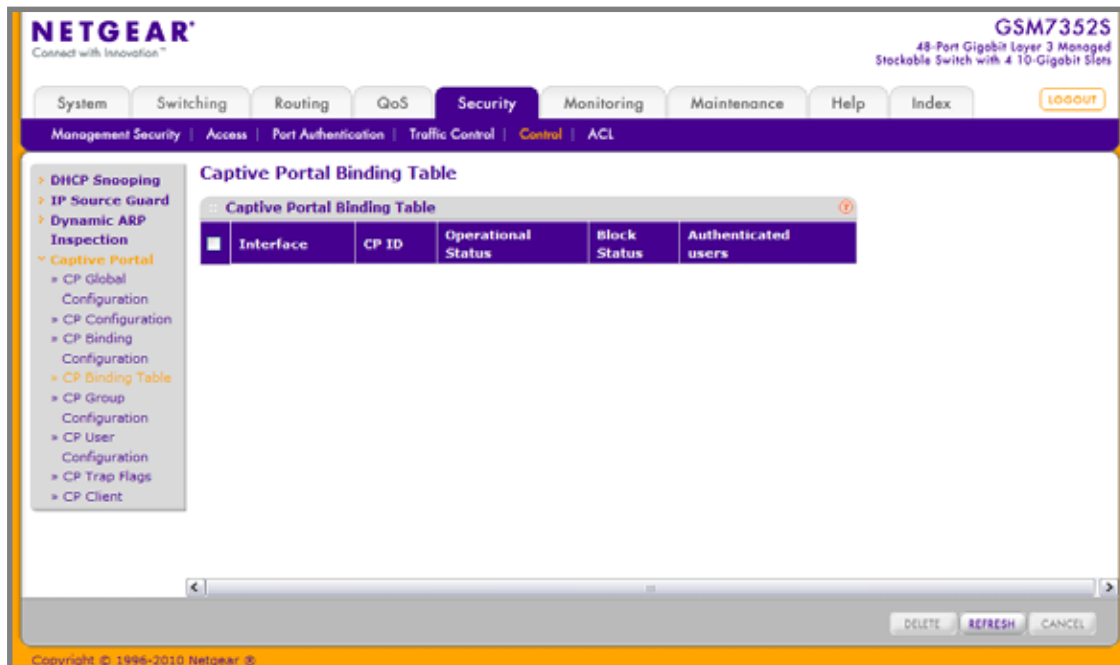
CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

1. Use the **CP ID** pull-down list to select the CP ID for which to create or update a CP instance.
2. Use **CP Name** to enter the name of the configuration. Name can contain 1 to 31 alphanumeric characters.
3. Use **Port List** to select the interface or interfaces.

## Captive Portal Binding Table

To display the Captive Portal Binding Table page, click **Security > Control > Captive Portal > CP Binding Table**.



Click **DELETE** to remove the currently selected interface.

**Table 6-106.**

Field	Description
Interface	The interface for which you want to view information.
CP ID	The ID of captive portal instance.
Operational Status	Shows whether the portal is active on the specified interface.
Block Status	Indicates whether the captive portal is temporarily blocked for authentications.
Authenticated users	Displays the number of authenticated users using the captive portal instance on this interface.

## Captive Portal Group Configuration

When you click **Add** from the CP Group Configuration page, the screen refreshes, and you can add a new group to the User Group database.

To display the Captive Portal Group Configuration page, click **Security > Control > Captive Portal > CP Group Configuration**.

The screenshot shows the Netgear web interface for a GSM7352S switch. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Security tab is active, and the sub-menu shows Management Security, Access, Port Authentication, Traffic Control, Control, and ACL. The Control tab is selected, leading to the CP Group Configuration page.

The CP Group Configuration page features a sidebar with a tree view of configuration options: DHCP Snooping, IP Source Guard, Dynamic ARP Inspection, Captive Portal (expanded), CP Global Configuration, CP Configuration, CP Binding Configuration, CP Binding Table, CP Group Configuration (highlighted), CP User Configuration, CP Trap Flags, and CP Client.

The main content area is titled "CP Group Configuration" and contains a table with two columns: Group ID and Group Name. The table has one row with Group ID "1" and Group Name "Default". Below the table are buttons for ADD, DELETE, CANCEL, and APPLY.

Group ID	Group Name
1	Default

1. Use the **Group ID** pull down menu to select the Group ID for which to create or update a group.
2. Use **Group Name** to enter the name of the user group. Name can contain 1 to 31 alphanumeric characters.
3. Click **ADD** to add a new group.
4. Click **DELETE** to remove the currently selected group.

## Captive Portal User Configuration

When you click **Add** from the CP User Configuration page, the screen refreshes, and you can add a new user to the Local User database.

To display the Captive Portal User Configuration page, click **Security > Control > Captive Portal > CP User Configuration**. (Shown in following two figures.)

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 2 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security | Access | Port Authentication | Traffic Control | **Control** | ACL

**CP User Configuration**

CP User Configuration

	User ID	User Name	Edit Password	Password	Confirm Password	Group	Session Timeout	Idle Timeout
<input type="checkbox"/>			Disable	*****	*****	1		

ADD DELETE CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 2 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security | Access | Port Authentication | Traffic Control | **Control** | ACL

**CP User Configuration**

CP User Configuration

	Group	Session Timeout	Idle Timeout	Max Bandwidth Down	Max Bandwidth Up	Max Input	Max Output	Max Total
<input type="checkbox"/>	1							

ADD DELETE CANCEL APPLY

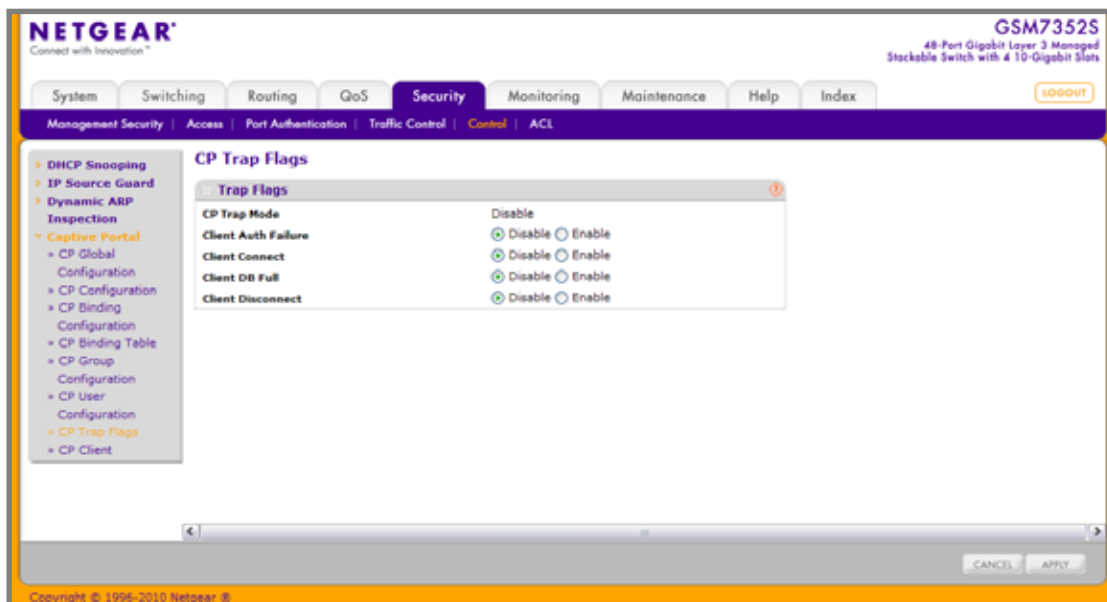
Copyright © 1996-2010 Netgear, Inc.

1. **User ID** identifies the name of the user.
2. Use **User Name** to enter the name of the user. Name can contain 1 to 31 alphanumeric characters. User names once created cannot be changed/modified.
3. Set **Edit Password** to “Enable” only when you want to change the password. The default value is “Disable”.
4. Use **Password** to enter a password for the user. The password length can be from 8 to 64 characters.
5. Use **Confirm Password** to enter the password for the user again.
6. Use **Group** to assign the user to at least one User Group. To assign a user to more than one group, press the Ctrl key and click each group. New users are assigned to the 1-Default user group by default.
7. Use **Session Timeout** to enter the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically. A value of 0 means that the user does not have a Session Timeout limit. The valid range is 0 to 86400 seconds and the default value is 0.
8. Use **Idle Timeout** to enable Logout once idle time-out is reached (seconds). If the attribute is 0 or not present then use the value configured for the captive portal.
9. Use **Max Bandwidth Down** to specify the maximum rate (Rate in bits per seconds) at which a client can receive data from the network. 0 indicates use global configuration (Range: 0 – 536870911 bps.)
10. Use **Max Bandwidth Up** to specify the maximum rate (Rate in bits per seconds) at which a client can send data into the network. 0 indicates to use the global limit (Range: 0 – 536870911 bps.)
11. Use **Max Output** to specify the number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. 0 indicates to use the global limit (Range: 0 – 4294967295.)
12. Use **Max Input** to specify the number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. 0 indicates to use the global limit (Range: 0 – 4294967295.)
13. Use **Max Total** to specify the number of bytes the user is allowed to transmit and receive. The maximum number of octets is the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. 0 indicates to use the global limit (Range: 0 – 4294967295.)

## Captive Portal Trap Flags

Use this page to configure whether or not SNMP traps are sent from the Captive Portal and to specify captive portal events that will generate a trap. All CP SNMP traps are disabled by default.

To display the Captive Portal Trap Flags page, click **Security > Control > Captive Portal > CP Trap Flags**.



1. **CP Trap Mode** - Displays the captive portal trap mode status. To enable or disable the mode, use the System > SNMP>SNMPv1/v2>Trap Flags page.
2. If you enable the **Client Auth Failure** field, the SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.
3. If you enable the **Client Connect** field, the SNMP agent sends a trap when a client authenticates with and connects to a captive portal.
4. If you enable the **Client DB Full** field, the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.
5. If you enable the **Client Disconnect** field, the SNMP agent sends a trap when a client disconnects from a captive portal.

## Captive Portal Client

To display the Captive Portal Client page, click **Security > Control > Captive Portal > CP Client**.

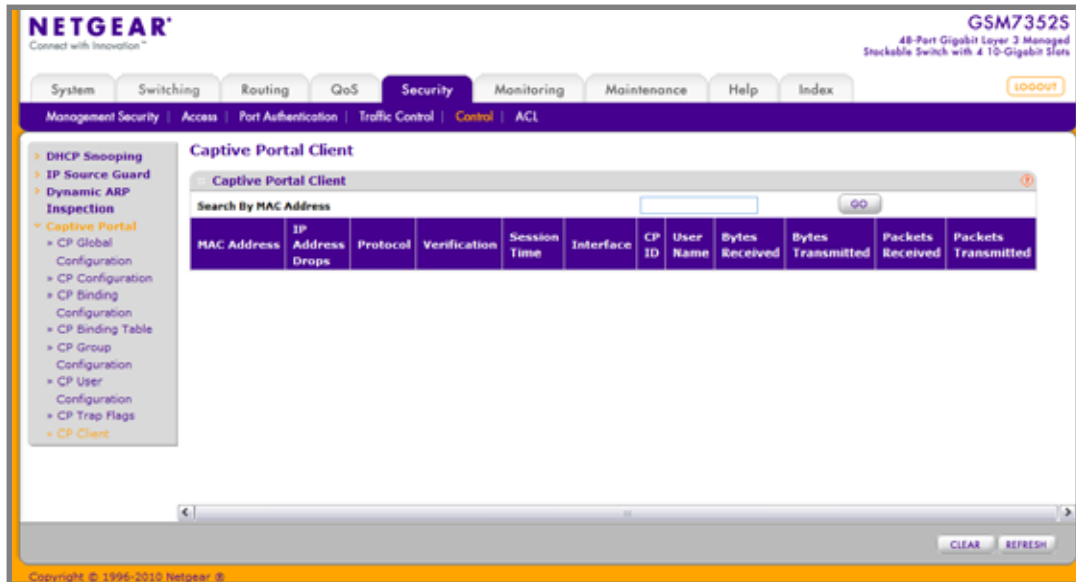


Table 6-107.

Field	Description
MAC Address	Identifies the MAC address of the client
IP Address Drops	Identifies the IP address of the client (if applicable)
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.
Session Time	Shows the amount of time that has passed since the client was authorized.
Interface	Identifies the interface the client is using.
CP ID	The ID of the Captive Portal instance.
User Name	Displays the user name (or Guest ID) of the connected client
Bytes Received	Total bytes the client has received
Bytes Transmitted	Total bytes the client has transmitted.
Packets Received	Total packets the client has received.
Packets Transmitted	Total packets the client has transmitted.

## 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. ProSafe® Managed Switches software supports IPv4 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:

### Basic

The Basic folder contains links to the following features:

- [MAC ACL](#) on page 524
- [MAC Rules](#) on page 526
- [MAC Binding Configuration](#) on page 528
- [MAC Binding Table](#) on page 530

### 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. On this menu the interfaces to which an MAC ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the MAC ACL are specified/created using the MAC ACL Rule Configuration menu.

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 screenshot shows the Netgear web interface for a GSM7352S switch. The 'Security' tab is selected, and the 'MAC ACL' page is displayed. The 'Basic' section is active, showing the 'MAC ACL' configuration. The 'Current Number of ACL' is 0 and the 'Maximum ACL' is 100. Below this is a table titled 'MAC ACL Table' with columns for Name, Rules, and Direction. The table is currently empty. At the bottom of the page are buttons for ADD, DELETE, CANCEL, and APPLY.

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 **ADD** to add a new MAC ACL to the switch configuration.

## 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**. (Following two figures.)

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security Access Port Authentication Traffic Control Control **ACL**

**Basic**  
+ MAC ACL  
+ MAC Rules  
+ MAC Binding Configuration  
+ Binding Table  
- Advanced

### MAC Rules

Rules

ACL Name:

ID	Action	Assign Queue Id	Mirror Interface	Match Every	CoS	Destination MAC	Destination MAC Mask	EtherType Key
1	<input type="text" value="Deny"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>

ADD RESET CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security Access Port Authentication Traffic Control Control **ACL**

**Basic**  
+ MAC ACL  
+ MAC Rules  
+ MAC Binding Configuration  
+ Binding Table  
- Advanced

### MAC Rules

Rules

ACL Name:

Destination MAC	Destination MAC Mask	EtherType Key	EtherType User Value	Source MAC	Source MAC Mask	VLAN	Logging
<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>

ADD RESET CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

To configure MAC ACL rules:

1. 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 &ltpdf>“MAC Binding Table” on page 6-530.
2. To add a new rule, enter a whole number in the range of (1 to 12) that will be used to identify the rule, configure the following settings, and click **Add**.
  - **Action** - Specify what action should be taken if a packet matches the rule's criteria. The choices are permit or deny.
  - **Assign Queue Id** - Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Valid range of Queue Ids is (0 to 6).
  - **CoS** - Specifies the 802.1p user priority to compare against an Ethernet frame. Valid range of values is 0 to 7.
  - **Ethertype User Value** - Specifies the user defined customized Ethertype value to be used when the user has selected “User Value” as Ethertype Key, to compare against an Ethernet frame. Valid range of values is 0x0600 to 0xFFFF.
  - **Source MAC** - Specifies the Source MAC address to compare against an Ethernet frame. Valid format is (xx:xx:xx:xx:xx:xx).
  - **Source MAC Mask** - Specifies the Source MAC address mask specifying which bits in the Source MAC to compare against an Ethernet frame. Valid format is (xx:xx:xx:xx:xx:xx).
  - **Destination MAC** - Specifies the destination MAC address to compare against an Ethernet frame. Valid format is (xx:xx:xx:xx:xx:xx). The BPDU keyword may be specified using a Destination MAC address of 01:80:C2:xx:xx:xx.
  - **Destination MAC Mask** - Specifies the destination MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame. Valid format is (xx:xx:xx:xx:xx:xx). The BPDU keyword may be specified using a Destination MAC mask of 00:00:00:ff:ff:ff. VLAN - Specifies the VLAN ID to compare against an Ethernet frame. Valid range of values is 0 to 4095. Either VLAN Range or VLAN can be configured.
  - **Logging** - When set to 'Enable', logging is enabled for this ACL rule (subject to resource availability in the device). 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 5 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**. Configuration changes take effect immediately.

## 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**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Management Security | Access | Port Authentication | Traffic Control | Control | **ACL**

Basic  
 > MAC ACL  
 > MAC Rules  
 > MAC Binding Configuration  
 > Binding Table  
 > Advanced

### MAC Binding Configuration

**Binding Configuration**

ACL ID:  Direction:

Sequence Number:  (1 to 4294967295)

**Port Selection Table**

Unit
Unit 1

**Interface Binding Status**

Interface	Direction	ACL Type	ACL ID	Sequence Number
-----------	-----------	----------	--------	-----------------

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

1. Select an existing MAC ACL from the ACL ID menu. You can select one and bind it to the interfaces you wanted.

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.

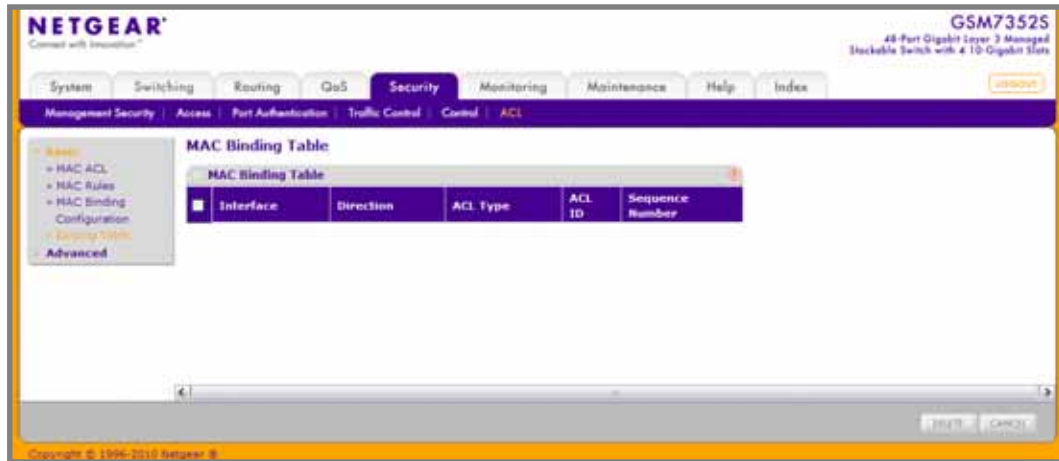
A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater 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. The Port Selection Table provides a list of all available valid interfaces for ACL binding. All non-routing physical interfaces, vlan interface and interfaces participating in LAGs are listed.
  - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that an X 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. An X in the box indicates that the ACL is applied to the interface.
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.

## 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**.



The following table describes the information displayed in the **MAC Binding Table**.

To delete a MAC ACL-to-interface binding, select the check box next to the interface and click **Delete**.

**Table 6-108.**

Field	Description
Interface	Displays the interface of the ACL assigned.
Direction	Displays selected packet filtering direction for ACL.
ACL Type	Displays the type of ACL assigned to selected interface and direction.
ACL ID	Displays the ACL Number (in case of IP ACL) or ACL Name (in case of MAC ACL) identifying 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.

## Advanced

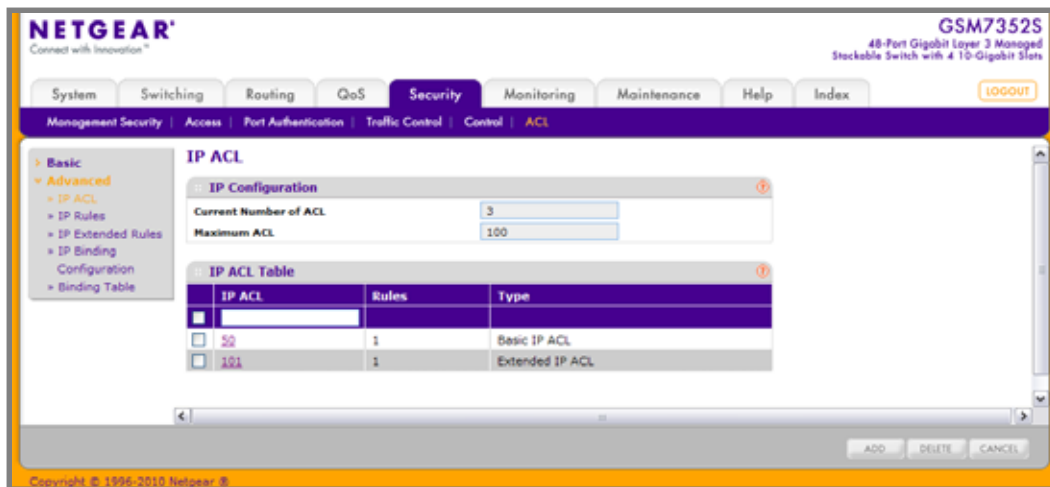
The Advanced folder contains links to the following features:

- [IP ACL](#) on page 531
- [IP Rules](#) on page 533
- [IP Extended Rules](#) on page 535
- [IPv6 ACL](#) on page 538
- [IPv6 Rules](#) on page 539
- [IP Binding Configuration](#) on page 542
- [IP Binding Table](#) on page 544

### IP ACL

An IP 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 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 or IP ACL name. The ID is an integer in the following range:
  - 1–99: Creates an IP Basic 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.
  - **IP ACL Name:** Create a Named IP ACL, which provides alternate to configure the IP Extended ACL. IP ACL Name string which includes alphanumeric characters only and must start with an alphabetic character.

Each configured ACL displays the following information:

- **Rules** - Displays the number of rules currently configured for the IP ACL.
  - **Type** - Identifies the ACL as a basic IP ACL, extended IP ACL and named IP ACL.
2. To delete an IP ACL, select the check box next to the IP ACL ID field, then click **Delete**.
  3. Click **ADD** to add a new IP ACL to the switch configuration.



## IP Rules

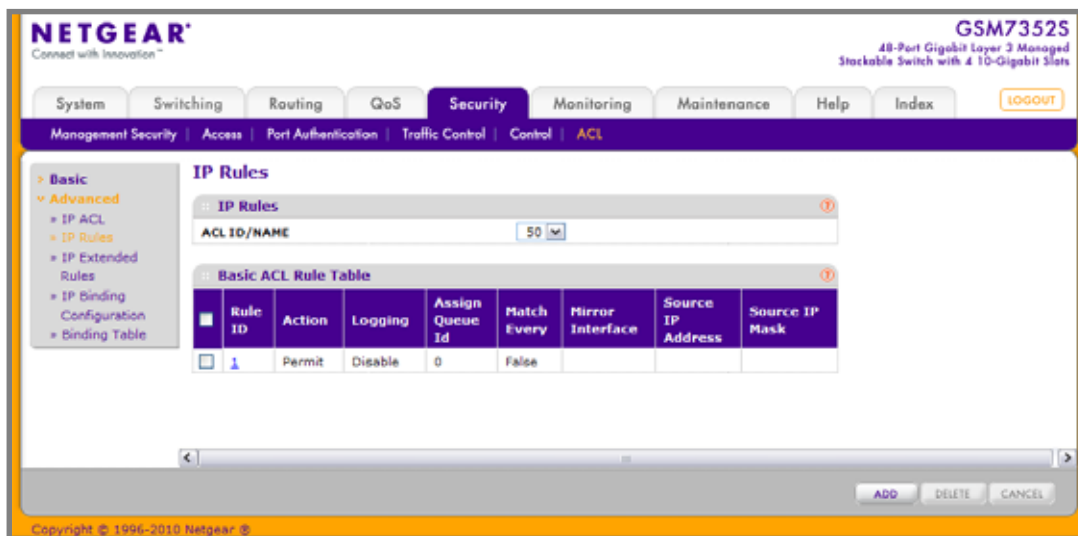
Use these screens to configure the rules for the IP Access Control Lists created using the IP Access Control List Configuration screen. What is shown on this screen varies depending on the current step in the rule configuration process.

---

**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:

- To add an IP ACL rule, select the ACL ID to add the rule to, complete the fields described in the following list, and click **Add**. (Only displays ACL IDs from 1 to 99.)
  - Rule ID** - Specify a number from 1–12 to identify the IP ACL rule. You can create up to 12 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.
  - Logging** - When set to 'Enable', logging is enabled for this ACL rule (subject to resource availability in the device). 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 5 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 visible for a 'Deny' Action.

- **Assign Queue ID** - 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.
  - **Match Every** - Select true or false from the pull-down menu. True signifies that all packets will match the selected IP 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 re-create it, or re-configure 'Match Every' to 'False' for the other match criteria to be visible.
  - **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.
  - **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.
  - **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** - Specify the IP Mask in dotted-decimal notation to be used with the Source IP Address value.
2. To delete an IP ACL rule, select the check box associated with the rule, and then click **Delete**.
  3. 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.
  4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
  5. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

## IP Extended Rules

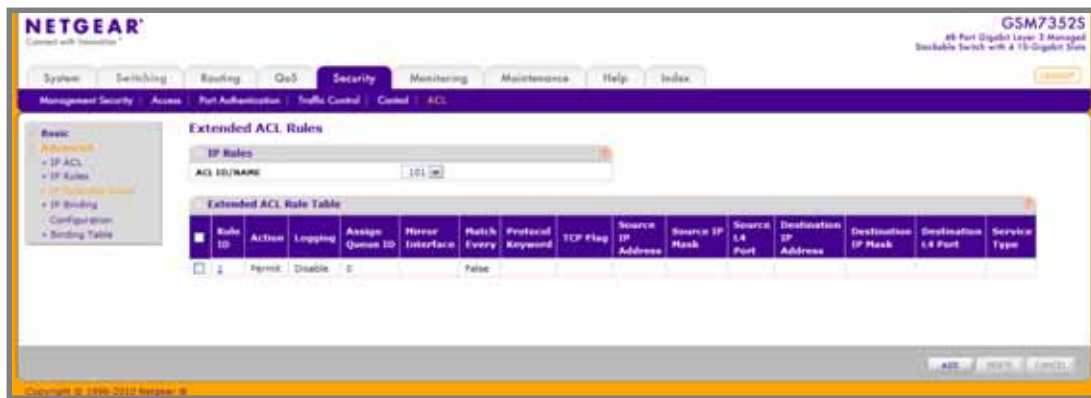
Use these screens to configure the rules for the IP Access Control Lists created using the IP Access Control List Configuration screen. What is shown on this screen varies depending on the current step in the rule configuration process.

---

**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, select the check box in the Extended ACL Rule table, and click **Add**. The page displays the extended ACL Rule Configuration fields.
2. Configure the new rule.
  - **Rule ID** - Specify a number from 1–12 to identify the IP ACL rule. You can create up to 12 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.
  - **Logging** - When set to 'Enable', logging is enabled for this ACL rule (subject to resource availability in the device). 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 5 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 visible for a 'Deny' Action.

- **Assign Queue** - Specifies the hardware egress queue identifier used to handle all packets matching this IP ACL rule. Valid range of Queue Ids is 0 to 6.
- **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.
- **Match Every** - Select true or false from the pull-down menu. True signifies that all packets will match the selected IP 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 re-create it, or re-configure 'Match Every' to 'False' for the other match criteria to be visible.
- **Protocol Keyword** - Specify that a packet's IP protocol is a match condition for the selected IP ACL rule. The possible values are ICMP, IGMP, IP, TCP, and UDP.
- **TCP Flag** - Specify that a packet's TCP flag is a match condition for the selected IP ACL rule. The TCP flag values are URG,ACK,PSH,RST,SYN,FIN. Each TCP flag has these possible values below and can be set separately.
  - Ignore - A packet matches this ACL rule whatever the TCP flag in this packet is set or not.
  - Set(+) - A packet matches this ACL rule if the TCP flag in this packet is set.
  - Clear(-) - A packet matches this ACL rule if the TCP flag in this packet is not set.
- **Src IP Address** - Enter an IP address using dotted-decimal notation to be compared to a packet's source IP Address as a match criteria for the selected IP ACL rule.
- **Src IP Mask** - Specify the IP Mask in dotted-decimal notation to be used with the Source IP Address value.
- **Src L4 Port** - Specify a packet's source layer 4 port as a match condition for the selected extended IP ACL rule. This is an optional configuration. The possible values are 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.
- **Dst IP Address** - Enter an IP address using dotted-decimal notation to be compared to a packet's destination IP Address as a match criteria for the selected extended IP ACL rule.
- **Dst IP Mask** - Specify the IP Mask in dotted-decimal notation to be used with the Destination IP Address value.
- **Dst L4 Port** - Specify the destination layer 4 port match conditions for the selected extended IP ACL rule. The possible values are 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. This is an optional configuration.
- **Service Type** - Select a Service Type match condition for the extended IP ACL rule from the pull-down menu. The possible values are IP DSCP, IP precedence, and IP TOS, which are alternative ways of specifying a match criterion for the same Service

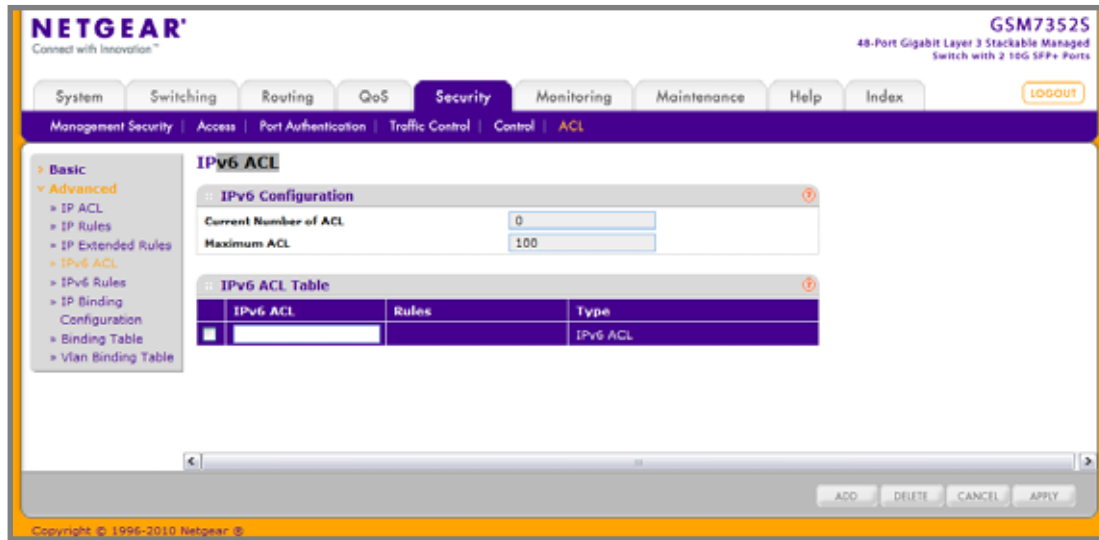
Type field in the IP header, however each uses a different user notation. After a selection is made the appropriate value can be specified.

- **IP DSCP** - 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 IP header. This is an optional configuration. Enter an integer from 0 to 63. The IP DSCP is selected by possibly selection one of the DSCP keyword from a dropdown box. If a value is to be selected by specifying its numeric value, then select the 'Other' option in the dropdown box and a text box will appear where the numeric value of the DSCP can be entered.
  - **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** - The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. The TOS Bits value is a hexadecimal number from 00 to FF. The TOS Mask value is a hexadecimal number from 00 to FF. The TOS Mask denotes the bit positions in the TOS Bits value that are used for comparison against the IP TOS field in 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 0xA0 and a TOS Mask of 0xFF. This is an optional configuration.
3. To delete an IP ACL rule, select the check box associated with the rule, and then click **Delete**.
  4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
  5. 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 IP 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**.



1. **IP ACL** is the IP ACL ID or IP ACL Name which is dependent on the IP ACL Type. IP ACL ID must be an integer from 1 to 99 for an IP basic ACL and from 100 to 199 for an IP Extended ACL. IPv6 ACL Name string includes alphanumeric characters only. The name must start with an alphabetic character.
2. Click **ADD** to add a new IP ACL to the switch configuration.
3. Click **DELETE** to remove the currently selected IP ACL from the switch configuration.

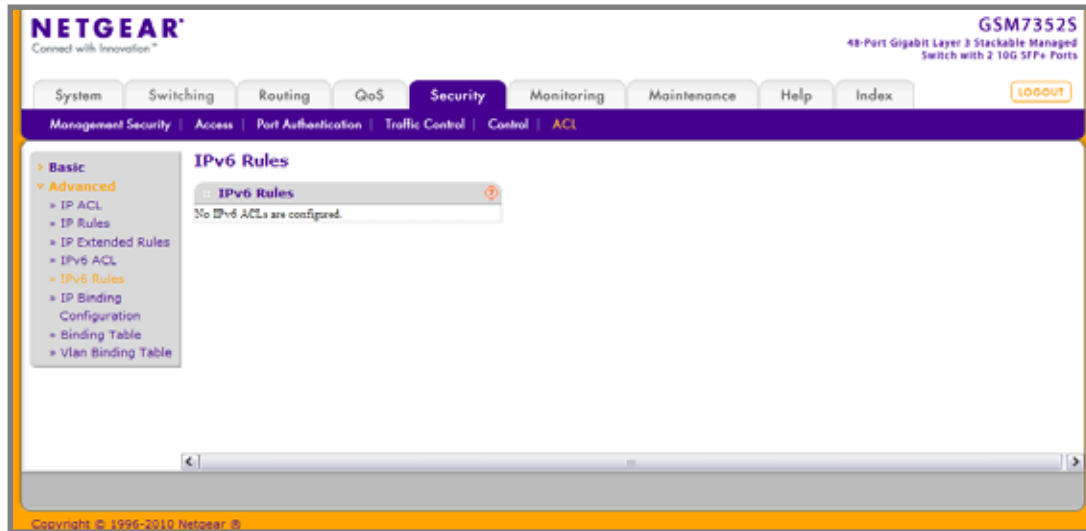
**Table 7.**

Field	Description
Current Number of ACL	The current number of the IP ACLs configured on the switch.
Maximum ACL	The maximum number of IP ACL can be configured on the switch, it depends on the hardware.
Rules	The number of the rules associated with the IP ACL.
Type	The the ACL type, basic IP ACL with id from 1 to 99 and Extended IP ACL with id from 100 to 199.

## IPv6 Rules

Use these screens to configure the rules for the IPv6 Access Control Lists, which is created using the IPv6 Access Control List Configuration screen. 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**.



1. Use the **ACL Name** pull down menu to select the IPv6 ACL for which to create or update a rule.
2. Use **Rule ID** to enter a whole number in the range of 1 to 12 that will be used to identify the rule. An IP ACL may have up to 12 rules.
3. Use **Action** to specify what action should be taken if a packet matches the rule's criteria. The choices are permit or deny.
4. Use **Logging** to enable logging for this ACL rule (subject to resource availability in the device). 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 5 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 visible for a 'Deny' Action.
5. Use **Assign Queue ID** to specify the hardware egress queue identifier used to handle all packets matching this IPv6 ACL rule. Valid range of Queue IDs is 0 to 6. This field is visible for a 'Permit' Action.
6. Use **Mirror Interface** to specify 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.
7. Use **Redirect Interface** to specify 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.
8. Use **Match Every** to 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.
9. Use **Protocol** to configure IPv6 protocol:
  - a. Specify an integer ranging from 0 to 255 after selecting protocol keyword "other". This number represents the IP protocol.
  - b. Select name of a protocol from the existing list of Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).
10. Use **Source Prefix / PrefixLength** to 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.
11. Use **Source L4 Port** to 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:
  - a. Select keyword "other" from the drop down menu and specify the number of the port in the range from 0 to 65535.
  - b. 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.



12. Use **Destination Prefix / PrefixLength** to 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.
13. Use **Destination L4 Port** to 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:
  - a. Select keyword "other" from the drop down menu and specify the number of the port in the range from 0 to 65535.
  - b. 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.
14. **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 specified within the range (0 to 1048575).
15. Use **IPv6 DSCP Service** to 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 dropdown box. If a value is to be selected by specifying its numeric value, then select the 'Other' option in the dropdown box and a text box will appear where the numeric value of the DSCP can be entered.
16. Click **ADD** to add an IPv6 rule.
17. Use **DELETE** to select the checkbox of the rule you want to delete 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**.

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Management Security | Access | Port Authentication | Traffic Control | Control | **ACL**

Basic  
Advanced  
  IP ACL  
  IP Rules  
  IP Extended Rules  
  IP Binding Configuration  
  Binding Table

### IP Binding Configuration

**Binding Configuration**

ACL ID:  Direction:

Sequence Number:  (1 to 4294967295)

**Port Selection Table**

**Interface Binding Status**

Interface	Direction	ACL Type	ACL ID/Name	Sequence Number
-----------	-----------	----------	-------------	-----------------

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

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. The Port Selection Table specifies list of all available valid interfaces for ACL mapping. All non-routing physical interfaces and interfaces participating in LAGs are listed.
  - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that an X 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. An X in the box indicates that the ACL is applied to the interface.
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.

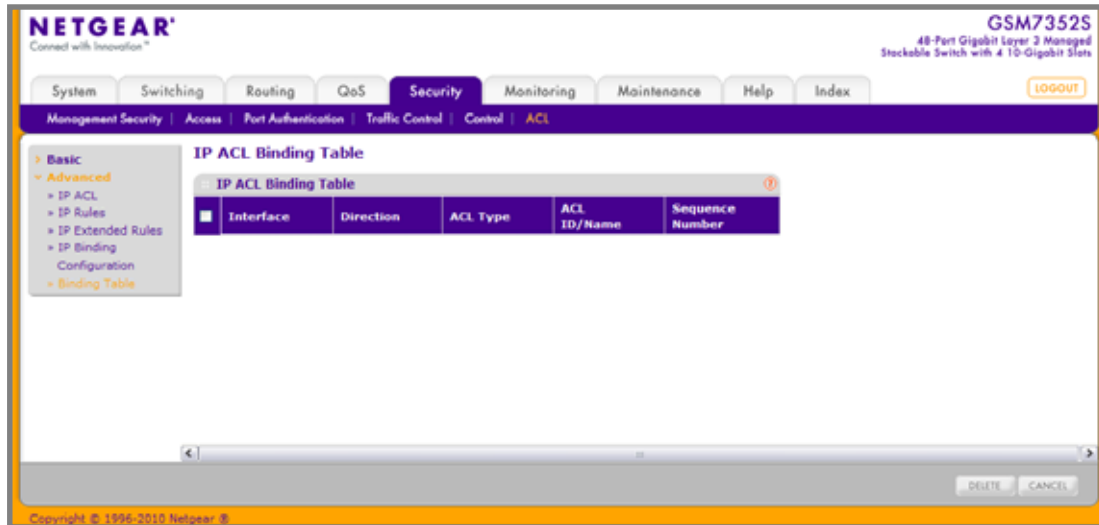
**Table 6-109.**

Field	Description
Interface	Displays selected interface.
Direction	Displays selected packet filtering direction for ACL.
ACL Type	Displays the type of ACL assigned to selected interface and direction.
ACL ID/Name	Displays the ACL Number (in the case of IP ACL) or ACL Name (in the case of named IP ACL and IPv6 ACL) identifying 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.

## 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 **MAC Binding Table**.

To delete an IP ACL-to-interface binding, select the check box next to the interface and click **Delete**.

**Table 6-110.**

Field	Description
Interface	Displays selected interface.
Direction	Displays selected packet filtering direction for ACL.
ACL Type	Displays the type of ACL assigned to selected interface and direction.
ACL ID/Name	Displays the ACL Number (in the case of IP ACL) or ACL Name (in the case of Named IP ACL and IPv6 ACL) identifying 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.



# 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 546
- [Logs](#) on page 560
- [Port Mirroring](#) on page 571
- [sFlow](#) on page 573

## 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:

- [Port Statistics](#) on page 546
- [Port Detailed Statistics](#) on page 549
- [EAP Statistics](#) on page 557
- [Cable Test](#) on page 559

## Port Statistics

The Port Statistics page displays a summary of per-port traffic statistics on the switch.

To access the Port Statistics page, click **Monitoring > Ports > Port Statistics**.

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed  
Stackable Switch with 4 10-Gigabit SFPs

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

Ports Logs Mirroring sFlow

**Port Statistics**

▼ Port Statistics  
▼ Port Detailed Statistics  
▼ EAP Statistics  
▼ Cable Test

**Port Statistics**

Status

All Go To Interface  GO

Interface	Total Packets received without Errors	Packets received with Errors	Broadcast Packets received	Packets transmitted without Errors	Transmit Packet Errors	Collision Frames	Time since counters last cleared
<input type="checkbox"/> 1/0/1	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/2	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/3	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/4	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/5	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/6	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/7	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/8	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/9	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/10	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/11	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/12	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/13	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/14	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/15	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/16	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/17	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/18	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec
<input type="checkbox"/> 1/0/19	0	0	0	0	0	0	9 day 23 hr 35 min 36 sec

CLEAR REFRESH

Copyright © 1996-2010 Netgear, Inc.

The following table describes the per-port statistics displayed on the screen.

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.

**Table 7-111.**

Field	Description
Interface	This object indicates the ifIndex of the interface table entry associated with this port on an adapter.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that have been transmitted by this port to its segment.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.



## Port Detailed Statistics

The Port Detailed Statistics page displays a variety of per-port traffic statistics.

To access the Port Detailed page, click **Monitoring > Ports > Port Detailed Statistics**. (Following two figures show some, but not all, of the fields on the Port Detailed Statistics page.)

The screenshot displays the 'Port Detailed Statistics' window. It features a title bar with the text 'Port Detailed Statistics' and a close button. Below the title bar, there are two dropdown menus: 'Interface' set to '1/0/1' and 'MST ID' set to 'CST'. The main content area is a list of port statistics, organized into two columns. The left column lists the statistic names, and the right column shows their current values, all of which are '0' in this instance.

Statistic	Value
Interface	1/0/1
MST ID	CST
ifIndex	1
Port Type	Normal
Port Channel ID	not a lag member
Port Role	
STP Mode	Enable
STP State	
Admin Mode	Enable
LACP Mode	Enable
Physical Mode	Auto
Physical Status	Unknown
Link Status	Link Down
Link Trap	Enable
Packets RX and TX 64 Octets	0
Packets RX and TX 65-127 Octets	0
Packets RX and TX 128-255 Octets	0
Packets RX and TX 256-511 Octets	0
Packets RX and TX 512-1023 Octets	0
Packets RX and TX 1024-1518 Octets	0
Packets RX and TX 1519-2047 Octets	0
Packets RX and TX 2048-4095 Octets	0
Packets RX and TX 4096-9216 Octets	0
Octets Received	0
Packets Received 64 Octets	0
Packets Received 65-127 Octets	0
Packets Received 128-255 Octets	0
Packets Received 256-511 Octets	0
Packets Received 512-1023 Octets	0
Packets Received 1024-1518 Octets	0
Packets Received > 1518 Octets	0
Total Packets Received Without Errors	0
Unicast Packets Received	0
Multicast Packets Received	0
Broadcast Packets Received	0
Total Packets Received with MAC Errors	0
Jabbers Received	0
Fragments Received	0
Undersize Received	0
Alignment Errors	0
Rx FCS Errors	0
Overruns	0
802.3x Pause Frames Received	0
Broadcast Storm Recovery	0
Total Packets Transmitted (Octets)	0
Packets Transmitted 64 Octets	0
Packets Transmitted 65-127 Octets	0
Packets Transmitted 128-255 Octets	0
Packets Transmitted 256-511 Octets	0
Packets Transmitted 512-1023 Octets	0

Packets Received 512-1023 Octets	0	
Packets Received 1024-1518 Octets	0	
Packets Received > 1518 Octets	0	
Total Packets Received Without Errors	0	
Unicast Packets Received	0	
Multicast Packets Received	0	
Broadcast Packets Received	0	
Total Packets Received with MAC Errors	0	
Jabbers Received	0	
Fragments Received	0	
Undersize Received	0	
Alignment Errors	0	
Rx FCS Errors	0	
Overruns	0	
802.3x Pause Frames Received	0	
Broadcast Storm Recovery	0	
Total Packets Transmitted (Octets)	0	
Packets Transmitted 64 Octets	0	
Packets Transmitted 65-127 Octets	0	
Packets Transmitted 128-255 Octets	0	
Packets Transmitted 256-511 Octets	0	
Packets Transmitted 512-1023 Octets	0	
Packets Transmitted 1024-1518 Octets	0	
Packets Transmitted > 1518 Octets	0	
Total Packets Transmitted Successfully	0	
Unicast Packets Transmitted	0	
Multicast Packets Transmitted	0	
Broadcast Packets Transmitted	0	
Total Transmit Errors	0	
Tx FCS Errors	0	
Underrun Errors	0	
Total Transmit Packets Discarded	0	
Single Collision Frames	0	
Multiple Collision Frames	0	
Excessive Collision Frames	0	
Port Membership Discards	0	
Dropped Transmit Frames	858993460	
STP BPDUs Received	0	
STP BPDUs Transmitted	0	
RSTP BPDUs Received	0	
RSTP BPDUs Transmitted	0	
MSTP BPDUs Received	0	
MSTP BPDUs Transmitted	0	
802.3x Pause Frames Transmitted	0	
GVRP PDUs Received	0	
GVRP PDUs Transmitted	0	
GVRP Failed Registrations	0	
GMRP PDUs Received	0	
GMRP PDUs Transmitted	0	
GMRP Failed Registrations	0	
EAPOL Frames Received	0	
EAPOL Frames Transmitted	0	
Time Since Counters Last Cleared	9 day 23 hr 41 min 52 sec	

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.

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.

**Table 7-112.**

Field	Description
ifIndex	This object indicates the ifIndex of the interface table entry associated with this port on an adapter.
Port Type	For normal ports this field will be 'normal.' Otherwise the possible values are: <ul style="list-style-type: none"> <li>• Mirrored - This port is a participating in port mirroring as a mirrored port. Look at the Port Mirroring screens for more information.</li> <li>• Probe - This port is a participating in port mirroring as the probe port. Look at the Port Mirroring screens for more information.</li> <li>• Trunk Member - The port is a member of a Link Aggregation trunk. Look at the Port Channel screens for more information.</li> </ul>
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	The Spanning Tree Protocol Administrative Mode associated with the port or Port Channel. The possible values are: <ul style="list-style-type: none"> <li>• Enable - Spanning tree is enabled for this port.</li> <li>• Disable - Spanning tree is disabled for this port.</li> </ul>
STP State	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"> <li>• Disabled</li> <li>• Blocking</li> <li>• Listening</li> <li>• Learning</li> <li>• Forwarding</li> <li>• Broken</li> </ul>
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. The factory default is enabled.
LACP Mode	Indicates the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation.

Table 7-112.

Field	Description
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.
Link Status	Indicates whether the Link is up or down.
Link Trap	Indicates whether or not the port will send a trap when 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 1519-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Received 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Table 7-112.

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 > 1518 Octets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Total Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
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).

Table 7-112.

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.
VLAN Membership Mismatch	The number of frames discarded on this port due to ingress filtering.
VLAN Viable Discards	The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.
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.
Received Packets Dropped including aborted	The number of packets without any errors that are dropped at the time of their receive.
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.

Table 7-112.

Field	Description
Packets Transmitted 64 Octets	The total number of packets (including bad packets) received 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) received 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) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 256-511 Octets	The total number of packets (including bad packets) received 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) received 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) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted > 1518 Octets	The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. This counter has a max increment rate of 815 counts per sec at 10 Mb/s.
Maximum Frame Size	The maximum ethernet frame size the interface supports or is configured, including 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
Underrun Errors	The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Table 7-112.

Field	Description
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Port Membership Discards	The number of frames discarded on egress for this port due to egress filtering being enabled.
Dropped Transmit Frames	Number of transmit frames discarded at the selected port.
Dropped Receive Frames	Number of Receive frames discarded at the selected port.
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.
GVRP PDUs Received	The count of GVRP PDUs received in the GARP layer.
GVRP PDUs Transmitted	The count of GVRP PDUs transmitted from the GARP layer.
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed.
GMRP PDUs Received	The count of GMRP PDUs received from the GARP layer.
GMRP PDUs Transmitted	The count of GMRP PDUs transmitted from the GARP layer.
GMRP Failed Registrations	The number of times attempted GMRP registrations could not be completed.
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.



## 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 **Monitoring > Ports > EAP Statistics**.

**NETGEAR**  
GSM73525  
48 Port Gigabit Layer 3 Managed Stackable Switch with 4 10 Gigabit SFPs

System Switching Routing QoS Security Monitoring Performance Help Index

Home > Setup > Monitoring > Ports > EAP Statistics

Port Statistics  
Port Detailed  
Statistics  
EAP Statistics  
Cable Test

**EAP Statistics**

Go to Interface:

Port	PAE Capabilities	EAPOL						EAP					
		Frame Received	Frame Transmitted	Start Frame Received	Logoff Frame Received	Last Frame Received	Last Frame Source	Successful Frame Received	Length Error Frame Received	Response/ID Frame Received	Response Frame Received	Request/ID Frame Transmitted	Request Frame Transmitted
<input type="checkbox"/> 1/0/1	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/2	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/3	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/4	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/5	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/6	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/7	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/8	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/9	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/10	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/11	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/12	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/13	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/14	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/15	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/16	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/17	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/18	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/19	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/20	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 1/0/21	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0

Copyright © 1999-2011 Netgear, Inc.

The following table describes the EAP statistics displayed on the screen.

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

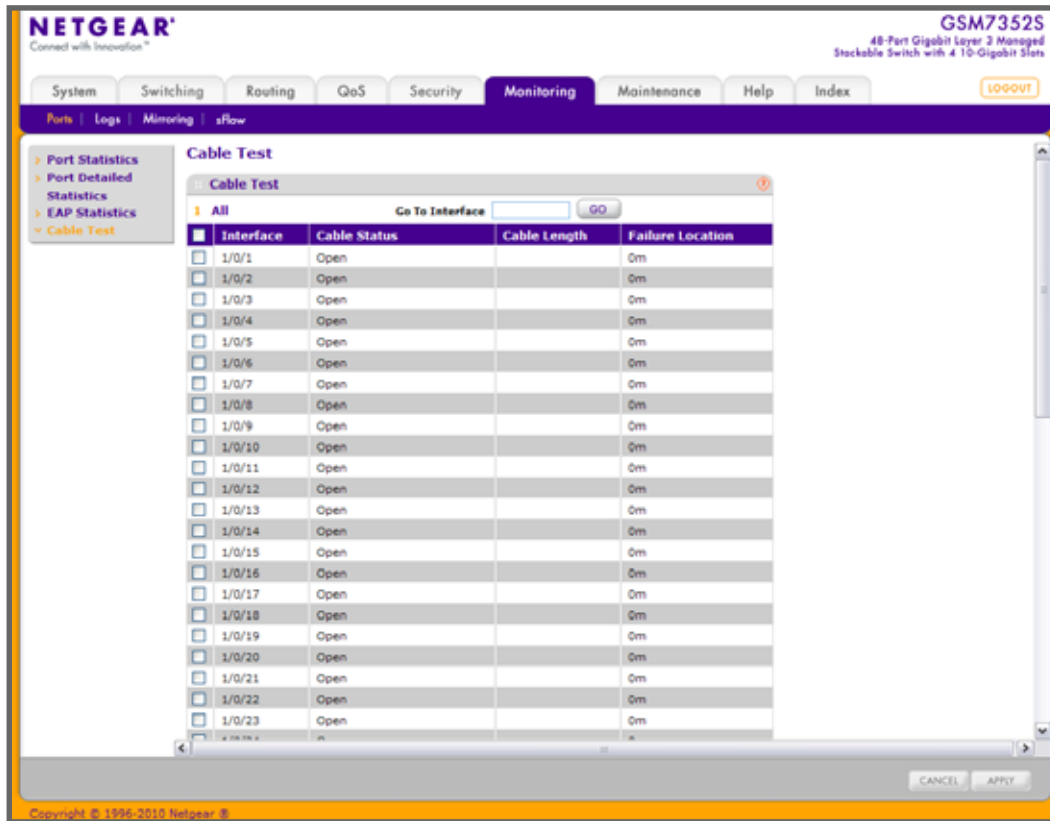
- To clear all the EAP counters for all ports on the switch, select the check box in the row heading and click **Clear**. The button resets all statistics for all ports to default values.
- To clear the counters for a specific port, select the check box associated with the port and click **Clear**.
- Click **Refresh** to refresh the data on the screen and display the most current statistics.

**Table 7-113.**

Field	Description
Port	Selects the port to be displayed. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port. All physical interfaces are valid.
PAE Capabilities	This displays the PAE capabilities of the selected port
EAPOL Frames Received	This displays the number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	This displays the number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	This displays the number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	This displays the number of EAPOL logoff frames that have been received by this authenticator.
EAPOL Last Frame Version	This displays the protocol version number carried in the most recently received EAPOL frame.
EAPOL Last Frame Source	This displays the source MAC address carried in the most recently received EAPOL frame.
EAPOL Invalid Frames Transmitted	This displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAPOL Length Error Frames Received	This displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Response/ID Frames Received	This displays the number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	This displays the number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/ID Frames Transmitted	This displays the number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	This displays the number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.

## Cable Test

To display the Cable Test page, click **Monitoring** > **Ports** > **Cable Test**.



1. **Interface** - Indicates the interface to which the cable to be tested is connected.
2. Click **Apply** to perform a cable test on the selected interface. The cable test may take up to 2 seconds to complete. If the port has an active link then the link is not taken down and the cable status is always "Normal". The command returns a cable length estimate if this feature is supported by the PHY for the current link speed. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter then the cable status may be "Open" or "Short" because some Ethernet adapters leave unused wire pairs unterminated or grounded.

Table 7-114.

Field	Description
Cable Status	This displays the cable status as Normal, Open or Short. <ul style="list-style-type: none"> <li>• Normal: the cable is working correctly.</li> <li>• Open: the cable is disconnected or there is a faulty connector.</li> <li>• Short: there is an electrical short in the cable.</li> <li>• Cable Test Failed: The cable status could not be determined. The cable may in fact be working.</li> </ul>
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 only displayed 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 only displayed if the cable status is Open or Short.

## Logs

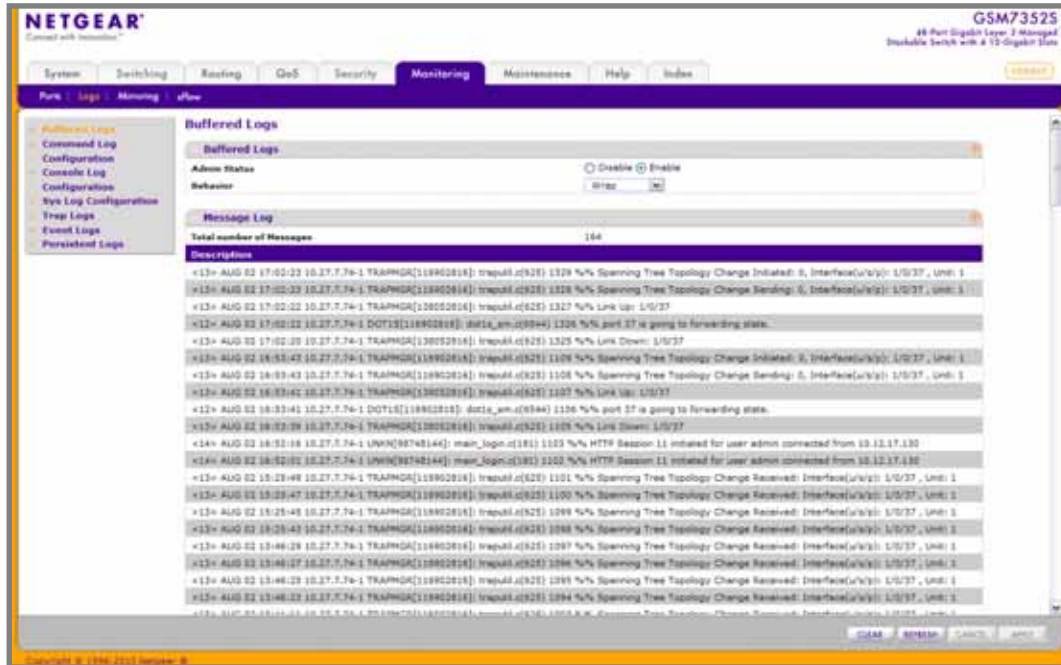
The switch may generate messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored locally and can be forwarded to one or more centralized points of collection for monitoring purposes or long term archival 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:

- [Buffered Logs](#) on page 561
- [Command Log Configuration](#) on page 563
- [Console Log Configuration](#) on page 564
- [SysLog Configuration](#) on page 565
- [Trap Logs](#) on page 566
- [Event Logs](#) on page 568
- [Persistent Logs](#) on page 570

## Buffered Logs

To access the Buffered Logs page, click **Monitoring > Logs > Buffered Logs**.



### Buffered Log Configuration

This log stores messages in memory based upon the settings for message component and severity. On stackable systems, this log exists only on the top of stack platform. Other platforms in the stack forward their messages to the top of stack log.

1. A log that is “Disabled” shall not log messages. A log that is “Enabled” shall log messages. Enable or Disable logging by selecting the corresponding radio button.
2. Behavior Indicates the behavior of the log when it is full. It can either wrap around or stop when the log space is filled.
3. Click **REFRESH** to refresh the web page to show the latest messages in the log.
4. Click **CLEAR** to clear the buffered log in the memory.

## Message Log

This help message applies to the format of all logged messages which are displayed for the message log, persistent log or console log.

### Format of the messages

Messages logged to a collector or relay via syslog have an identical format of either type:

#### If system is not stacked

- <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt\_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry.

The above example indicates a message with severity 7(15 mod 8) (debug) on a system that is not stack and generated by component MSTP running in thread id 2110 on Aug 24 05:34:05 by line 318 of file mstp\_api.c. This is the 237th message logged.

#### If the system is stacked

- <15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt\_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry.

The above example indicates a message with severity 7(15 mod 8) (debug) on a system that is stacked and generated by component MSTP running in thread id 2110 on Aug 24 05:34:05 by line 318 of file mstp\_api.c. This is the 237th message logged with system IP 0.0.0.0 and task-id 1.

### Format of the messages

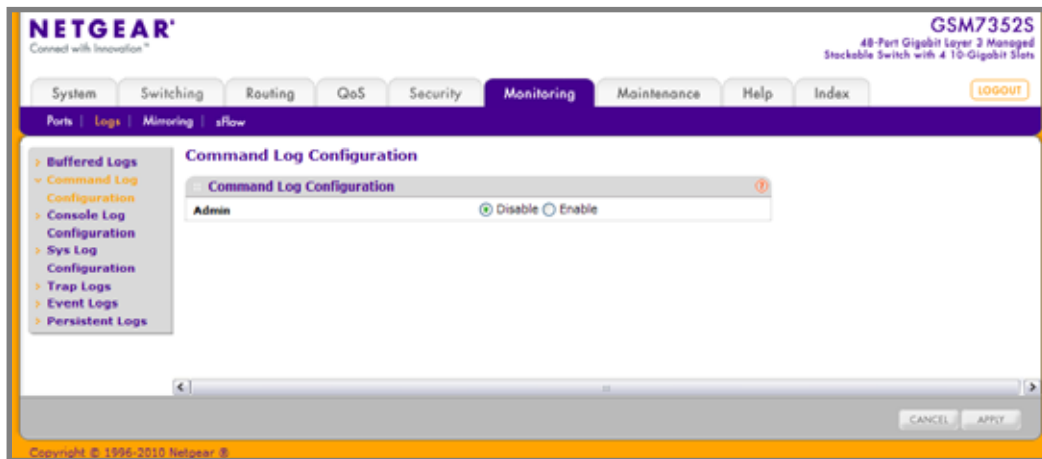
- <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt\_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry.

The above example indicates a user-level message (1) with severity 7 (debug) on a system that is not stack and generated by component MSTP running in thread id 2110 on Aug 24 05:34:05 by line 318 of file mstp\_api.c. This is the 237th message logged. Messages logged to a collector or relay via syslog have an identical format to the above message.

- Total number of Messages: For the message log, only the latest 200 entries are displayed on the webpage

## Command Log Configuration

To access the Command Log Configuration page, click **Monitoring** > **Logs** > **Command Log Configuration**.

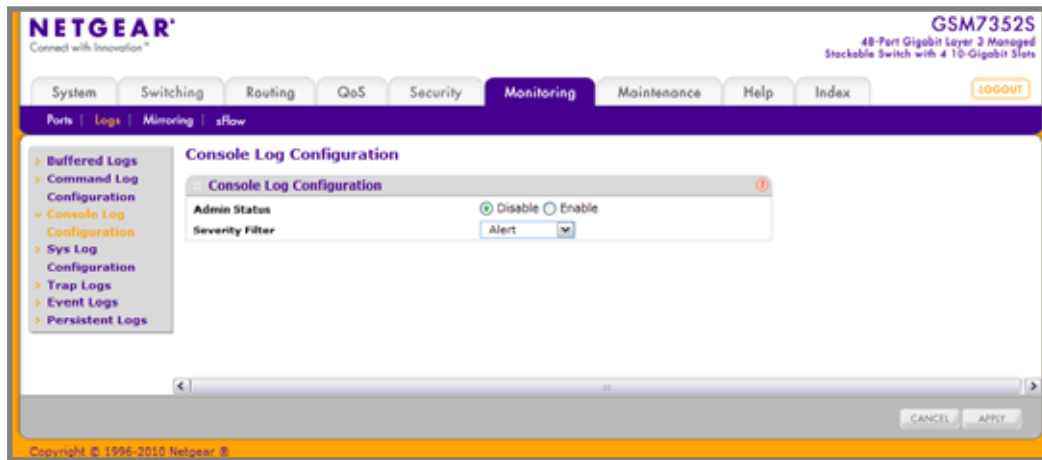


1. Use **Admin Mode** to enable/disable the operation of the CLI Command logging by selecting the corresponding radio button.

## Console Log Configuration

This allows logging to any serial device attached to the host.

To access the Console Log Configuration page, click **Monitoring > Logs > Console Log Configuration**.



1. A log that is “Disabled” shall not log messages. A log that is “Enabled” shall log messages. Enable or Disable logging by selecting the corresponding radio button.
2. **Severity Filter.** A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the pull-down entry field. These severity levels have been enumerated below:
  - Emergency (0) - system is unusable
  - Alert (1) - action must be taken immediately
  - Critical (2) - critical conditions
  - Error (3) - error conditions
  - Warning (4) - warning conditions
  - Notice(5) - normal but significant conditions
  - Informational(6) - informational messages
  - Debug(7) - debug-level messages



## SysLog Configuration

To access the SysLog Configuration page, click **Monitoring > Logs > Sys Log Configuration**.

The screenshot shows the Netgear web interface for Syslog Configuration. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring (selected), Maintenance, Help, and Index. The left sidebar lists various log types: Buffered Logs, Command Log Configuration, Console Log Configuration, Sys Log Configuration (selected), Trap Logs, Event Logs, and Persistent Logs. The main content area is titled 'Syslog Configuration' and contains two sections: 'Syslog Configuration' and 'Host Configuration'. The 'Syslog Configuration' section has a form with 'Admin Status' (radio buttons for Disable and Enable), 'Local UDP Port' (text field with value 514), 'Messages Relayed' (0), and 'Messages Ignored' (0). The 'Host Configuration' section is a table with columns for Host Address, Status, Port, and Severity Filter. The bottom of the page shows a copyright notice: Copyright © 1996-2010 Netgear Inc.

1. Use **Admin Status** to enable/disable logging to configured syslog hosts. Setting this to disable stops logging to all syslog hosts. Disable means no messages will be sent to any collector/relay. Enable means messages will be sent to configured collector/relays using the values configured for each collector/relay. Enable/Disable the operation of the syslog function by selecting the corresponding radio button.
2. Use **Local UDP Port** to specify the port on the local host from which syslog messages are sent. The default port is 514. Specify the local port in the text field.

**Table 7-115.**

Field	Description
Messages Relayed	The count of syslog messages relayed.
Messages Ignored	The count of syslog messages ignored.

## Trap Logs

This screen lists the entries in the trap log. The information can be retrieved as a file by using System Utilities, Upload File from Switch.

To access the Trap Logs page, click **Monitoring > Logs > Trap Logs**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

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

Ports Logs **Monitoring** sFlow

> Buffered Logs  
 > Command Log  
 > Configuration  
 > Console Log  
 > Configuration  
 > Sys Log  
 > Configuration  
 > **Trap Logs**  
 > Event Logs  
 > Persistent Logs

### Trap Logs

Number of Traps Since Last Reset: 118  
 Trap Log Capacity: 256  
 Number of Traps Since Log Last Viewed: 118

#### Trap Logs

Log	System Up Time	Trap
0	AUG 02 17:02:23 2010	Spanning Tree Topology Change Initiated: 0, Interface(u/s/p): 1/0/37, Unit: 1
1	AUG 02 17:02:23 2010	Spanning Tree Topology Change Sending: 0, Interface(u/s/p): 1/0/37, Unit: 1
2	AUG 02 17:02:22 2010	Link Up: 1/0/37
3	AUG 02 17:02:20 2010	Link Down: 1/0/37
4	AUG 02 16:53:43 2010	Spanning Tree Topology Change Initiated: 0, Interface(u/s/p): 1/0/37, Unit: 1
5	AUG 02 16:53:43 2010	Spanning Tree Topology Change Sending: 0, Interface(u/s/p): 1/0/37, Unit: 1
6	AUG 02 16:53:41 2010	Link Up: 1/0/37
7	AUG 02 16:53:39 2010	Link Down: 1/0/37
8	AUG 02 15:25:49 2010	Spanning Tree Topology Change Received: Interface(u/s/p): 1/0/37, Unit: 1
9	AUG 02 15:25:47 2010	Spanning Tree Topology Change Received: Interface(u/s/p): 1/0/37, Unit: 1
10	AUG 02 15:25:45 2010	Spanning Tree Topology Change Received: Interface(u/s/p): 1/0/37, Unit: 1
11	AUG 02 15:25:43 2010	Spanning Tree Topology Change Received: Interface(u/s/p): 1/0/37, Unit: 1
12	AUG 02 13:46:29 2010	Spanning Tree Topology Change Received: Interface(u/s/p): 1/0/37, Unit: 1
13	AUG 02 13:46:27 2010	Spanning Tree Topology Change Received: Interface(u/s/p): 1/0/37, Unit: 1
14	AUG 02 13:46:25 2010	Spanning Tree Topology Change Received: Interface(u/s/p): 1/0/37, Unit: 1
15	AUG 02 13:46:23 2010	Spanning Tree Topology Change Received: Interface(u/s/p): 1/0/37, Unit: 1
16	AUG 02 13:41:11 2010	Spanning Tree Topology Change Received: Interface(u/s/p): 1/0/37, Unit: 1

CLEAR REFRESH

Copyright © 1996-2010 Netgear ®

The following table describes the Trap Log information displayed on the screen.

The page also displays information about the traps that were sent.

Click **Clear Counters** to clear all the counters. This resets all statistics for the trap logs to the default values.

**Table 7-116.**

Field	Description
Number of Traps Since Last Reset	The number of traps that have occurred since the switch last reboot.
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries will overwrite the oldest entries.
Number of Traps since log last viewed	The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, Web display, upload file from switch etc.) will cause this counter to be cleared to 0.
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.

## Event Logs

This panel displays the event log, which contains error messages from the system. Event log is not cleared on a system reset.

To access the Event Log page, click **Monitoring > Logs > Event Logs**.

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit Slots

System Switching Routing QoS Security **Monitoring** Maintenance Help Index [LOGOUT](#)

Ports **Logs** Monitoring [eFlow](#)

> Buffered Logs  
 > Command Log  
 > Configuration  
 > Console Log  
 > Sys Log  
 > Configuration  
 > Trap Logs  
 > **Event Logs**  
 > Persistent Logs

### Event Logs

Entry	Type	Filename	Line	TaskID	Code	Time
1	EVENT>	bootos.c	231	0	AAAAAAAA	0 0 0 7
2	EVENT>	unitmgr.c	5032	3	00000000	3 3 26 28
3	EVENT>	bootos.c	231	0	AAAAAAAA	0 0 0 7
4	EVENT>	unitmgr.c	5781	0	00000000	0 0 5 22
5	EVENT>	bootos.c	229	0	AAAAAAAA	0 0 0 20
6	EVENT>	unitmgr.c	5032	7	00000000	7 16 40 43
7	EVENT>	bootos.c	231	0	AAAAAAAA	0 0 0 7
8	EVENT>	unitmgr.c	5032	2	00000000	2 16 51 28
9	EVENT>	bootos.c	231	0	AAAAAAAA	0 0 0 6
10	EVENT>	bootos.c	231	0	AAAAAAAA	0 0 0 6
11	EVENT>	unitmgr.c	5032	1	00000000	1 9 27 27
12	EVENT>	bootos.c	231	0	AAAAAAAA	0 0 0 6
13	EVENT>	unitmgr.c	5032	0	00000000	0 0 7 45
14	EVENT>	bootos.c	231	0	AAAAAAAA	0 0 0 6
15	EVENT>	unitmgr.c	5032	0	00000000	0 0 11 32
16	EVENT>	bootos.c	227	0	AAAAAAAA	0 0 0 6
17	EVENT>	unitmgr.c	5032	18	00000000	18 16 23 4
18	EVENT>	bootos.c	227	0	AAAAAAAA	0 0 0 6
19	EVENT>	unitmgr.c	5032	0	00000000	0 0 8 41
20	EVENT>	bootos.c	227	0	AAAAAAAA	0 0 0 6
21	EVENT>	bootos.c	227	0	AAAAAAAA	0 0 0 7
22	EVENT>	unitmgr.c	5032	3	00000000	3 18 48 38

← →

[CLEAR](#) [REFRESH](#)

Copyright © 1996-2010 Netgear ®

The following table describes the Event Log information displayed on the screen.

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.

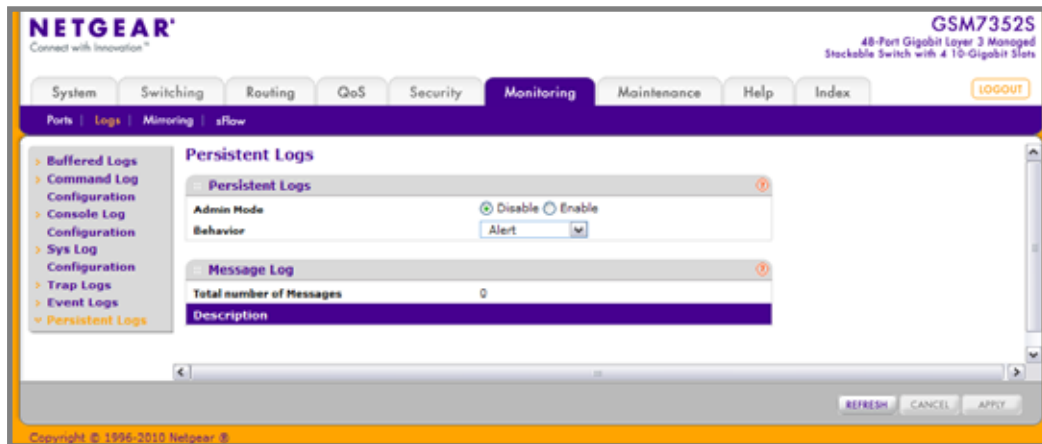
**Table 7-117.**

Field	Description
Entry	The sequence number of the event.
Type	The type of the event.
File Name	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time this event occurred.

## Persistent Logs

A persistent log is a log that is stored in persistent storage. Persistent storage survives across platform reboots. The first log type is the system startup log. The system startup log stores the first N messages received after system reboot. The second log type is the system operation log. The system operation log stores the last N messages received during system operation.

To access the Persistent Logs page, click **Monitoring > Logs > Persistent Logs**.



1. A log that is “Disabled” shall not log messages. A log that is “Enabled” shall log messages. Enable or Disable logging by selecting the corresponding line on the pull-down entry field.
2. **Behavior.** A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the pull-down entry field. These severity levels have been enumerated below:
  - Emergency (0) - system is unusable
  - Alert (1) - action must be taken immediately
  - Critical (2) - critical conditions
  - Error (3) - error conditions
  - Warning (4) - warning conditions
  - Notice(5) - normal but significant conditions
  - Informational(6) - informational messages
  - Debug(7) - debug-level messages
3. Click **REFRESH** to refresh the web page to show the latest messages in the persistent log.

### Format of the messages

- Total number of Messages: Number of persistent log messages displayed on the switch.
- <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt\_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry

The above example indicates a user-level message (1) with severity 7 (debug) on a system that is not stack and generated by component MSTP running in thread id 2110 on Aug 24 05:34:05 by line 318 of file mstp\_api.c. This is the 237th message logged. Messages logged to a collector or relay via syslog have an identical format to the above message.

## Port Mirroring

The page under the Mirroring link allows you to view and configure port mirroring on the system.

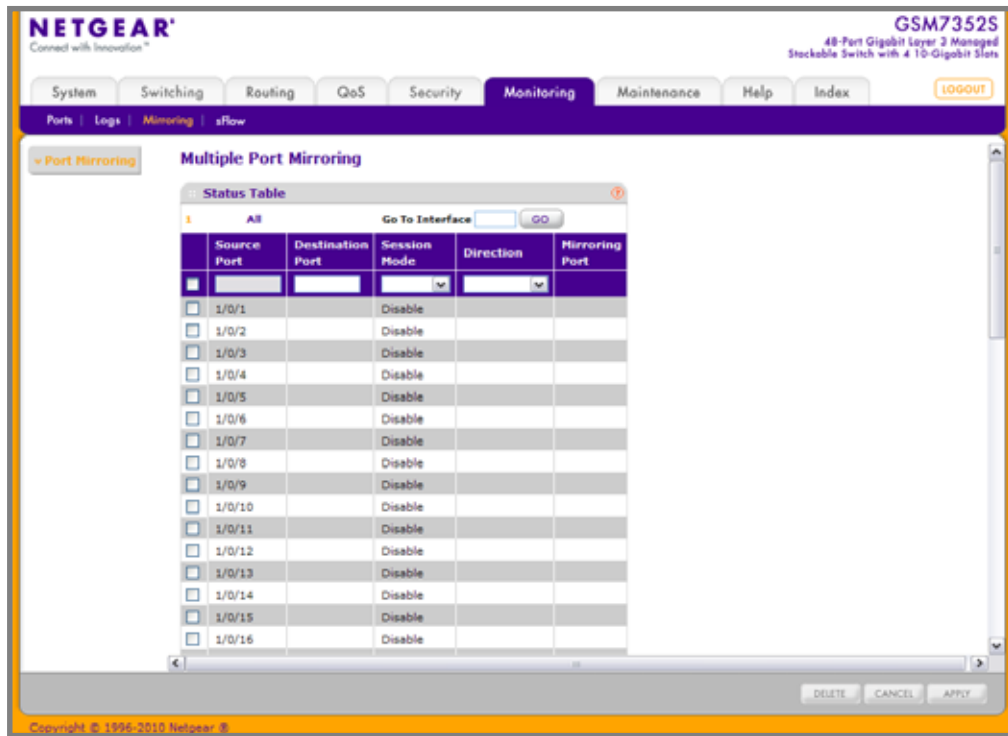
### Multiple Port Mirroring

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 > Mirroring > Port Mirroring**.





To configure Port Mirroring:

1. Select the check box next to a port to configure it as a source port.
  - **Mode** - Specifies the Mode for mirroring. By default Mode is disabled.
2. Use **Source Port** to specify the configured port(s) as mirrored port(s). Traffic of the configured port(s) is sent to the probe port.
3. In the **Destination Port** field, specify the port to which port traffic is be copied. Use the unit/slot/port format to specify the port. You can configure only one destination port on the system. Acts as a probe port and will receive all the traffic from configured mirrored port(s). Default value is blank.
4. 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.
5. **Direction** - Specifies the direction of the Traffic to be mirrored from the configured mirrored port(s). Default value is Tx and Rx.
6. Click **Apply** to apply the settings to the system. If the port is configured as a source port, the **Mirroring Port** field value is Mirrored.
7. To delete a mirrored port, select the check box next to the mirrored port, and then 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.

Table 7-118.

Field	Description
Mirroring Port	Indicates the port to be in a mirrored state.

## sFlow

From the sFlow link under the Monitoring tab, you can access the following pages:

- [Basic](#) on page 573
- [Advanced](#) on page 575

### Basic

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

- [sFlow Agent](#) on page 573

#### sFlow Agent

To display the sFlow Agent page, click **Monitoring** > **sFlow** > **Basic** > **sFlow Agent**.

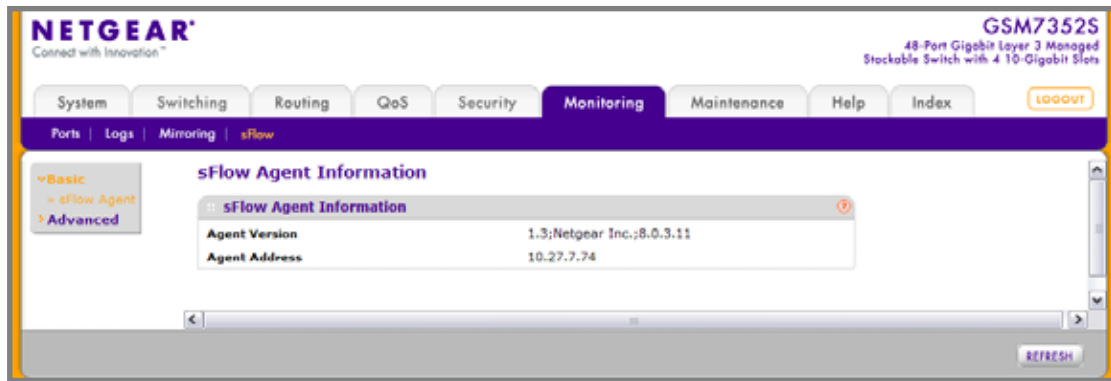


Table 7-119.

Field	Description
<b>Agent Version</b>	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version;Organization;Software Revision where: <ul style="list-style-type: none"> <li>• MIB Version: '1.3', the version of this MIB.</li> <li>• Organization: NETGEAR Inc.</li> <li>• Revision: 1.0</li> </ul>
<b>Agent Address</b>	The IP address associated with this agent.

Click **REFRESH** to refresh the web page to show the latest sFlow agent information.

## Advanced

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

- [sFlow Agent](#) on page 575
- [sFlow Receiver Configuration](#) on page 576
- [sFlow Interface Configuration](#) on page 577

### sFlow Agent

To display the sFlow Agent page, click **Monitoring** > **sFlow** > **Advanced** > **sFlow Agent**.

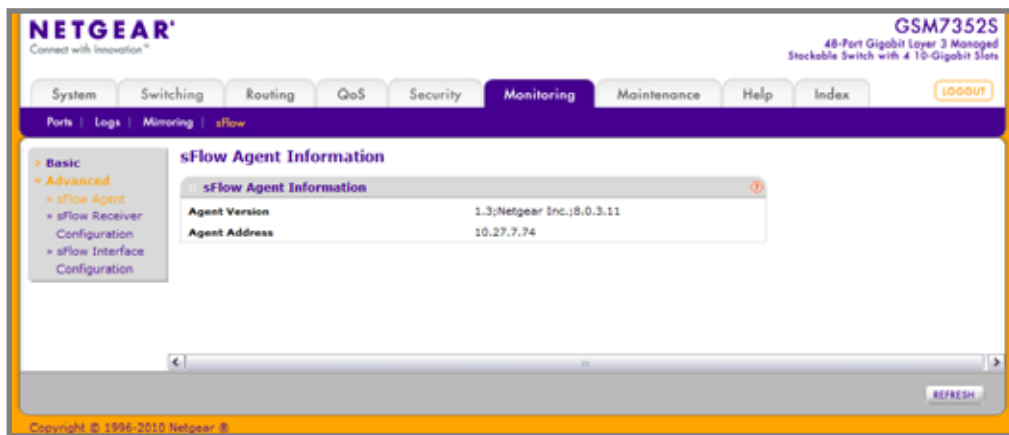


Table 7-120.

Field	Description
Agent Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version;Organization;Software Revision where: <ul style="list-style-type: none"> <li>• MIB Version: '1.3', the version of this MIB.</li> <li>• Organization: NETGEAR Inc.</li> <li>• Revision: 1.0</li> </ul>
Agent Address	The IP address associated with this agent.

Click **REFRESH** to refresh the web page to show the latest sFlow agent information.

## sFlow Receiver Configuration

To display the sFlow Receiver Configuration page, click **Monitoring > sFlow > Advanced > sFlow Receiver Configuration**.

Receiver Index	Receiver Owner	Receiver Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
1		0	1400	0.0.0.0	6343	5
2		0	1400	0.0.0.0	6343	5
3		0	1400	0.0.0.0	6343	5
4		0	1400	0.0.0.0	6343	5
5		0	1400	0.0.0.0	6343	5
6		0	1400	0.0.0.0	6343	5
7		0	1400	0.0.0.0	6343	5
8		0	1400	0.0.0.0	6343	5

1. **Receiver Index.** Selects the receiver for which data is to be displayed or configured. Allowed range is 1 to 8.
2. Use **Receiver Owner** to specify the entity making use of this sFlowRcvrTable entry. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string. The entry must be claimed before any changes can be made to other sampler objects.
3. Use **Receiver Timeout** to specify the time (in seconds) remaining before the sampler is released and stops sampling. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. Allowed range is 0 to 4294967295 secs. A value of zero sets the selected receiver configuration to its default values.
4. Use **Maximum Datagram Size** to specify the maximum number of data bytes that can be sent in a single sample datagram. The manager should set this value to avoid fragmentation of the sFlow datagrams. Default Value: 1400. Allowed range is 200 to 9116.
5. Use **Receiver Address** to specify the IP address of the sFlow collector. If set to 0.0.0.0, no sFlow datagrams will be sent.
6. Use **Receiver Port** to specify the destination port for sFlow datagrams. Allowed range is 1 to 65535.

Table 7-121.

Field	Description
Receiver Datagram Version	The version of sFlow datagrams that should be sent.

## sFlow Interface Configuration

sFlow agent collects statistical packet-based sampling of switched flows and sends them to the configured receivers. A data source configured to collect flow samples is called a sampler. sFlow agent also collects time-based sampling of network interface statistics and sends them to the configured sFlow receivers. A data source configured to collect counter samples is called a poller.

To display the sFlow Interface Configuration page, click **Monitoring > sFlow > Advanced > sFlow Interface Configuration**.

**NETGEAR** GSM7352S  
48-Port Gigabit Layer 3 Managed Stackable Switch with 4 10-Gigabit SFPs

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

Home Logs Monitoring **sFlow**

Basic  
Advanced  
sFlow Agent  
sFlow Receiver Configuration  
sFlow Interface Configuration

**sFlow Interface Configuration**

Go To Interface

Interface	Poller		Sampler		
	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
<input type="checkbox"/> 1/0/1	0	0	0	0	128
<input type="checkbox"/> 1/0/2	0	0	0	0	128
<input type="checkbox"/> 1/0/3	0	0	0	0	128
<input type="checkbox"/> 1/0/4	0	0	0	0	128
<input type="checkbox"/> 1/0/5	0	0	0	0	128
<input type="checkbox"/> 1/0/6	0	0	0	0	128
<input type="checkbox"/> 1/0/7	0	0	0	0	128
<input type="checkbox"/> 1/0/8	0	0	0	0	128
<input type="checkbox"/> 1/0/9	0	0	0	0	128
<input type="checkbox"/> 1/0/10	0	0	0	0	128
<input type="checkbox"/> 1/0/11	0	0	0	0	128
<input type="checkbox"/> 1/0/12	0	0	0	0	128
<input type="checkbox"/> 1/0/13	0	0	0	0	128
<input type="checkbox"/> 1/0/14	0	0	0	0	128
<input type="checkbox"/> 1/0/15	0	0	0	0	128
<input type="checkbox"/> 1/0/16	0	0	0	0	128

Copyright © 1996-2012 Netgear, Inc.

1. **Interface** - Interface for this flow poller and sampler. This Agent will support Physical ports only.
2. Use **Receiver Index** to specify the allowed range for the sFlowReceiver associated with this counter poller. Allowed range is 1 to 8.
3. Use **Poller Interval** to specify the maximum number of seconds between successive samples of the counters associated with this data source. A sampling interval of 0 disables counter sampling. Allowed range is 0 to 86400 secs.
4. Use **Receiver Index** to specify the sFlow Receiver for this flow sampler. If set to 0, the sampler configuration is set to default and the sampler is deleted. Only active receivers can be set. If a receiver expires then all samplers associated with the receiver will also expire. Allowed range is 1 to 8.
5. Use **Sampling Rate** to specify the statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A sampling rate of 0 disables sampling. Allowed range is 1024 to 65536.
6. Use **Maximum Header Size** to specify the maximum number of bytes that should be copied from a sampled packet. Allowed range is 20 to 256.

Use the features available from the Maintenance tab to help you manage the switch. The Maintenance tab contains links to the following features:

- [Save Configuration](#) on page 578
- [Reset](#) on page 580
- [Upload File From Switch](#) on page 583
- [Download File To Switch](#) on page 587
- [File Management](#) on page 592
- [Troubleshooting](#) on page 595

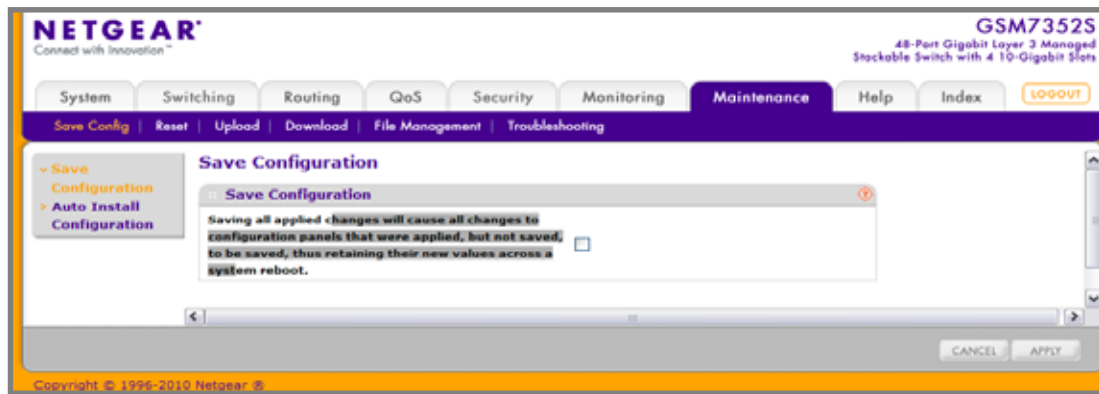
## Save Configuration

The **Save Configuration** menu contains links to the following options:

- [Save Configuration](#) on page 578
- [Auto Install Configuration](#) on page 580

## Save Configuration

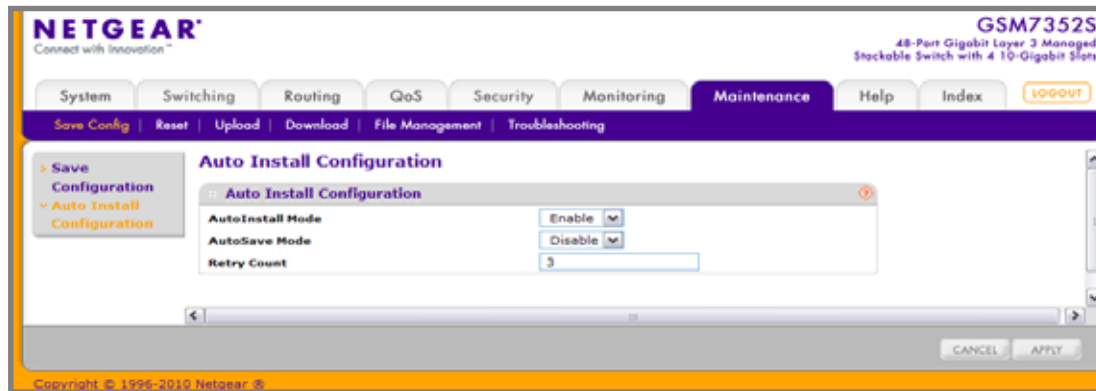
To access the Save Configuration page, click **Maintenance** > **Save Config** > **Save Configuration**.



1. Select the check box and click the **APPLY** button to have configuration changes you have made saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

## Auto Install Configuration

To access the Auto Install Configuration page, click **Maintenance > Save Config> Auto Install Configuration**.



1. Use **Auto Install** to enable/disable start/stop auto install mode on the switch.
2. Select the **Auto Save** check box and click the **APPLY** button to have configuration changes you have made saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.
3. Use **Auto Install Retry Count** to specify the number of times the unicast TFTP tries should be made for the DHCP specified file before falling back for broadcast TFTP tries.

## Reset

The **Reset** menu contains links to the following options:

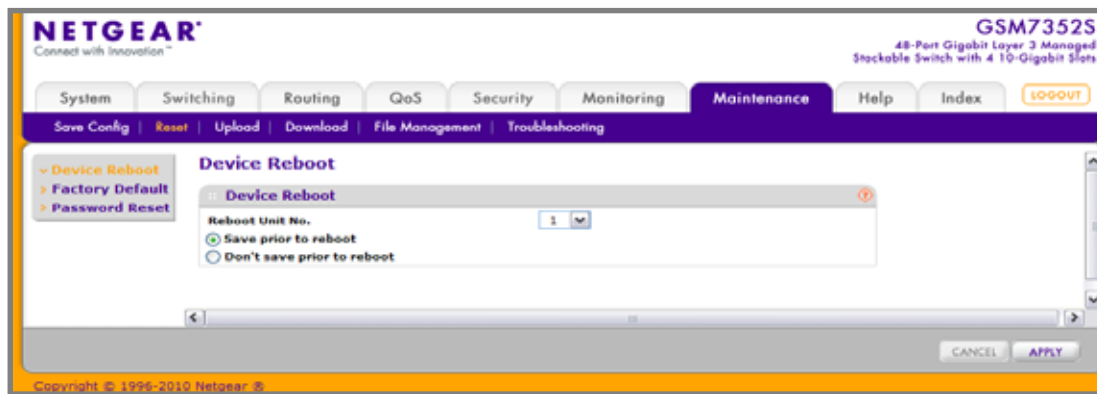
- [Device Reboot](#) on page 580
- [Factory Default](#) on page 582
- [Password Reset](#) on page 583

## Device Reboot

Use the Device Reboot page to reboot ProSafe® Managed Switches.

To access the Device Reboot page, click **Maintenance > Reset > Device Reboot**.





To reboot the switch:

1. Use **Reboot Unit No** to select the unit to reset. Select all to run reset for all units.
2. Select the **Save prior to reboot** radio button and click the **APPLY** button to reboot the switch. Prior to reboot the unit, the current configuration will be saved first.
3. Select the **Don't save prior to reboot** radio button and click the **APPLY** button to reboot the switch. This option permits the user to reboot the unit without saving the current configuration.

## Factory Default

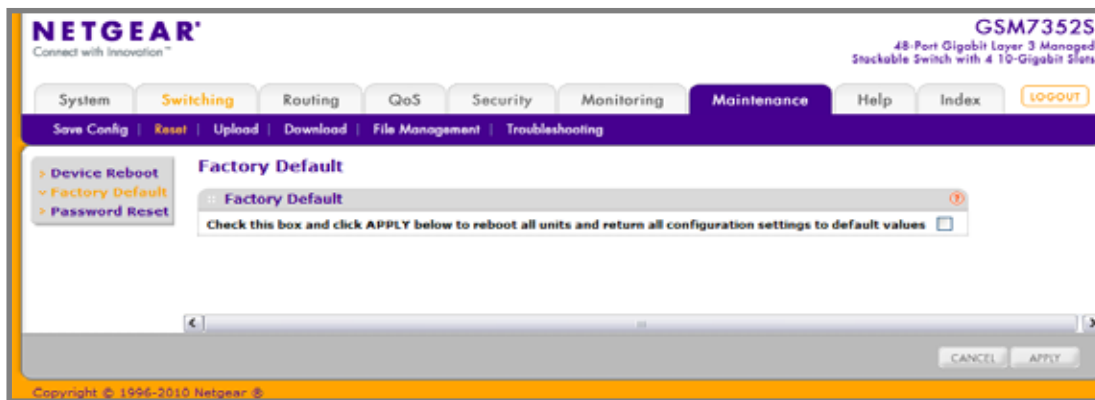
Use the Factory Default page to reset the system configuration to the factory default values.

---

**Note:** If you reset the switch to the default configuration, the IP address is reset to 169.254.100.100, and the DHCP client is enabled. If you lose network connectivity after you reset the switch to the factory defaults, see [Web Access](#) on page 9.

---

To access the Factory Defaults page, click **Maintenance > Reset > Factory Default**.



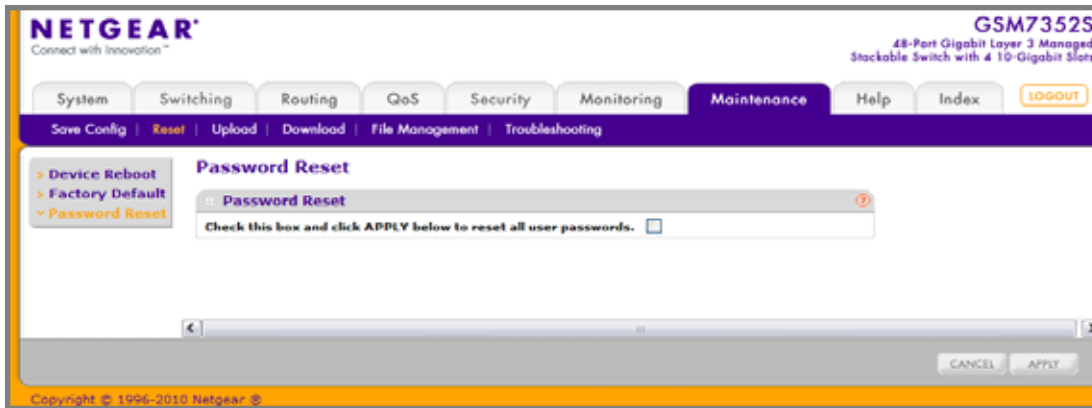
To reset the switch to the factory default settings:

1. Select the check box and click the **APPLY** button to have all configuration parameters reset to their factory default values. All changes you have made will be lost, even if you have issued a save. You will be shown a confirmation screen after you select the button.

## Password Reset

Use the Password Reset page to reset all user passwords to defaults.

To access the Password Reset page, click **Maintenance** > **Reset** > **Password Reset**.



1. Select the check box and click the **APPLY** button to have all user passwords reset to their factory default values. All changes you have made will be lost, even if you have issued a save.

## Upload File From Switch

Use the File Upload page to upload configuration (ASCII), log (ASCII), and image (binary) files from the switch to the TFTP server.

The Upload menu contains links to the following options:

- [File Upload](#) on page 583
- [HTTP File Upload](#) on page 586
- [USB File Upload](#) on page 587

## File Upload

To display the File Upload page, click **Maintenance** > **Upload** > **File Upload**.

The screenshot displays the Netgear web management interface for a GSM7352S switch. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance (selected), Help, and Index. A 'LOGOUT' button is located in the top right corner. Below the navigation bar, a secondary bar contains links for Save Config, Reset, Upload (selected), Download, File Management, and Troubleshooting. The main content area is titled 'File Upload' and features a sidebar with 'File Upload' and 'HTTP File Upload' options. The 'File Upload' form includes the following fields: File Type (set to Archive), Image Name (set to image1), Transfer Mode (set to TFTP), Server Address Type (set to IPv4), Server Address (set to 0.0.0.0), and Remote File Name (empty). At the bottom of the form are 'CANCEL' and 'APPLY' buttons. The footer of the interface shows the copyright notice: Copyright © 1996-2010 Netgear, Inc.

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed  
Stackable Switch with 4 10-Gigabit Slots

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

Save Config Reset **Upload** Download File Management Troubleshooting

File Upload  
File Upload

File Type Archive  
Image Name image1  
Transfer Mode TFTP  
Server Address Type IPv4  
Server Address 0.0.0.0  
Remote File Name

CANCEL APPLY

Copyright © 1996-2010 Netgear, Inc.

To upload a file from the switch to the TFTP server:

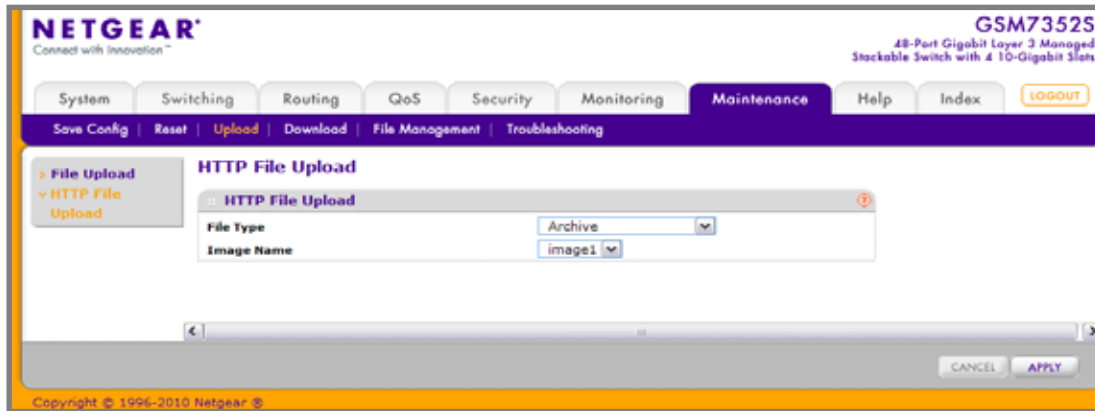
1. Use **File Type** to specify what type of file you want to upload:
  - **Archive** - Specify archive (STK) code when you want to retrieve from the operational flash:
    - **Image1** - Specify the code image1 when you want to retrieve.
    - **Image2** - Specify the code image2 when you want to retrieve.
  - **CLI Banner** - Specify CLI Banner when you want retrieve the CLI banner file.
  - **Startup Configuration** - Specify configuration when you want to retrieve the stored configuration.
  - **Text Configuration** - Specify configuration in text mode when you want to retrieve the stored configuration.
  - **Script File** - Specify script file when you want to retrieve the stored configuration.
  - **Error Log** - Specify error log to retrieve the system error (persistent) log, sometimes referred to as the event log.
  - **Buffered Log** - Specify buffered log to retrieve the system buffered (in-memory) log.
  - **Trap Log** - Specify trap log to retrieve the system trap records.
  - **Tech Support** - Specify Tech Support to retrieve the switch information needed for trouble-shooting.

The factory default is Archive.

2. Use **Transfer Mode** to specify what protocol to use to transfer the file:
  - **TFTP** - Trivial File Transfer Protocol
  - **SFTP** - Secure File Transfer Program
  - **SCP** - Secure Copy
3. Use **Server Address Type** to specify either IPv4 or IPv6 to indicate the format of the Server Address field. The factory default is IPv4.
4. Use **Server Address** to enter the IP address of the server in accordance with the format indicated by the Seer Address Type. The factory default is the IPv4 address 0.0.0.0.
5. Use **Remote File Name** to enter the name of the file you want to download from the server. You may enter up to 32 characters. The factory default is blank.
6. Use **User Name** to enter the username for remote login to SFTP/SCP server where the file will be sent. This field is visible only when SFTP or SCP transfer modes are selected.
7. Use **Password** to enter the password for remote login to SFTP/SCP server where the file will be sent. This field is visible only when SFTP or SCP transfer modes are selected.
8. The last row of the table is used to display information about the progress of the file transfer.

## HTTP File Upload

To display the HTTP File Upload page, click **Maintenance** > **Upload** > **HTTP File Upload**.



1. Use **File Type** to specify what type of file you want to upload:
  - **Archive** - Specify archive (STK) code when you want to retrieve from the operational flash:
    - **Image1** - Specify the code image1 when you want to retrieve.
    - **Image2** - Specify the code image2 when you want to retrieve.
  - **CLI Banner** - Specify CLI Banner when you want retrieve the CLI banner file.
  - **Startup Configuration** - Specify configuration when you want to retrieve the stored configuration.
  - **Text Configuration** - Specify configuration in text mode when you want to retrieve the stored configuration.
  - **Script File** - Specify script file when you want to retrieve the stored configuration.
  - **Error Log** - Specify error log to retrieve the system error (persistent) log, sometimes referred to as the event log.
  - **Trap Log** - Specify trap log to retrieve the system trap records.
  - **Buffered Log** - Specify buffered log to retrieve the system buffered (in-memory) log.
  - **Tech Support** - Specify Tech Support to retrieve the switch information needed for troubleshooting.

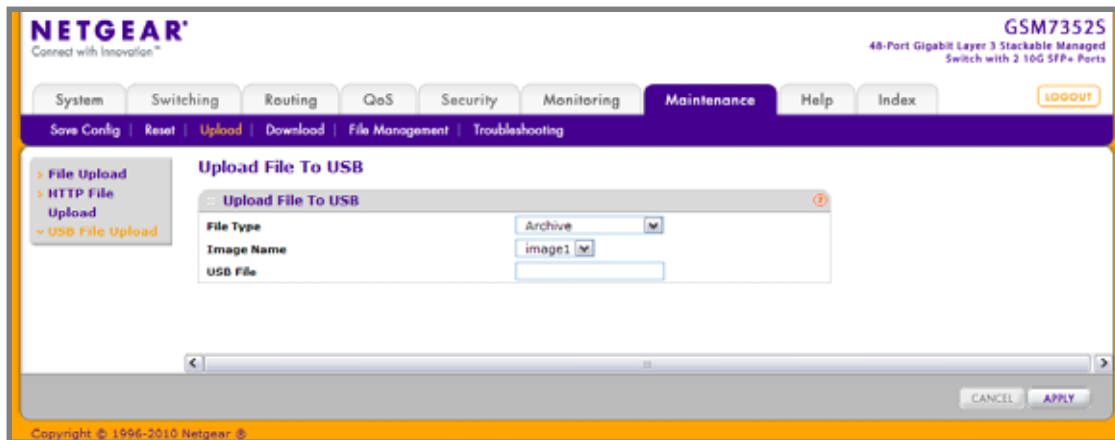
The factory default is Archive.

2. Use **Local File Name** to specify the local script file name you want to upload.

## USB File Upload

Use this menu to upload a file from the switch to USB device.

To display the Upload File to USB page, click **Maintenance** > **Upload** > **USB File Upload**.



1. Use **File Type** to specify what type of file you want to upload:
  - a. Use **Archive** to specify archive (STK) code when you want to retrieve from the operational flash.
    - **Image1** - Specify the code image1 when you want to retrieve.
    - **Image2** - Specify the code image2 when you want to retrieve.
  - b. Use **Text Configuration** to specify configuration in text mode when you want to retrieve the stored configuration.
- The factory default is image1.
2. Use **USB File** to specify a name along with path for the file you want to upload. You may enter up to 32 characters. The factory default is blank.
3. The last row of the table is used to display information about the progress of the file transfer.

## Download File To Switch

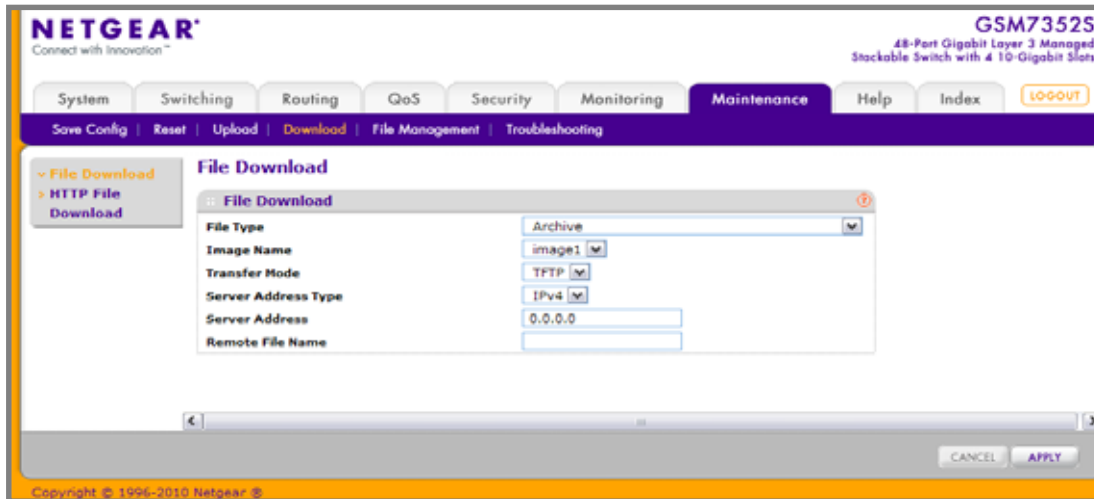
The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.

The Download menu contains links to the following options:

- [File Download](#) on page 588
- [HTTP File Download](#) on page 589
- [USB File Download](#) on page 592

## File Download

To display the File Download page, click **Maintenance** > **Download** > **File Download**.



1. Use **File Type** to specify what type of file you want to transfer.
  - **Archive** - Specify archive (STK) code when you want to upgrade the operational flash:
    - **Image1** - Specify the code image1 you want to download.
    - **Image2** - Specify the code image2 you want to download.
  - **CLI Banner** - Specify CLI Banner when you want a banner to be displayed before the login prompt.
  - **Configuration** - Specify configuration when you want to update the switch's configuration. If the file has errors the update will be stopped.
  - **Text Configuration** - Specify configuration in text mode when you want to update the switch's configuration. If the file has errors the update will be stopped.
  - Use **Config Script** to specify script configuration file.
  - Use **SSH-1 RSA Key File** to specify SSH-1 Rivest-Shamir-Adleman (RSA) Key File.
  - Use **SSH-2 RSA Key PEM File** to specify SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded).
  - Use **SSH-2 DSA Key PEM File** to specify SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded).
  - Use **SSL Trusted Root Certificate PEM File** to specify SSL Trusted Root Certificate File (PEM Encoded).
  - Use **SSL Server Certificate PEM File** to specify SSL Server Certificate File (PEM Encoded).
  - Use **SSL DH Weak Encryption Parameter PEM File** to specify SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).



- Use **SSL DH Strong Encryption Parameter PEM File** to specify SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)
- **License Key** - Specify license key in order to support licensing features.

The factory default is Image1.

---

**Note:** To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

---



---

**Note:** To download SSL PEM files SSL must be administratively disabled and there can be no active SSH sessions.

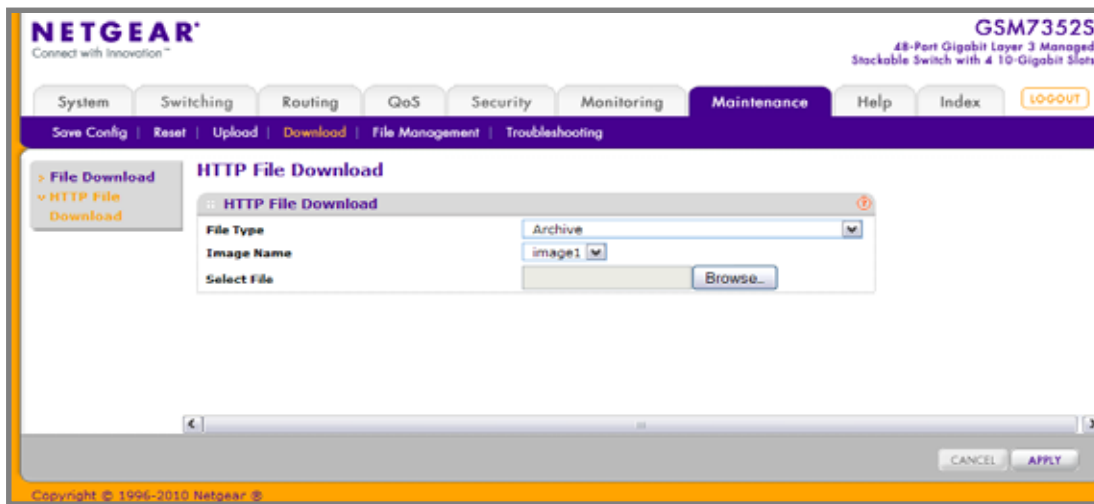
---

2. Use **Transfer Mode** to specify what protocol to use to transfer the file:
  - **TFTP** - Trivial File Transfer Protocol
  - **SFTP** - Secure File Transfer Program
  - **SCP** - Secure Copy
3. Use **Server Address Type** to specify either IPv4 or IPv6 to indicate the format of the TFTP/SFTP/SCP Server Address field. The factory default is IPv4.
4. Use **Server Address** to enter the IP address of the server in accordance with the format indicated by the Server Address Type. The factory default is the IPv4 address 0.0.0.0.
5. Use **Remote File Name** to enter the name of the file you want to download from the server. You may enter up to 32 characters. The factory default is blank.
6. Use **User Name** to enter the username for remote login to SFTP/SCP server where the file resides. This field is visible only when SFTP or SCP transfer modes are selected.
7. Use **Password** to enter the password for remote login to SFTP/SCP server where the file resides. This field is visible only when SFTP or SCP transfer modes are selected.
8. The last row of the table is used to display information about the progress of the file transfer. The screen will refresh automatically until the file transfer completes.

## 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 by using HTTP:

1. Use **File Type** to specify what type of file you want to transfer:

- **Archive** - Specify archive (STK) code when you want to upgrade the operational flash:
  - **Image1** - Specify the code image1 you want to download.
  - **Image2** - Specify the code image2 you want to download.
- **CLI Banner** - Specify CLI Banner when you want a banner to be displayed before the login prompt.
- **Configuration** - Specify configuration when you want to update the switch's configuration. If the file has errors the update will be stopped.
- **Text Configuration** - Specify configuration in text mode when you want to update the switch's configuration. If the file has errors the update will be stopped.
- Use **Config Script** to specify script configuration file.
- Use **SSH-1 RSA Key File** to specify SSH-1 Rivest-Shamir-Adleman (RSA) Key File.
- Use **SSH-2 RSA Key PEM File** to specify SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded)
- Use **SSH-2 DSA Key PEM File** to specify SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded)
- Use **SSL Trusted Root Certificate PEM File** to specify SSL Trusted Root Certificate File (PEM Encoded)
- Use **SSL Server Certificate PEM File** to specify SSL Server Certificate File (PEM Encoded)
- Use **SSL DH Weak Encryption Parameter PEM File** to specify SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded)
- Use **SSL DH Strong Encryption Parameter PEM File** to specify SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)

- **License Key** - Specify license key in order to support licensing features.

The factory default is Archive.

2. If you are downloading a GSM7352Sv1 or GSM7352Sv2 image (Archive), select the image on the switch to overwrite. 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 file upload window 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.

---

---

**Note:** To download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

---

---

**Note:** To download SSL PEM files SSL must be administratively disabled and there can be no active SSH sessions.

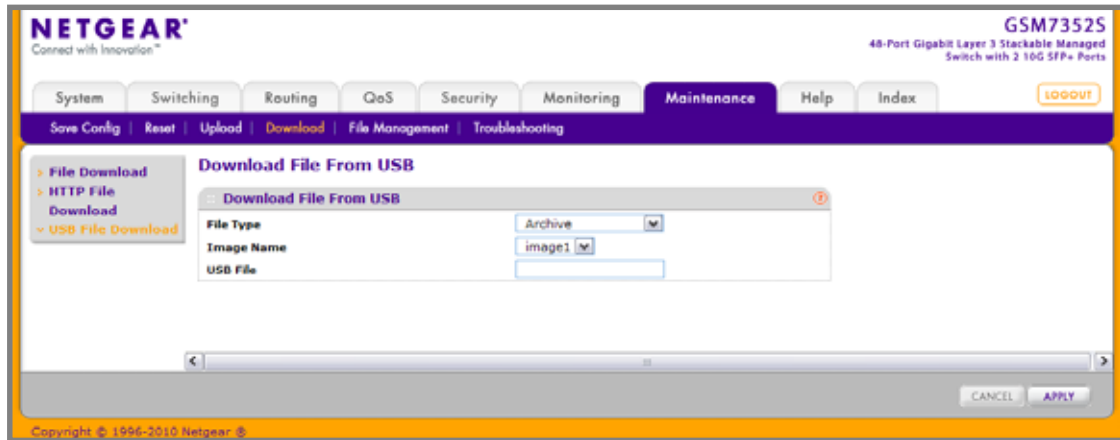
---

6. Use **Select File** to browse/give name along with path for the file you want to download. You may enter up to 80 characters. The factory default is blank.
7. **Download Status** - Displays the status during transfer file to the switch.

## USB File Download

Use this menu to download a file to the switch from a USB device.

To display this page, click **Maintenance** > **Download** > **USB File Download**.



1. Use **File Type** to specify what type of file you want to transfer:
  - a. Use **Archive** to specify archive (STK) code when you want to download to the operational flash:
    - **Image1** - Specify the code image1 when you want to download.
    - **Image2** - Specify the code image2 when you want to download.
  - b. Use **Text Configuration** to specify configuration in text mode when you want to update the switch's configuration. If the file has errors the update will be stopped.

The factory default is Image1.

2. Use **USB File** to specify a name along with path for the file you want to download. You may enter up to 32 characters. The factory default is blank.
3. **Download Status** displays the status during transfer file to the switch.
4. The last row of the table is used to display information about the progress of the file transfer. The screen will refresh automatically until the file transfer completes.

## File Management

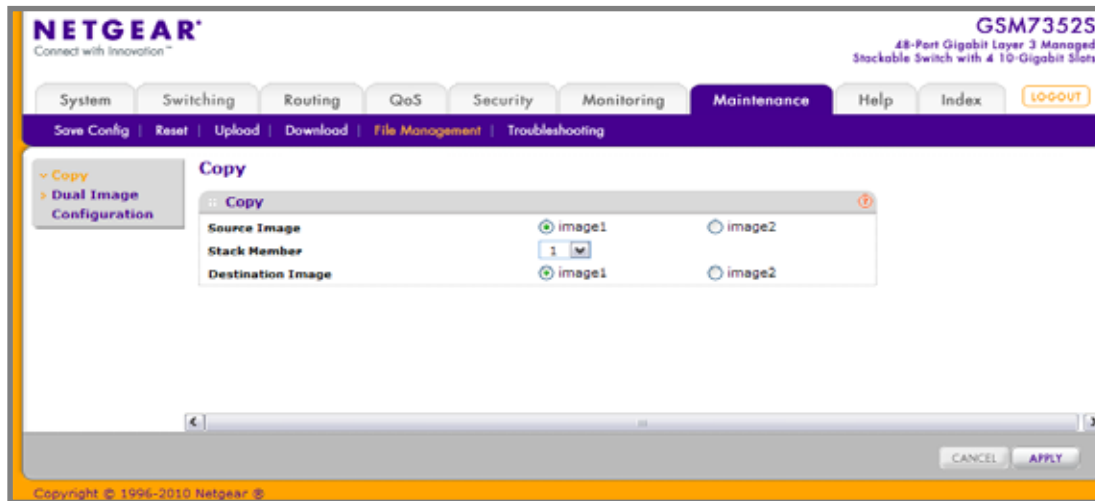
The system maintains two versions of the ProSafe® Managed Switches software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded during subsequent switch restarts. This feature reduces switch down time when upgrading or downgrading the ProSafe® Managed Switches software.

The **File Management** menu contains links to the following options:

- [Copy](#) on page 593
- [Dual Image Configuration](#) on page 594

## Copy

To display the Copy page, click **Maintenance** > **File Management** > **Copy**.



1. Use **Source Image** to select the image1 or image2 as source image when copy occurs.
2. Use **Stack member** to select the destination unit to which you are going to copy from master.
3. Use **Destination Image** to select the image1 or image2 as destination image when copy occurs.

## Dual Image Configuration

The Dual Image feature allows switch to retain two images in permanent storage. The user designates one of these images as the active image to be loaded during subsequent switch restarts. This feature reduces switch down time when upgrading / downgrading the image.

To display the Dual Image Configuration page, click **Maintenance > File Management > Dual Image Configuration**.

**NETGEAR**  
Connect with Innovation™

GSM7352S  
48-Port Gigabit Layer 3 Managed  
Stackable Switch with 4 10-Gigabit Slots

System Switching Routing QoS Security Monitoring **Maintenance** Help Index **LOG-OUT**

Save Config | Reset | Upload | Download | **File Management** | Troubleshooting

> Copy  
v Dual Image  
Configuration

### Dual Image Configuration

	Unit	Image Name	Active Image	Next Active Image	Description	Version	Update Bootcode
<input type="checkbox"/>							True
<input type="checkbox"/>	1	image1	True	True	default image	8.0.3.11	True
<input type="checkbox"/>	1	image2	False	False		N.7.20.1	True

DELETE CANCEL APPLY

Copyright © 1996-2010 Netgear ®

To configure Dual Image settings:

1. Use **Unit** to select the unit whose code image you want to activate, update, or delete.
2. Use **Image Description** to specify the description for the image that you have selected.
3. Use **Next Active Image** to make the selected image the next active image for subsequent reboots.
4. Use **Update Bootcode** to update the bootloader with the selected image.
5. Click **DELETE** to delete the selected image from permanent storage on the switch.
6. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

---

**Note:** After activating an image, you must perform a system reset of the switch in order to run the new code.

---

Table 8-122.

Field	Description
Image Name	This displays the image name for the selected unit.
Active Image	Displays the current active image of the selected unit.
Version	Displays the version of the image1 code file.

## Troubleshooting

The **Troubleshooting** menu contains links to the following options:

- [Ping IPv4](#) on page 595
- [Ping IPv6](#) on page 598
- [Traceroute IPv4](#) on page 599
- [Traceroute IPv6](#) on page 601

### Ping IPv4

Use this screen to tell the switch to send a Ping request to a specified IP address. You can use this to check whether the switch can communicate with a particular IP station. Once you click the APPLY button, the switch will send specified number of ping requests and the results will be displayed.

If a reply to the ping is not received, you will see:

- Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec

If a reply to the ping is received, you will see:

- Received response for Seq Num 0 Rtt xyz usec
- Received response for Seq Num 1 Rtt abc usec
- Received response for Seq Num 2 Rtt def usec
- Tx = Count, Rx = Count Min/Max/Avg RTT = xyz/abc/def msec.

To access the Ping IPv4 page, click **Maintenance > Troubleshooting > Ping IPv4**.

The screenshot displays the Netgear web management interface for a GSM7352S switch. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance (selected), Help, and Index. A secondary bar contains links for Save Config, Reset, Upload, Download, File Management, and Troubleshooting. The left sidebar lists navigation options: Ping IPv4 (selected), Ping IPv6, Traceroute IPv4, and Traceroute IPv6. The main content area is titled 'Ping' and features a 'Details' section with the following fields: IP Address/Host Name (text input), Count (1, range 1 to 15), Interval(secs) (3, range 1 to 60), and Datagram Size (0, range 0 to 65507). Below these fields is a 'Ping' status area. At the bottom right of the main area are 'CANCEL' and 'APPLY' buttons. The footer shows the copyright notice: Copyright © 1996-2010 Netgear.

**NETGEAR**  
Connect with Innovation™

**GSM7352S**  
48-Port Gigabit Layer 3 Managed  
Stackable Switch with 4 10-Gigabit Slots

System Switching Routing QoS Security Monitoring **Maintenance** Help Index [LOG-OUT](#)

[Save Config](#) [Reset](#) [Upload](#) [Download](#) [File Management](#) [Troubleshooting](#)

▼ Ping IPv4  
➤ Ping IPv6  
➤ Traceroute IPv4  
➤ Traceroute IPv6

### Ping

**Details**

IP Address/Host Name

Count  (1 to 15)

Interval(secs)  (1 to 60)

Datagram Size  (0 to 65507)

Ping

[CANCEL](#) [APPLY](#)

Copyright © 1996-2010 Netgear ®



To configure the settings and ping a host on the network:

1. Use **IP Address/Host Name** to enter the IP address or Hostname of the station you want the switch to ping. The initial value is blank. The IP Address or Hostname you enter is not retained across a power cycle.
2. Optionally, configure the following settings:
  - **Count** - Enter the number of echo requests you want to send. The initial value is default value. The Count you enter is not retained across a power cycle.
  - **Interval(secs)** - Enter the Interval between ping packets in seconds. initial value is default value. The Interval you enter is not retained across a power cycle.
  - **Datagram Size** - Enter the Size of ping packet. initial value is default value. The Size you enter is not retained across a power cycle.
3. **PING** displays the result after the switch sends a Ping request to the specified address.
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 **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.

## Ping IPv6

This screen is used 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. Once you click the Apply button, the switch will send three pings and the results will be displayed below the configurable data. The output will be Send count=3, Receive count=n from (IPv6 Address). Average round trip time = n ms.

To access the Ping IPv6 page, click **Maintenance** > **Troubleshooting** > **Ping IPv6**.

1. Use **Ping** to select either global IPv6 Address, Hostname, or Link Local Address to ping.
2. Use **IPv6 Address/Hostname** to 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.
3. Use **Datagram Size** to enter the datagram size. The valid range is (48 to 2048).

## Traceroute IPv4

Use this screen to tell the switch to send a TraceRoute request to a specified IP address or Hostname. You can use this to discover the paths packets take to a remote destination. Once you click the **Apply** button, the switch will send traceroute and the results will be displayed below the configurable data.

If a reply to the traceroute is received, you will see:

- 1 x.y.z.w 9869 usec 9775 usec 10584 usec
- 2 0.0.0.0 0 usec \* 0 usec \* 0 usec \*
- 3 0.0.0.0 0 usec \* 0 usec \* 0 usec \*
- Hop Count = w Last TTL = z Test attempt = x Test Success = y.

To display the Traceroute IPv4 page, click **Maintenance > Troubleshooting > Traceroute IPv4**.

The screenshot shows the Netgear web interface for a GSM7352S switch. The 'Maintenance' tab is selected, and the 'Troubleshooting' section is active. The 'Traceroute IPv4' page is displayed, featuring a sidebar with navigation links: 'Ping IPv4', 'Ping IPv6', 'Traceroute IPv4' (selected), and 'Traceroute IPv6'. The main content area is titled 'TraceRoute' and contains a form with the following fields:

Field	Value	Range/Description
IP Address/Hostname		(Max 255 Characters/x.x.x.x.x)
Probes Per Hop	3	(1 to 10)
MaxTTL	30	(1 to 255)
InitTTL	1	(0 to 255)
MaxFail	5	(0 to 255)
Interval(secs)	3	(1 to 60)
Port	33434	(1 to 65535)
Size	0	(0 to 65507)

Below the form is a 'Results' section. At the bottom of the page are 'CANCEL' and 'APPLY' buttons. The footer indicates 'Copyright © 1996-2010 Netgear'.

To configure the Traceroute settings and send probe packets to discover the route to a host on the network:

1. Use **IP Address/Hostname** to enter the IP address or Hostname of the station you want the switch to discover path. The initial value is blank. The IP Address or Hostname you enter is not retained across a power cycle.
2. Optionally, configure the following settings:
  - **Probes Per Hop** - Enter the number of probes per hop. The initial value is default. The Probes per Hop you enter is not retained across a power cycle.
  - **MaxTTL** - Enter the maximum TTL for the destination. The initial value is default value. The MaxTTL you enter is not retained across a power cycle.
  - **InitTTL** - Enter the initial TTL to be used. The initial value is default value. The InitTTL you enter is not retained across a power cycle.
  - **MaxFail** - Enter the maximum Failures allowed in the session. The initial value is default value. The MaxFail you enter is not retained across a power cycle.
  - **Interval(secs)** - Enter the Time between probes in seconds. The initial value is default value. The Interval you enter is not retained across a power cycle.
  - **Port** - Enter the UDP Dest port in probe packets. The initial value is default value. The port you enter is not retained across a power cycle.
  - **Size** - Enter the Size of probe packets. The initial value is default value. The Size you enter is not retained across a power cycle.
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.

## Traceroute IPv6

Use this screen to tell the switch to send a TraceRoute request to a specified IP address or Hostname. You can use this to discover the paths packets take to a remote destination. Once you click the Apply button, the switch will send traceroute and the results will be displayed below the configurable data.

If a reply to the traceroute is received, you will see:

- 1 a:b:c:d:e:f:g 9869 usec 9775 usec 10584 usec
- 2 0:0:0:0:0:0:0:0 0 usec \* 0 usec \* 0 usec \*
- Hop Count = w Last TTL = z Test attempt = x Test Success = y.

To display the Traceroute IPv6 page, click **Maintenance** > **Troubleshooting** > **Traceroute IPv6**.

The screenshot shows the Netgear ProSafe web interface. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. The Maintenance tab is active. Below it, a sub-menu shows Save Config, Reset, Upload, Download, File Management, and Troubleshooting. The Troubleshooting tab is selected, leading to the Traceroute IPv6 page. On the left, a sidebar menu lists options: Ping IPv4, Ping IPv6, Traceroute IPv4, and Traceroute IPv6 (which is highlighted). The main content area is titled 'Traceroute IPv6' and contains two input fields: 'IPv6 Address/Host Name' and 'Port' (with a value of 33434 and a range of 1 to 65535). Below these fields is a 'Results' section. At the bottom of the page are 'CANCEL' and 'APPLY' buttons. The footer indicates 'Copyright © 1996-2010 Netgear Inc.'.

1. Use **IPv6 Address/Hostname** to enter the IPv6 address or Hostname of the station you want the switch to discover path. The initial value is blank. The IPv6 Address or Hostname you enter is not retained across a power cycle.
2. Use **Port** to enter the UDP Dest port in probe packets. The initial value is default value. The port you enter is not retained across a power cycle.

Use the features available from the Help tab to connect to online resources for assistance. The Help tab contains a link to [Online Help](#).

## Online Help

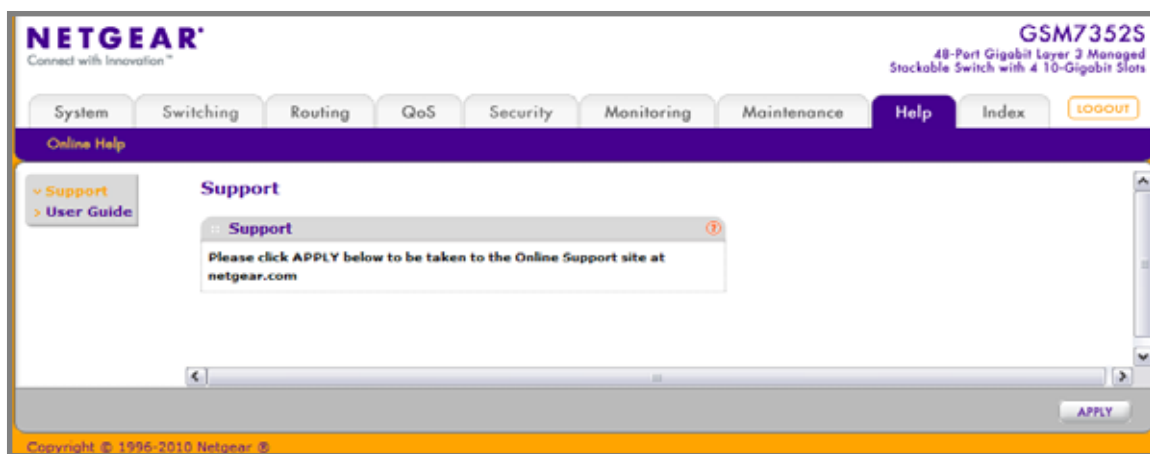
The Online Help includes the following pages:

- [Support](#) on page 602
- [User Guide](#) on page 603

## Support

Use the Support page to connect to the Online Support site at [netgear.com](http://netgear.com).

To access the Support page, click **Help** > **Online Help** > **Support**.

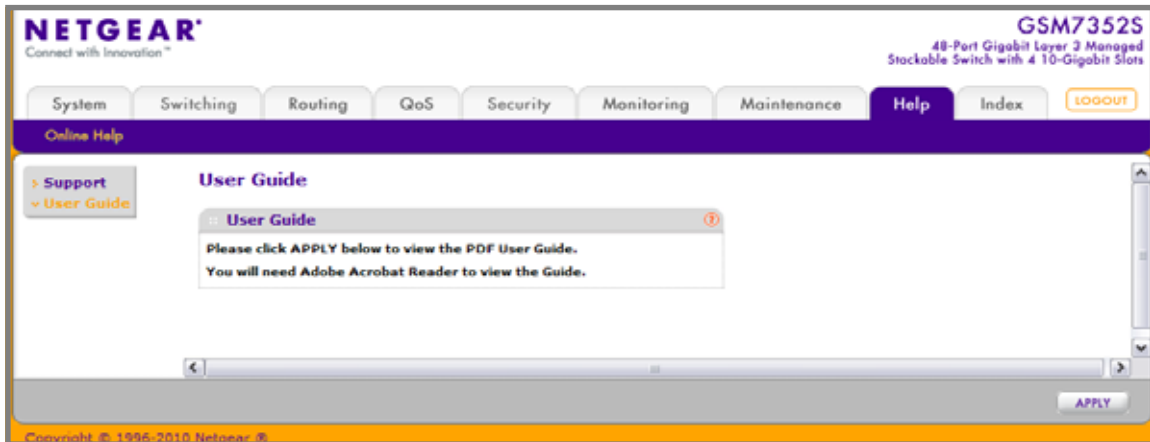


To connect to the NETGEAR support site for ProSafe® Managed Switches, click **Apply**.

## User Guide

Use the User Guide page to access the *ProSafe® Managed Switch* (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**.

# A Default Settings



This appendix describes the default settings for many of the NETGEAR 7000 series Managed Switch software features.

**Table 9. Default Settings**

Feature	Default
IP address	169.254.100.100
Subnet mask	255.255.0.0
Default gateway	0.0.0.0
Protocol	DHCP
Management VLAN ID	1
Minimum password length	8 characters
IPv6 management mode	Enabled
SNTP client	Enabled
SNTP server	time-d.netgear.com
Global logging	Enabled
CLI command logging	Disabled
Console logging	Enabled (Severity level: debug and above)
RAM logging	Enabled (Severity level: debug and above)
Persistent (FLASH) logging	Disabled
DNS	Enabled (No servers configured)
SNMP	Enabled (SNMPv1/SNMPv2, SNMPv3)
SNMP Traps	Enabled
Auto Install	Enabled



**Table 9. Default Settings (Continued)**

<b>Feature</b>	<b>Default</b>
Auto Save	Disabled
Stacking	Enabled
sFlow	Enabled
ISDP	Enabled (Versions 1 and 2)
RMON	Enabled
TACACS+	Not configured
RADIUS	Not configured
SSH/SSL	Disabled
Telnet	Enabled
Denial of Service Protection	Disabled
Captive Portal	Disabled
Dot1x Authentication (IEEE 802.1X)	Disabled
MAC-Based Port Security	All ports are unlocked
Access Control Lists (ACL)	None configured
IP Source Guard (IPSG)	Disabled
DHCP Snooping	Disabled
Dynamic ARP Inspection	Disabled
Protected Ports	None
Private Groups	None
PoE Plus (GSM7228PS and GSM7252PS)	Enabled
Flow Control Support (IEEE 802.3x)	Enabled
Head of Line Blocking Prevention	Disabled
Maximum Frame Size	1518 bytes
Auto-MDI/MDIX Support	Enabled
Auto Negotiation	Enabled
Advertised Port Speed	Maximum Capacity
Broadcast Storm Control	Enabled
Port Mirroring	Disabled

**Table 9. Default Settings (Continued)**

<b>Feature</b>	<b>Default</b>
LLDP	Enabled
LLDP-MED	Disabled
MAC Table Address Aging	300 seconds (Dynamic Addresses)
DHCP Layer 2 Relay	Disabled
Default VLAN ID	1
Default VLAN Name	Default
GVRP	Disabled
GARP Timers	Leave: 60 centiseconds Leave All: 1000 centiseconds Join: 20 centiseconds
Voice VLAN	Disabled
Guest VLAN	Disabled
RADIUS-assigned VLANs	Disabled
Double VLANs	Disabled
Spanning Tree Protocol (STP)	Enabled
STP Operation Mode	IEEE 802.1s Multiple Spanning Tree
Optional STP Features	Disabled
STP Bridge Priority	32768
Multiple Spanning Tree	Enabled
Link Aggregation	No Link Aggregation Groups (LAGs) configured
LACP System Priority	1
Routing Mode	Disabled
OSPF Admin Mode	Enabled
OSPF Router ID	0.0.0.0
IP Helper and UDP Relay	Enabled
RIP	Enabled
VRRP	Disabled
Tunnel and Loopback Interfaces	None
IPv6 Routing	Disabled
DHCPv6	Disabled

**Table 9. Default Settings (Continued)**

<b>Feature</b>	<b>Default</b>
OSPFv3	Enabled
DiffServ	Enabled
Auto VoIP	Enabled
Auto VoIP Traffic Class	6
Bridge Multicast Filtering	Disabled
MLD Snooping	Disabled
IGMP Snooping	Disabled
IGMP Snooping Querier	Disabled
GMRP	Disabled
IPv4 Multicast	Disabled
IPv6 Multicast	Disabled
Licensing Support (GSM72xxPS and GSM73xxSv1)	

## B Configuration Examples

---

# B

This appendix contains information about how to configure the following features:

- “Virtual Local Area Networks (VLANs)” on page B-608
- “Access Control Lists (ACLs)” on page B-610
- “Differentiated Services (DiffServ)” on page B-613
- “802.1X” on page B-617
- “MSTP” on page B-620

### 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 PVID Configuration” on page 3-139](#).
- 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 3-132](#)), create the following VLANs:
  - A VLAN with VLAN ID 10.
  - A VLAN with VLAN ID 20.
2. In the VLAN Membership screen (see [“VLAN Configuration” on page 3-132](#)) 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 PVID Configuration” on page 3-139](#)), specify the PVID for ports g1 and g4 so that packets entering these ports are tagged with the port VLAN ID:
    - Port g1: PVID 10
    - Port g4: 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.

ProSafe® Managed 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 6-524](#)).

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 ID: 0
  - Match Every: False
  - CoS: 0
  - Destination MAC: 01:02:1A:BC:DE:EF
  - Destination MAC Mask: 00:00:00:00:FF:FF
  - EtherType User Value: ????????
  - 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 6-526](#).

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 6-528](#)).

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 6-530](#)).

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 6-531](#)).
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 6-533](#).

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 6-542](#)).  
  
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 6-544](#)).

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.

Gigabit L3 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 5-416](#).

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 5-416](#).

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 5-420](#).

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 5-420](#).

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 Interface Configuration” on page 5-424](#)).

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 Gigabit L3 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:

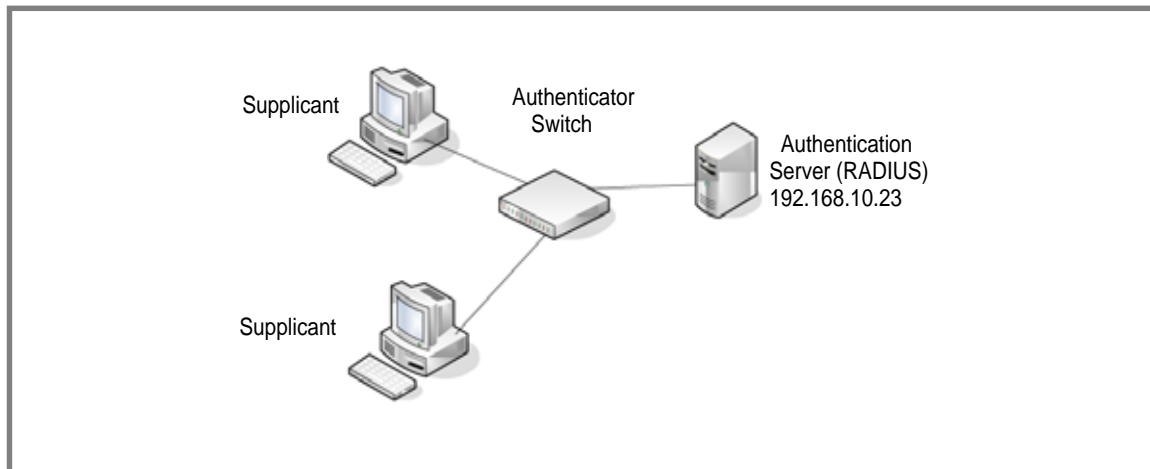
1. **Authenticator:** A Port that enforces authentication before allowing access to services available via that Port.
2. **Supplicant:** A Port that attempts to access services offered by the Authenticator.

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.

Gigabit L3 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 (1/0/5 - 1/0/8). 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 1/0/5, 1/0/6, 1/0/7 and 1/0/8.
2. From the Port Control menu, select Unauthorized.

The Port Control setting for all other ports where authentication is not needed should 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 1/0/5 - 1/0/8, 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 6-486](#) 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 6-484](#)).

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” on page 6-433](#).

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 6-443](#)).

This example enables 802.1X-based port security on ProSafe® Managed Switches and prompts the hosts connected on ports g5-g8 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.

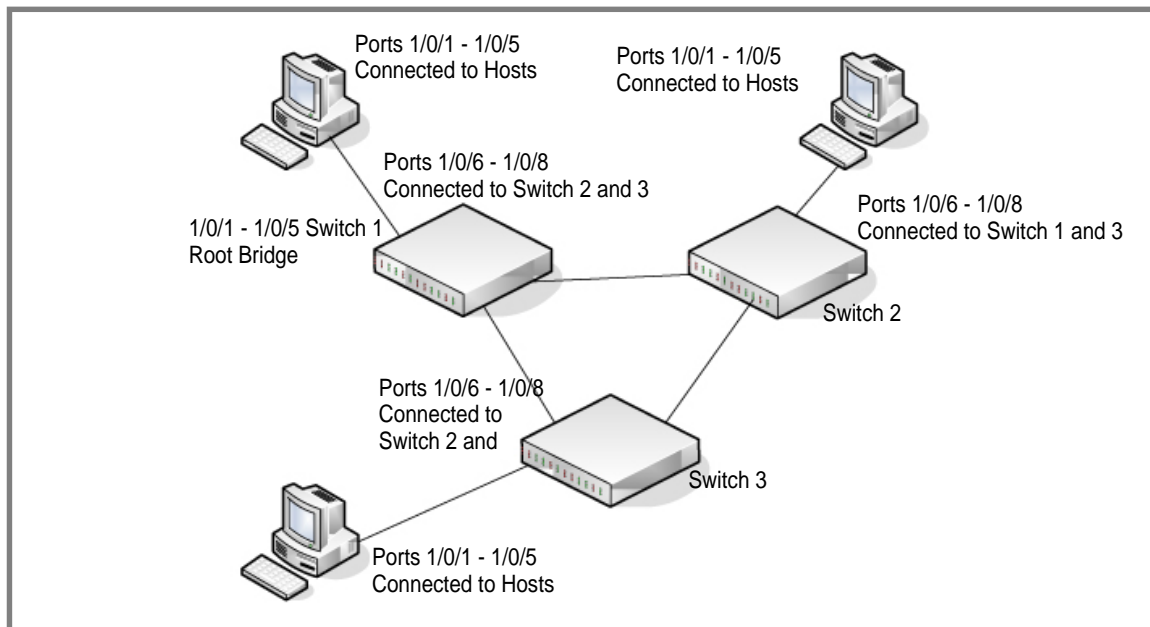
With this allocation we ensure that every VLAN is assigned to one and only one MSTI. The CIST is also an instance of spanning tree with a MSTID of 0.

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 GSM7352Sv1 or GSM7352Sv2 switch. The example network has three different ProSafe® Managed Switches that serve different locations in the network. In this example, ports 1/0/1-1/0/5 are connected to host stations, so those links are not subject to network loops. Ports 1/0/6 - 1/0/8 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 3-132](#)).
2. Use the VLAN Membership screen to include ports 1/0/1 - 1/0/8 as tagged (T) or untagged (U) members of VLAN 300 and VLAN 500 (see [“VLAN Configuration” on page 3-132](#)).
3. From the STP Configuration screen, enable the Spanning Tree State option (see [“STP Configuration” on page 3-153](#)).

Use the default values for the rest of the STP configuration settings. By default, the STP Operation Mode is MSTP and the Configuration Name is the switch MAC address.

4. 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 3-157](#)).

5. From the CST Port Configuration screen, select ports 1/0/1 - 1/0/8 and select Enable from the STP Status menu (see [“CST Port Configuration” on page 3-159](#)).
6. Click **Apply**.

7. Select ports 1/0/1 - 1/0/5 (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.

8. Click **Apply**.

You can use the CST Port Status screen to view spanning tree information about each port.

9. 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 3-163](#).

10. Click **Add**.

11. Create a second MST instance with the following settings

- MST ID: 2
- Priority: 49152
- VLAN ID: 500

12. 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 1/0/1, 1/0/2, and 1/0/3) and in the HR department (ports 1/0/4 and 1/0/5). 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.

# c 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 GSM7352S ProSafe 48+4 Gigabit Ethernet L3 Managed Stackable Switch 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**

This digital apparatus, GSM7352S ProSafe 48+4 Gigabit Ethernet L3 Managed Stackable Switch, does 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.

### **European Union**

The GSM7352S ProSafe 48+4 Gigabit Ethernet L3 Managed Stackable Switch 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

# Index

## Numerics

802.1X **433**, **468**, **470**  
example configuration **617**

## A

access control  
ACL example configuration **610**  
ACLs **524**  
authentication  
802.1X **466**, **617**  
enable **17**  
port-based **466**  
RADIUS **433**  
SNMP **17**  
TACACS+ **440**

## C

certificate **456**  
compliance **624**  
Configuration  
802.1X **468**, **470**  
Access Control Lists **524**  
Class **416**  
Community **95**  
CoS **400**  
Differentiated Services **407**  
DNS **46**  
Dual Image **594**  
Dynamic Host **49**  
Global **173**  
IGMP Snooping **172**  
LAG **201**  
MAC Filter **481**  
Management Access **450**  
Policy **420**  
Port Security **484**  
Port VLAN ID **139**  
RADIUS  
Global **433**  
Secure HTTP **453**  
SNTP Server **43**  
Standard IP ACL Example **612**  
STP **151**  
TACACS+ **440**

Trap **96**  
VLAN **132**  
VLAN example **609**

CoS **400**

## D

defaults  
CoS **611**  
DES **17**  
Device View **14**  
DiffServ **407**  
DNS **46**  
download  
from a remote system **587**

## E

EAP **557**

## F

file management **592**  
firmware download **587**

## G

guest VLAN configuration **619**

## H

help, HTML-based **13**  
HTTP **452**  
management interface access **9**  
secure **450**  
using to download files **589**  
HTTPS **453**

## I

IEEE 802.11x **617**  
IEEE 802.1AB **102**  
IEEE 802.1D **151**  
IEEE 802.1Q **130**, **152**

IEEE 802.1s **152**

IEEE 802.1w **151**

IEEE 802.1X **433**

IGMP **172**

interface

LAG **201**

logical **18**

naming convention **18**

physical **18**

queue configuration **406**

IP DSCP **400**

Mapping **403**

## L

LAG VLAN **201**

LAGPDUs **201**

LAGs **201**

Membership **203**

Static **201**

LLDP **102**

LLDP-MED **103**

## M

MAC **172**

CPU Management Interface **18**

filter summary **483**

rules **526**

MD5 **38**

MIBs **17**

## N

navigation **12**

## P

port

authentication **466**

summary **476**

## Q

QoS **398**

802.1p to Queue Mapping **402**

## R

RADIUS **427**

server **433**

reboot **580**

reset

configuration to defaults **582**

switch **580**

RSTP **151**

## S

Simple Network Time Protocol **38**

SNMP

traps **96**

using **17**

v1, v2 **93**

SNTP **38**

server configuration **43**

server status **45**

SSL **453**

storm control **493**

STP **151**

example configuration **620**

Status **153, 155**

Stratum

0 **38**

1 **38**

2 **38**

## T

T1 **38**

T2 **38**

T3 **38**

T4 **38**

TACACS+

folder **440**

settings **441**

technical support **2**

time **38**

levels **38**

trademarks **2**

traffic control **481**

trap

flags **97**

## U

Unicast **38**

upload configuration **583**

## V

VLAN **130**

example configuration **608**

guest **617**

ID **130**

managing **130**

Port VLAN ID **139**  
PVID **139**