



# NETGEAR®

---

## ProSafe® Managed Switch Web Management User Manual

Version 9.0.2

GSM5212P

GSM7212F

GSM7212P

GSM7224P

350 East Plumeria Drive  
San Jose, CA 95134  
USA

November, 2011  
202-10967-01  
v1.0

©2011 NETGEAR, Inc. All rights reserved

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

### Technical Support

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

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

Phone (Other Countries): Check the list of phone numbers at [http://support.netgear.com/app/answers/detail/a\\_id/984](http://support.netgear.com/app/answers/detail/a_id/984)

### Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, ProSecure, 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
202-10967-01	v1.0	November, 2011	First publication

# Contents

## Chapter 1 Getting Started

- Switch Management Interface . . . . . 8
- Web Access . . . . . 8
- Understanding the User Interfaces . . . . . 9
  - Using the Web Interface . . . . . 9
  - Using SNMP . . . . . 14
- Interface Naming Convention . . . . . 14

## Chapter 2 Configuring System Information

- Management . . . . . 16
  - System Information . . . . . 16
  - Switch Statistics . . . . . 21
  - System CPU Status . . . . . 24
  - Loopback Interface . . . . . 26
  - Network Interface . . . . . 27
  - Time . . . . . 31
  - DNS . . . . . 38
  - SDM Template Preference . . . . . 40
- Services . . . . . 42
  - DHCP Server . . . . . 42
  - DHCP Relay . . . . . 51
  - DHCP L2 Relay . . . . . 52
  - UDP Relay . . . . . 55
- PoE . . . . . 57
  - Basic . . . . . 57
  - Advanced . . . . . 59
- SNMP . . . . . 64
  - SNMPV1/V2 . . . . . 64
  - SNMP V3 . . . . . 70
- LLDP . . . . . 71
  - LLDP . . . . . 72
  - LLDP-MED . . . . . 78
- ISDP . . . . . 87
  - Basic . . . . . 87
  - Advanced . . . . . 88
- Timer Schedule . . . . . 93
  - Timer Global Configuration . . . . . 93
  - Timer Schedule Configuration . . . . . 94

**Chapter 3 Configuring Switching Information**

VLANs .....	96
Basic.....	97
Advanced .....	99
Spanning Tree Protocol .....	112
Basic.....	112
Advanced .....	115
Multicast .....	127
MFDB .....	127
IGMP Snooping .....	129
MLD Snooping .....	140
MVR Configuration .....	147
Basic.....	147
Advanced .....	148
Address Table .....	152
Basic.....	152
Advanced .....	154
Ports .....	158
Port Configuration.....	158
Port Description .....	160
Link Aggregation Groups .....	161
LAG Configuration .....	162
LAG Membership .....	163

**Chapter 4 Routing**

Routing Table .....	166
Basic.....	167
Advanced .....	169
IP .....	171
Basic.....	171
Advanced .....	178
VLAN .....	186
VLAN Routing Wizard.....	187
VLAN Routing Configuration.....	188
ARP .....	189
Basic.....	189
Advanced .....	190
Router Discovery .....	193

**Chapter 5 Configuring Quality of Service**

Class of Service .....	197
Basic.....	197
Advanced .....	199
Differentiated Services .....	204
DiffServ Wizard.....	205

Auto VoIP Configuration . . . . .	207
Basic . . . . .	207
Advanced . . . . .	209

## Chapter 6 Managing Device Security

Management Security Settings . . . . .	224
Local User . . . . .	224
Enable Password Configuration . . . . .	227
Line Password Configuration . . . . .	227
RADIUS . . . . .	228
Configuring TACACS+ . . . . .	234
Authentication List Configuration . . . . .	236
Login Sessions . . . . .	240
Configuring Management Access . . . . .	241
HTTP . . . . .	241
HTTPS . . . . .	243
SSH . . . . .	246
Telnet . . . . .	249
Console Port . . . . .	251
Denial of Service . . . . .	252
Port Authentication . . . . .	253
Basic . . . . .	254
Advanced . . . . .	255
Traffic Control . . . . .	262
MAC Filter . . . . .	263
Port Security . . . . .	265
Private Group . . . . .	270
Protected Ports Configuration . . . . .	272
Storm Control . . . . .	273
Control . . . . .	275
DHCP Snooping . . . . .	275
IP Source Guard . . . . .	281
Dynamic ARP Inspection . . . . .	283
Configuring Access Control Lists . . . . .	288
ACL Wizard . . . . .	288
Basic . . . . .	289
Advanced . . . . .	294

## Chapter 7 Monitoring the System

Ports . . . . .	308
Port Statistics . . . . .	309
Port Detailed Statistics . . . . .	311
EAP Statistics . . . . .	317
Cable Test . . . . .	320
Logs . . . . .	321
Buffered Logs . . . . .	322

Command Log Configuration . . . . .	324
Console Log Configuration . . . . .	324
SysLog Configuration . . . . .	325
Trap Logs . . . . .	326
Event Logs . . . . .	328
Persistent Logs . . . . .	329
Port Mirroring . . . . .	330
Multiple Port Mirroring . . . . .	330
sFlow . . . . .	332
Basic . . . . .	332
Advanced . . . . .	333

## Chapter 8 Maintenance

Save Configuration . . . . .	336
Save Configuration . . . . .	336
Auto Install Configuration . . . . .	337
Reset . . . . .	337
Device Reboot . . . . .	338
Factory Default . . . . .	338
Password Reset . . . . .	339
Upload File From Switch . . . . .	339
File Upload . . . . .	340
HTTP File Upload . . . . .	341
USB File Upload . . . . .	342
Download File To Switch . . . . .	342
File Download . . . . .	343
HTTP File Download . . . . .	344
USB File Download . . . . .	346
File Management . . . . .	347
Copy . . . . .	347
Dual Image Configuration . . . . .	348
Troubleshooting . . . . .	349
Ping IPv4 . . . . .	349
Ping IPv6 . . . . .	350
Traceroute IPv4 . . . . .	351
Traceroute IPv6 . . . . .	352

## Chapter 9 Help

Online Help . . . . .	354
Support . . . . .	354
User Guide . . . . .	355

## Appendix A Default Settings

## Appendix B Configuration Examples

- Virtual Local Area Networks (VLANs) ..... 361
  - VLAN Example Configuration ..... 362
- Access Control Lists (ACLs) ..... 363
  - MAC ACL Example Configuration ..... 364
  - Standard IP ACL Example Configuration ..... 365
- Differentiated Services (DiffServ) ..... 366
  - Class ..... 366
  - DiffServ Traffic Classes ..... 367
  - Creating Policies ..... 367
  - DiffServ Example Configuration ..... 368
- 802.1X ..... 370
  - 802.1X Example Configuration ..... 371
- MSTP ..... 372
  - MSTP Example Configuration ..... 374

**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 8
- *Web Access* on page 8
- *Understanding the User Interfaces* on page 9
- *Interface Naming Convention* on page 14

## Switch Management Interface

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

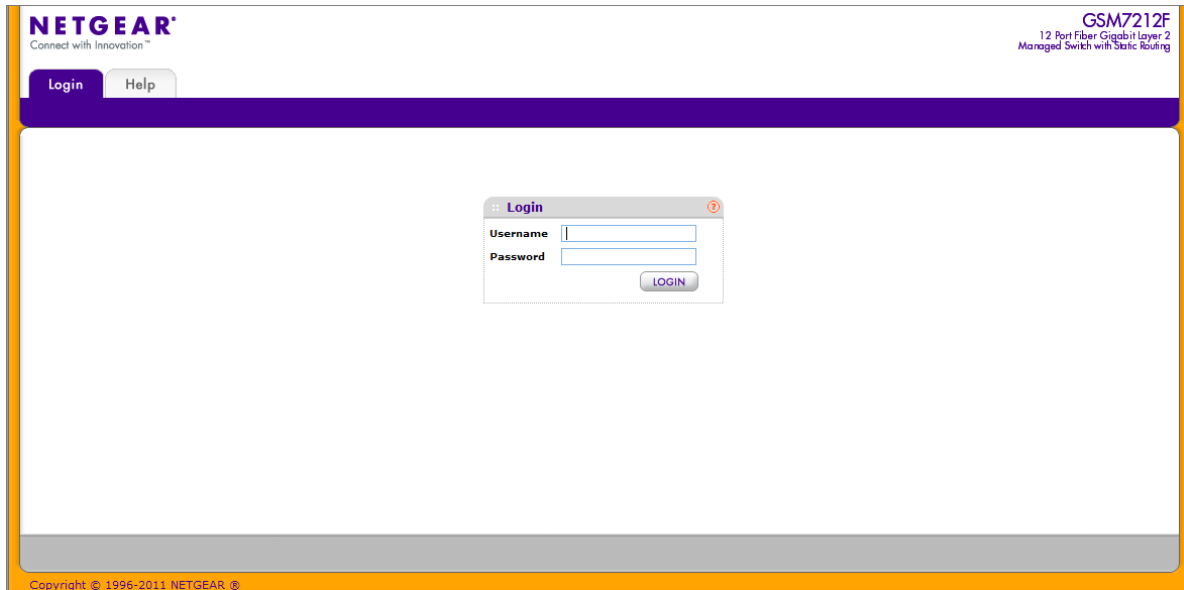
To access the ProSafe® Managed Switches management interface:

- 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

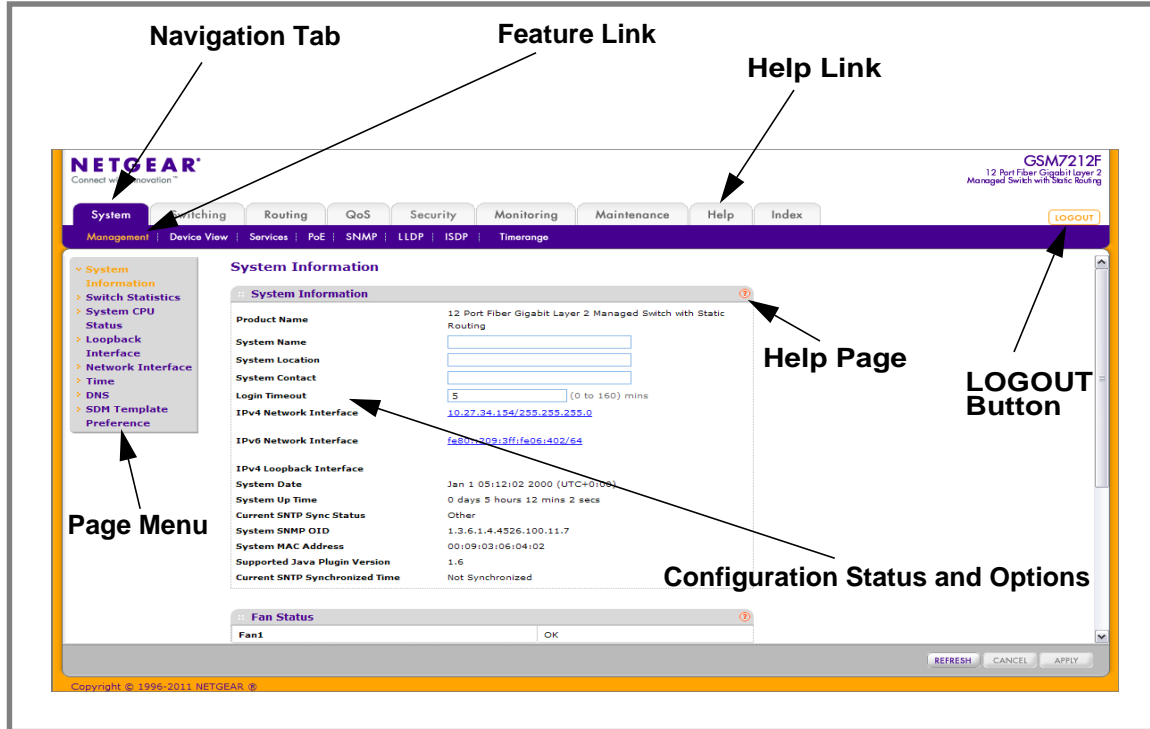
To access the switch by using a Web browser, the browser must meet the following software requirements:

- 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.
2. 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.
3. After the system authenticates you, the System Information page displays.

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

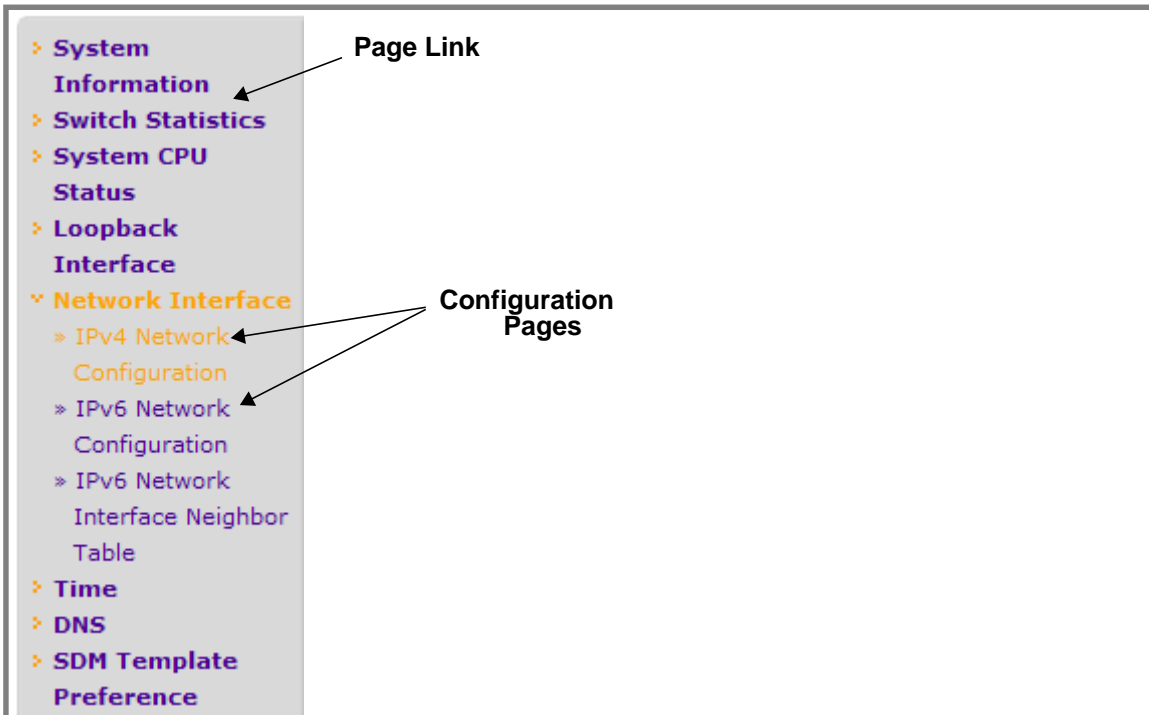


### Navigation Tabs, Feature Links, and Page Menu

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. Command Buttons**

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.

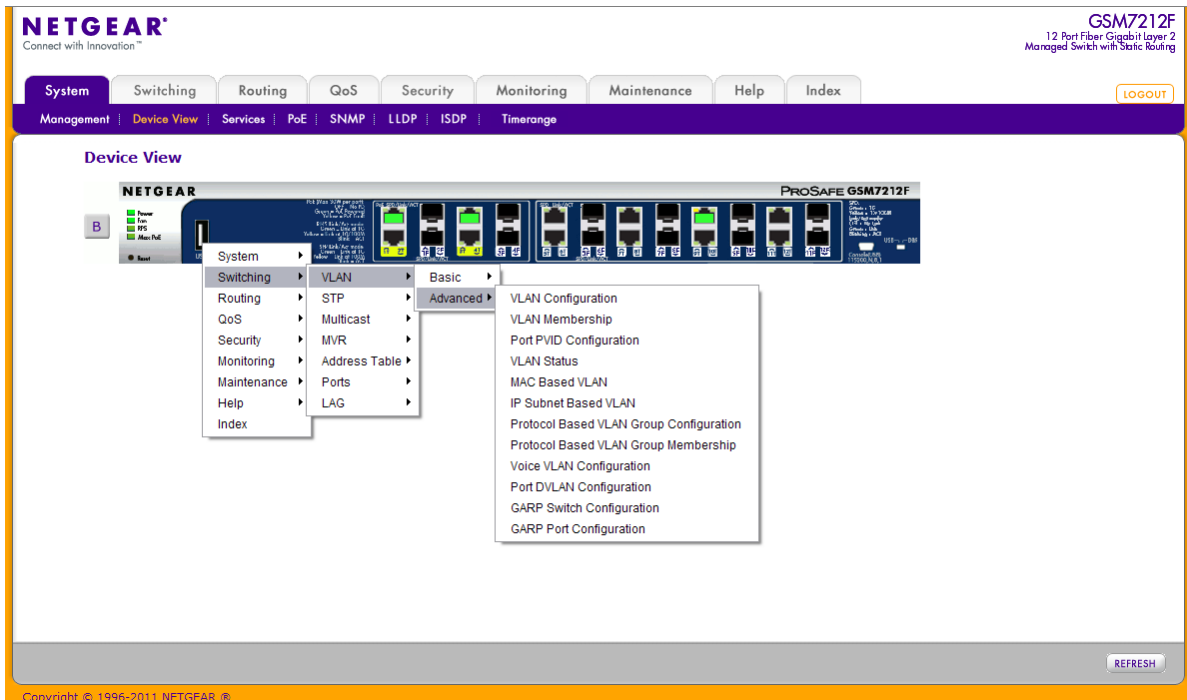
The Device View is available from the **System> Device View** page.

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.

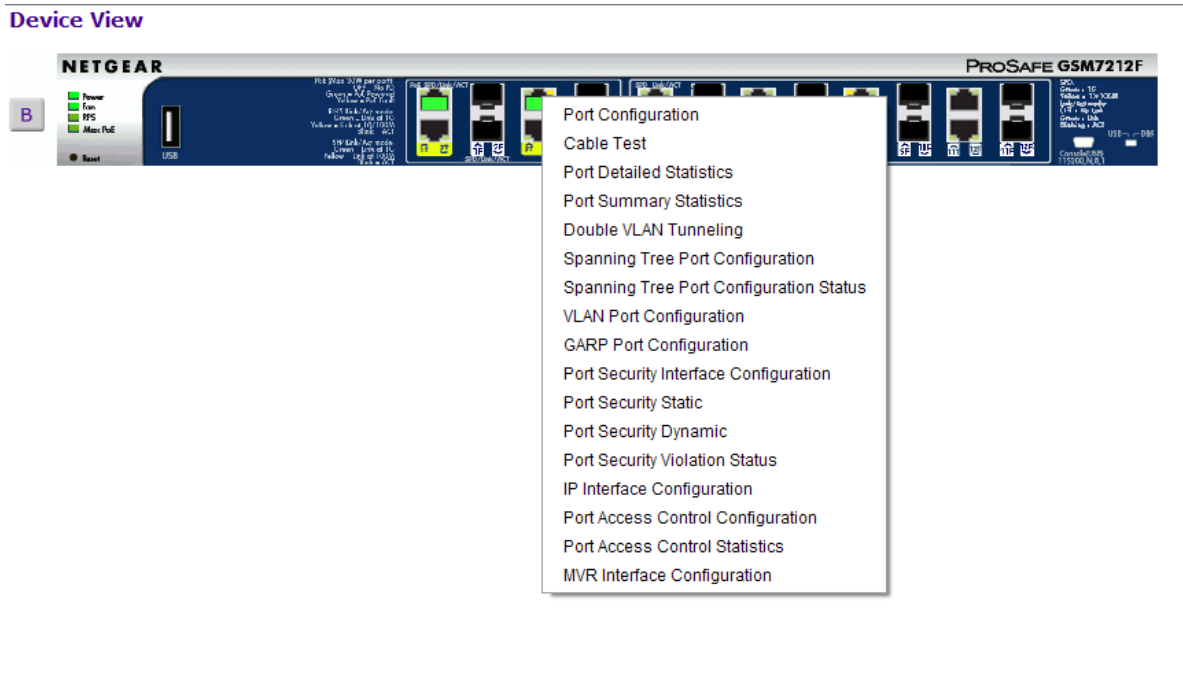
The Device View of the switch is shown below.




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):

\            <  
/            >|  
\*            |  
?

## 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 2](#) describes the naming convention for all interfaces available on the switch.

**Table 2. Naming Conventions for Interfaces**

Interface	Description	Example
Physical	The physical ports are gigabit Ethernet interfaces and are numbered sequentially starting from one.	0/1, 0/2, 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.	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 16
- Device View (See [Device View](#) on page 12)
- [Services](#) on page 42
- [PoE](#) on page 57
- [SNMP](#) on page 64
- [LLDP](#) on page 71
- [ISDP](#) on page 87
- [Timer Schedule](#) on page 93

## 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 16
- [Switch Statistics](#) on page 21
- [System CPU Status](#) on page 24
- [Loopback Interface](#) on page 26
- [Network Interface](#) on page 27
- [Time](#) on page 31
- [DNS](#) on page 38
- [SDM Template Preference](#) on page 40

## 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.

:: **System Information** ?

<b>Product Name</b>	12 port Gigabit Layer 2 POE Managed Switch with Static Routing
<b>System Name</b>	<input style="width: 90%;" type="text"/>
<b>System Location</b>	<input style="width: 90%;" type="text"/>
<b>System Contact</b>	<input style="width: 90%;" type="text"/>
<b>Login Timeout</b>	<input style="width: 60%;" type="text" value="5"/> (0 to 160) mins
<b>IPv4 Network Interface</b>	<a href="#">10.27.34.52/255.255.255.0</a>
<b>IPv6 Network Interface</b>	<a href="#">fe80::209:2ff:fe07:909/64</a>
<b>IPv4 Loopback Interface</b>	
<b>System Date</b>	Jan 1 04:40:29 2000 (UTC+0:00)
<b>System Up Time</b>	0 days 4 hours 40 mins 29 secs
<b>Current SNTP Sync Status</b>	Other
<b>System SNMP OID</b>	1.3.6.1.4.1.4526.100.11.9
<b>System MAC Address</b>	00:09:02:07:09:09
<b>Supported Java Plugin Version</b>	1.6
<b>Current SNTP Synchronized Time</b>	Not Synchronized

:: **Fan Status** ?

<b>Fan1</b>	OK
<b>Fan2</b>	OK

:: **Temperature Status** ?

<b>System</b>	35°C
---------------	------

The System Information provides various statuses:

### Switch Status

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.

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).

The following table describes the Fan Status information.

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.

The following table describes the Temperature Status information.

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.

The following table describes the Device Status information.

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.

## Web Management User Guide

Field	Description
Serial Number	The serial number of this switch.
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.

The screenshot shows a window titled "Switch Statistics" with a sub-header "Statistics". It contains a list of statistics for an interface with index 97. The statistics include received and transmitted octets and packets, with breakdowns for unicast, multicast, and broadcast traffic, as well as discarded packets and VLAN-related metrics.

Field	Value
ifIndex	97
Octets Received	19478502
Packets Received Without Errors	261421
Unicast Packets Received	2048
Multicast Packets Received	223544
Broadcast Packets Received	35829
Receive Packets Discarded	83571
Octets Transmitted	5190490
Packets Transmitted Without Errors	21000
Unicast Packets Transmitted	2754
Multicast Packets Transmitted	18238
Broadcast Packets Transmitted	8
Transmit Packets Discarded	0
Most Address Entries Ever Used	11
Address Entries in Use	10
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 22 hr 22 min 42 sec

The following table describes Switch Statistics information.

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).

## Web Management User Guide

Field	Description
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.
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.

## Web Management User Guide

Field	Description
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 CPU Status

Use this page to display the system resources.

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

**System CPU Status**

**CPU Memory Status**

Total System Memory 126564 KBytes  
Available Memory 20904 KBytes

**CPU Utilization**

Memory Utilization Report

Status	bytes
Free	21405696
Alloc	108195840

CPU Utilization:

PID	Name	5 Secs	60 Secs	300 Secs
223	_interrupt_thread	0.41%	0.16%	0.05%
225	bcmL2X.0	4.16%	4.12%	4.12%
226	bcmCNTR.0	0.20%	0.18%	0.13%

### System CPU Status

The following table describes CPU Memory Status information.

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.

## 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.

### Loopback Interface Configuration

:: IPv4 Loopback Interface Configuration ?

	Loopback ID	Primary IP Address	Primary IP Subnet Mask	Loopback Interface Status
<input type="checkbox"/>	<input type="text" value="▼"/>	<input type="text"/>	<input type="text"/>	

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.

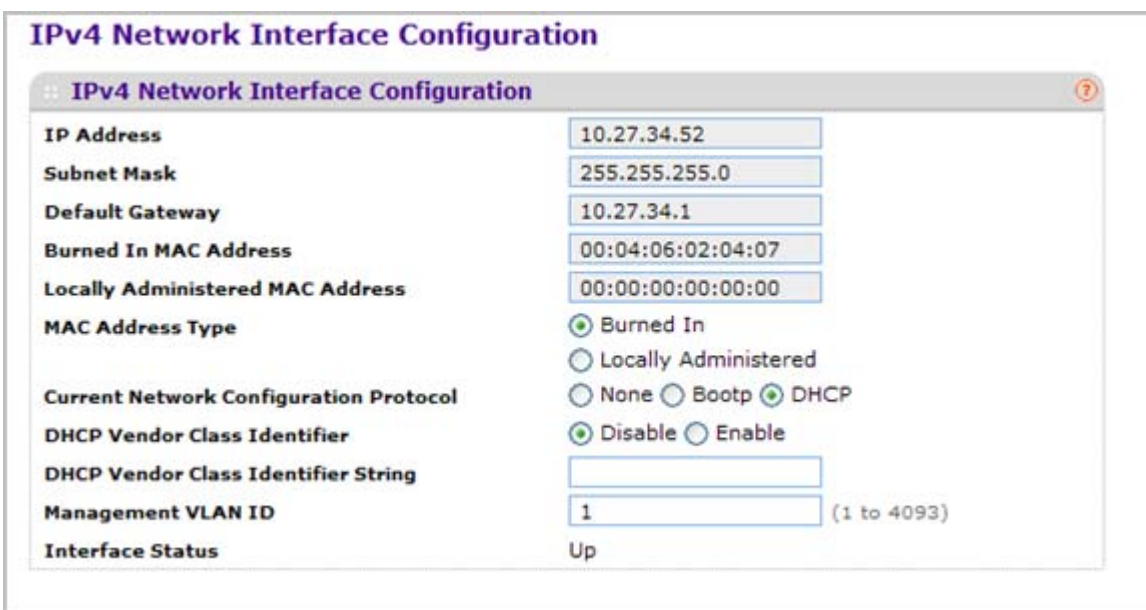
## Network Interface

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

- [IPv4 Network Configuration](#) on page 27
- [IPv6 Network Interface Configuration](#) on page 29
- [IPv6 Network Interface Neighbor Table](#) on page 30

### 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.



IPv4 Network Interface Configuration	
IP Address	10.27.34.52
Subnet Mask	255.255.255.0
Default Gateway	10.27.34.1
Burned In MAC Address	00:04:06:02:04:07
Locally Administered MAC Address	00:00:00:00:00:00
MAC Address Type	<input checked="" type="radio"/> Burned In <input type="radio"/> Locally Administered
Current Network Configuration Protocol	<input type="radio"/> None <input type="radio"/> Bootp <input checked="" type="radio"/> DHCP
DHCP Vendor Class Identifier	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
DHCP Vendor Class Identifier String	
Management VLAN ID	1 (1 to 4093)
Interface Status	Up

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.

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 Interface Configuration

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

**IPv6 Network Interface Configuration**

**Global Configuration**

Admin Mode  Disable  Enable

IPv6 Address Auto Configuration Mode  Disable  Enable

Current Network Configuration Protocol  None  DHCPv6

IPv6 Gateway

Interface Status Up

**IPv6 Network Interface Configuration**

	IPv6 Prefix/Prefix Length	EUI64
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	FE80::204:6FF:FE02:407/64	True

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 Interface Neighbor Table

Use this page to display IPv6 Network Port Neighbor entries.

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

IPv6 Network Interface Neighbor Table				
IPv6 Address	MAC Address	isRtr	Neighbor State	Last Updated

The following table displays IPv6 Network Interface Neighbor Table information.

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.

Field	Description
Neighbor State	<p>The state of the neighboring switch:</p> <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**.



### SNTP Global Configuration

**SNTP Global Configuration**

**Client Mode**       Disable  Unicast  Broadcast

**Port**               (1 to 65535) Default:123

**Unicast Poll Interval**       (6 to 10)

**Broadcast Poll Interval**       (6 to 10)

**Unicast Poll Timeout**       (1 to 30)

**Unicast Poll Retry**           (0 to 10)

**Time Zone Name**             

**Offset Hours**                 (-12 to 13)

**Offset Minutes**               (0 to 59)

**SNTP Global Status**

**Version**                        4

**Supported Mode**              Unicast and Broadcast

**Last Update Time**            JAN 01 00:00:00 1970 (UTC+0:00)

**Last Attempt Time**          JAN 01 00:00:00 1970 (UTC+0:00)

**Last Attempt Status**        Other

**Server IP Address**

**Address Type**                Unknown

**Server Stratum**              0

**Reference Clock Id**

**Server Mode**                 Reserved

**Unicast Server Max Entries**    3

**Unicast Server Current Entries** 0

**Broadcast Count**              0

## 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.

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.

Field	Description
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.
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**.

SNTP Server Configuration					
:: SNTP Server Configuration					
Server Type	Address	Port	Priority	Version	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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

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**.
- Repeat the previous steps to add additional SNTP servers. You can configure up to three SNTP servers.
- 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.

Field	Description
Address	Specifies all the existing Server Addresses. If no Server configuration exists, a message saying "No SNTP server exists" flashes on the screen.
Last Update Time	Specifies the local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	Specifies the local date and time (UTC) that this SNTP server was last queried.
Last Attempt Status	Specifies the status of the last SNTP request to this server. If no packet has been received from this server, a status of Other is displayed. <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**.

### DNS Configuration

**DNS Configuration**

DNS Status  Disable  Enable

DNS Default Name  (1 to 255 alphanumeric characters)

Retry Number  (0 to 100)

Response Timeout (secs)  (0 to 3600 secs)

**DNS Server Configuration**

	Serial No	DNS Server	Preference
<input type="checkbox"/>		<input type="text"/>	
<input type="checkbox"/>	1	10.27.138.20	0
<input type="checkbox"/>	2	10.27.138.21	1

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.

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**.

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.

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.

## SDM Template Preference

You can use this page to configure SDM template preferences for the switch.

To access this page, click **System > Management > DNS > SDM Template Preference**.

SDM Template	ARP Entries	IPv4 Unicast Routes	IPv6 NDP Entries	IPv6 Unicast Routes	ECMP Next Hops	IPv4 Multicast Routes	IPv6 Multicast Routes
Dual IPv4 and IPv6	6144	6112	2560	3072	4	1536	512
IPv4 Routing Default	6144	12256	0	0	4	2048	0
IPv4 Data Center	6144	6112	0	0	16	2048	0

To configure the SDM Template Preference settings:

1. Use **SDM Next Template ID** to configure the next active template. It will be active only after the next reboot. To revert to the default template after the next reboot, use the Default option. Possible values are:
  - Default
  - Dual IPv4 and IPv6
  - IPv4-routing Default
  - IPv4 Data Center



The following table displays Summary information.

Field	Description
SDM Current Template ID	Displays the current active SDM Template. Possible values are: <ul style="list-style-type: none"> <li>• Dual IPv4 and IPv6</li> <li>• IPv4-routing Default</li> <li>• IPv4 Data Center</li> </ul>
SDM Template	Identifies the Template. The possible values are: <ul style="list-style-type: none"> <li>• Dual IPv4 and IPv6</li> <li>• IPv4-routing Default</li> <li>• IPv4 Data Center</li> </ul>
ARP Entries	The maximum number of entries in the IPv4 Address Resolution Protocol (ARP) cache for routing interfaces.
IPv4 Unicast Routes	The maximum number of IPv4 unicast forwarding table entries.
IPv6 NDP Entries	The maximum number of IPv6 Neighbor Discovery Protocol (NDP) cache entries.
IPv6 Unicast Routes	The maximum number of IPv6 unicast forwarding table entries.
ECMP Next Hops	The maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables.
IPv4 Multicast Routes	The maximum number of IPv4 multicast forwarding table entries.
IPv6 Multicast Routes	The maximum number of IPv6 multicast forwarding table entries.

## Services

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

- [DHCP Server](#) on page 42
- [DHCP Relay](#) on page 51
- [DHCP L2 Relay](#) on page 52
- [UDP Relay](#) on page 55

## DHCP Server

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

- [DHCP Server Configuration](#) on page 42
- [DHCP Pool Configuration](#) on page 44
- [DHCP Pool Options](#) on page 47
- [DHCP Server Statistics](#) on page 48
- [DHCP Bindings Information](#) on page 49
- [DHCP Conflicts Information](#) on page 50

### 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.

**DHCP Server Configuration**

**DHCP Server Configuration**

Admin Mode  Disable  Enable

Ping Packet Count  (0, 2 to 10)

Conflict Logging Mode  Disable  Enable

Bootp Automatic Mode  Disable  Enable

**Excluded Address**

	IP Range From	IP Range To
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

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.

DHCP Pool Configuration	
Pool Name	Create <input type="button" value="v"/>
Pool Name	<input type="text"/> (1 to 31 alphanumeric characters)
Type of Binding	Unallocated <input type="button" value="v"/>
Network Address	<input type="text" value="0.0.0.0"/>
Network Mask	<input type="text" value="0.0.0.0"/>
Network Prefix Length	<input type="text"/> (0 to 32)
Client Name	<input type="text"/>
Hardware Address	<input type="text" value="00:00:00:00:00:00"/>
Hardware Address Type	Ethernet <input type="button" value="v"/>
Client ID	<input type="text"/>
Host Number	<input type="text" value="0.0.0.0"/>
Host Mask	<input type="text" value="0.0.0.0"/>
Host Prefix Length	<input type="text"/> (8 to 32)
Lease Time	Infinite <input type="button" value="v"/>
Days	<input type="text" value="0"/> (0 to 59)
Hours	<input type="text" value="0"/> (0 to 23)
Minutes	<input type="text" value="0"/> (0 to 59)
<input type="button" value="v"/> Default Router Addresses	
<input type="button" value="v"/> DNS Server Addresses	
<input type="button" value="v"/> NetBIOS Name Server Addresses	
NetBIOS Node Type	b-node Broadcast <input type="button" value="v"/>
Next Server Address	<input type="text" value="0.0.0.0"/>
Domain Name	<input type="text"/> (0 to 255 characters)
Bootfile	<input type="text"/> (0 to 128 characters)

The following table describes the DHCP Pool Configuration fields.

## Web Management User Guide

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.
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.

## Web Management User Guide

Field	Description
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".
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.

The screenshot shows the DHCP Server Statistics page with three sections, each containing a table of counts:

- 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

The following table describes the DHCP Server Statistics fields.

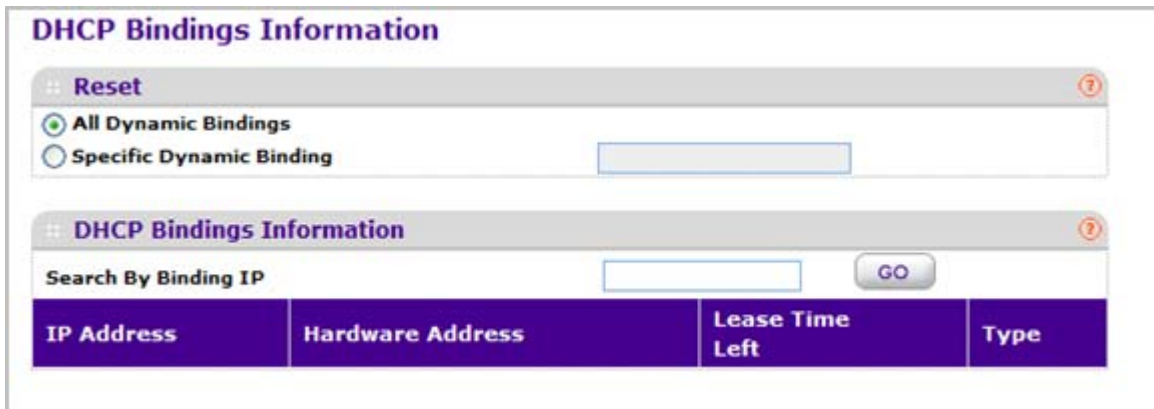
Field	Description
Automatic Bindings	Specifies the number of Automatic Bindings on the DHCP Server.
Expired Bindings	Specifies the number of Expired Bindings on the DHCP Server.
Malformed Messages	Specifies the number of the malformed messages.
DHCPDISCOVER	Specifies the number of DHCPDISCOVER messages 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.



Field	Description
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.
DHCPNAK	Specifies the number of DHCPNAK 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.

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.

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.

**DHCP Relay**

**DHCP Relay**

Maximum Hop Count: 4 (1 to 16)

Admin Mode:  Disable  Enable

Minimum Wait Time (secs): 0 (0 to 100)

Circuit ID Option Mode:  Disable  Enable

**DHCP Status**

Requests Received: 0

Requests Relayed: 0

Packets Discarded: 0

### 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.

Field	Description
Requests Received	The total number of DHCP requests received from all clients since the last time the switch was reset.

Field	Description
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 52
- [DHCP L2 Relay Interface Configuration](#) on page 53
- [DHCP L2 Relay Interface Statistics](#) on page 53

### 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.

**DHCP L2 Relay Configuration**

:: DHCP L2 Relay Configuration

1 LAGS All Go To Interface  GO

	Interface	Admin Mode	82 Option Trust Mode
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	0/1	Disable	Disable
<input type="checkbox"/>	0/2	Disable	Disable
<input type="checkbox"/>	0/3	Disable	Disable
<input type="checkbox"/>	0/4	Disable	Disable
<input type="checkbox"/>	0/5	Disable	Disable
<input type="checkbox"/>	0/6	Disable	Disable
<input type="checkbox"/>	0/7	Disable	Disable
<input type="checkbox"/>	0/8	Disable	Disable
<input type="checkbox"/>	0/9	Disable	Disable
<input type="checkbox"/>	0/10	Disable	Disable
<input type="checkbox"/>	0/11	Disable	Disable
<input type="checkbox"/>	0/12	Disable	Disable

1 LAGS All Go To Interface  GO

### 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.

The screenshot shows the 'DHCP L2 Relay Configuration' page. At the top, there is a title bar with a help icon. Below it, there is a navigation bar with 'LAGS All' and a 'Go To Interface' search box with a 'GO' button. The main content is a table with the following columns: 'Interface', 'Admin Mode', and '82 Option Trust Mode'. Each row represents an interface from 0/1 to 0/12, with a checkbox in the first column. The 'Admin Mode' and '82 Option Trust Mode' columns contain dropdown menus, all currently set to 'Disable'. At the bottom, there is another navigation bar with 'LAGS All' and another 'Go To Interface' search box with a 'GO' button.

	Interface	Admin Mode	82 Option Trust Mode
<input type="checkbox"/>		<input type="text" value="▼"/>	<input type="text" value="▼"/>
<input type="checkbox"/>	0/1	Disable	Disable
<input type="checkbox"/>	0/2	Disable	Disable
<input type="checkbox"/>	0/3	Disable	Disable
<input type="checkbox"/>	0/4	Disable	Disable
<input type="checkbox"/>	0/5	Disable	Disable
<input type="checkbox"/>	0/6	Disable	Disable
<input type="checkbox"/>	0/7	Disable	Disable
<input type="checkbox"/>	0/8	Disable	Disable
<input type="checkbox"/>	0/9	Disable	Disable
<input type="checkbox"/>	0/10	Disable	Disable
<input type="checkbox"/>	0/11	Disable	Disable
<input type="checkbox"/>	0/12	Disable	Disable

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.

**DHCP L2 Relay Interface Statistics**

DHCP L2 Relay Interface Statistics

LAGS All

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
1/0/24	0	0	0	0

LAGS All

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

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 55
- [UDP Relay Interface Configuration](#) on page 56

### 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.

UDP Relay				
UDP Relay Configuration				
Admin Mode <input checked="" type="radio"/> Disable <input type="radio"/> Enable				
UDP Relay Global Configuration				
	Server Address	UDP Port	UDP Port Other Value	Hit Count
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

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.

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.

UDP Relay Interface Configuration						
Interface	Server Address	UDP Port	UDP Port Other Value	Discard	Hit Count	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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.

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

## PoE

From PoE link under the System tab, you can configure the PoE settings.

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

- [Basic](#) on page 57
- [Advanced](#) on page 59

### Basic

Use the Basic page to configure the basic PoE settings.

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

## PoE Configuration

:: Unit Selection
?

Unit: 1 ▼

:: PoE Configuration
?

**Firmware Version**

**Power Status**

**Total Power (Main AC)** Watt

**Total Power (RPS)** Watt

**Power Source** Main AC

**Threshold Power** Watt

**Consumed Power** Watt

**System Usage Threshold** 90 (1% to 99%)

**Power Management Mode** Dynamic ▼

**Auto Reset Mode**  Enable  Disable

**Traps**  Enable  Disable

1. The **Unit Selection** field displays the current PoE unit. To change the PoE unit, select another unit from the drop down box.

The following table describes the PoE Configuration non-configurable fields.

Field	Description
Units	Displays the Current PoE Unit. You can change the PoE Unit by selecting another unit ID listed here.
Firmware Version	Version of the PoE controller's FW image.
Power Status	Indicates the power status.
Total Power (Main AC)	Displays the total power provided by the main ac power source.
Total Power (RPS)	Displays the total power provided by the redundant power source.
Power Source	Current source of system power (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 & 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.

2. To set the **System Usage Threshold**, enter a number from 1 to 99. This sets the threshold level at which a trap is sent if consumed power is greater than the threshold power.
3. The **Power Management Mode** describes or controls the power management algorithm used by the PSE to deliver power to the requesting PDs. Select **Static** to indicate that the power allocated for each port depends on the type of power threshold configured on the port. Select **Dynamic** to indicate that the power consumption on each port is measured and calculated in real-time.
4. To set the **Auto Reset Mode**, select **Enable** to reset the PSE port without administrator intervention whenever a fault condition occurs. Select **Disable** to allow only the administrator to reset the PSE port whenever a fault condition is detected.
5. To set the traps, select **Enable** to activate the PoE traps. Select **Disable** to deactivate the PoE traps. The default setting is enabled.
6. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

## Advanced

Use the Advanced page to configure the advanced PoE settings.

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

- [PoE Configuration](#) on page 59
- [PoE Port Configuration](#) on page 60
- [PoE PD Port Status](#) on page 63

## PoE Configuration

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

1. The **Unit Selection** field displays the current PoE unit. To change the PoE unit, select another unit from the drop down box.

The following table describes the PoE Configuration non-configurable fields.

Field	Description
Units	Displays the Current PoE Unit. You can change the PoE Unit by selecting another unit ID listed here.
Firmware Version	Version of the PoE controller's FW image.
Power Status	Indicates the power status.
Total Power (Main AC)	Displays the total power provided by the main ac power source.
Total Power (RPS) Total Power (PD) for GSM5212P switches only	Displays the total power provided by the redundant power source.
Power Source	Current source of system power (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 & 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.

2. To set the **System Usage Threshold**, enter a number from 1 to 99. This sets the threshold level at which a trap is sent if consumed power is greater than the threshold power.
3. The **Power Management Mode** describes or controls the power management algorithm used by the PSE to deliver power to the requesting PDs. Select **Static** to indicate that the power allocated for each port depends on the type of power threshold configured on the port. Select **Dynamic** to indicate that the power consumption on each port is measured and calculated in real-time.
4. To set the **Auto Reset Mode**, select **Enable** to reset the PSE port without administrator intervention whenever a fault condition occurs. Select **Disable** to allow only the administrator to reset the PSE port whenever a fault condition is detected.
5. To set the traps, select **Enable** to activate the PoE traps. Select **Disable** to deactivate the PoE traps. The default setting is enabled.
6. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

### PoE Port Configuration

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

The screenshot shows the 'PoE Port Configuration' page. At the top, there is a 'GoToPort' search bar with a 'GO' button. Below this is a table with 16 columns: Port, Admin Mode, High Power, Max Power, Port Priority, High Power Mode, Power Limit Type, Power Limit (Watts), Detection Type, Class, Timer Schedule, Output Voltage (Volts), Output Current (mA), Output Power (Watts), Status, and Fault Status. The table contains 10 rows of data for ports 0/3 through 0/12. Each row has a checkbox on the left. The 'Admin Mode' column is set to 'Enable' for all ports. 'High Power' is 'Yes', 'Max Power' is '32.0', and 'Port Priority' is 'Low'. 'High Power Mode' is '802.3at' and 'Power Limit Type' is 'User'. 'Power Limit (Watts)' is '30.000'. 'Detection Type' is 'auto', 'Class' is 'Unknown', and 'Timer Schedule' is 'None'. 'Output Voltage (Volts)' and 'Output Current (mA)' are both '0'. 'Output Power (Watts)' is '0.000'. 'Status' is 'Searching' and 'Fault Status' is 'No Error' for all ports.

Port	Admin Mode	High Power	Max Power	Port Priority	High Power Mode	Power Limit Type	Power Limit (Watts)	Detection Type	Class	Timer Schedule	Output Voltage (Volts)	Output Current (mA)	Output Power (Watts)	Status	Fault Status
0/3	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error
0/4	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error
0/5	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error
0/6	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error
0/7	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error
0/8	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error
0/9	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error
0/10	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error
0/11	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error
0/12	Enable	Yes	32.0	Low	802.3at	User	30.000	auto	Unknown	None	0	0	0.000	Searching	No Error

1. Select the **Admin Mode (Enable or Disable)** to determine the ability of the port to deliver power.
2. **Port Priority** is used to determine which ports can deliver power when the total power delivered by the system crosses a specific threshold. If the switch is not be able to supply power to all connected devices, priority is used to determine which ports can supply power. The lowest numbered port which is one of the ports of the same priority will have a higher priority. Select the priority order from the following list:
  - **Low** - Low priority
  - **Medium** - Medium priority
  - **High** - High priority
  - **Critical** - Critical priority
3. Select the **High Power Mode** from the following options:
  - **Disabled** indicates that a port is powered in the IEEE 802.3af mode.
  - **Legacy** indicates that a port is powered using high-inrush current, used by legacy PD's whose power requirements are more than 15W from powerup.
  - **Pre-802.3at** indicates a port is powered in the IEEE 802.3af mode initially and then switched to the high-power IEEE 802.3at mode before 75 msec. This mode needs to be selected if the PD is NOT performing Layer 2 Classification or the PSE is performing 2-Event Layer 1 Classification.
  - **802.3at** indicates that a port is powered in the IEEE 802.3at mode. For example, if the class detected by PSE is not class4, then the PSE port will not power up the PD.
4. The **Power Limit Type** describes or controls the maximum power that a port can deliver. Select the type from the following list:
  - **Class** indicates that the port power limit is equal to the class of the PD attached.
  - **User** indicates that the port power limit is equal to the value specified by Power Limit.
  - **None** indicates that the port will draw up to class 0 max power in case of low power mode and up to class 4 max power in case of high power mode.
5. Select the **Power Limit** to define the maximum power (in watts) which can be delivered by a port.

6. The **Detection Type** Describes a PD detection mechanism performed by the PSE port.
  - **pre-ieee** - Only legacy detection is done.
  - **ieee** - 4 Point Resistive Detection is done.
  - **auto** - 4 Point Resistive Detection followed by Legacy Detection is done.
  - 4point and Legacy indicates that the resistive 4 point detection scheme is used and when it fails to detect a connected PD, legacy capacitive detection is used.
7. The **Timer Schedule** defines the timer schedule assigned to the port. Select **None** to remove the timer schedule assignment.
8. Click **Reset** to forcibly resets the PSE port.
9. Click **CANCEL** to cancel the configuration on the screen. This will also reset 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.

The following table describes the PoE Configuration non-configurable fields.

Field	Description
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 defines the range of power a PD is drawing from the system. Class definitions: 0 - 0.44-12.95(watts) 1 - 0.44-3.83(watts) 2 - 0.44-6.48(watts) 3 - 0.44-12.95(watts) 4 - 0.44-25.5(watts)
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.

Field	Description
Status	<p>The status is the operational status of the port PD detection.</p> <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	<p>Describes the error description when the PSE port is in fault status. No Error indicates that the PSE port is not in any error state. MPS Absent indicates that the PSE port has detected an absence of main power supply. Short indicates that the PSE port has detected a short circuit condition. Overload indicates that the pd connected to the PSE port had tried to provide more power than it is permissible by the hardware. Power Denied indicates that the PSE port has been denied power because of shortage of power or due to administrative action.</p>

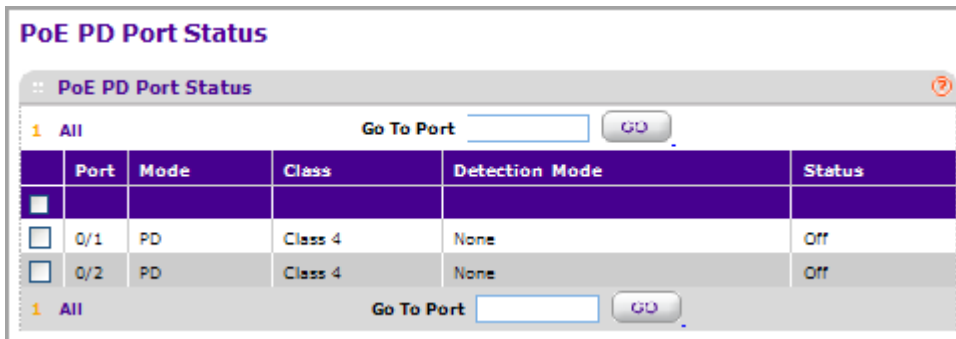
### PoE PD Port Status

---

**Note:** The PoE PD Port Status is only available on the GSM5212P switch.

---

To display the Advanced PoE PD Port Status page, click **System > Services > PoE > Advanced > PoE PD Port Status**. A screen similar to the following displays.



1. Enter the Port in slot/port format and click **Go**. The entry corresponding to the specified Port, will be selected.

The following table describes the PoE PD Port Status non-configurable fields.

Field	Description
Port	The interface for which data is to be displayed.
Mode	The Mode is PD always.
Class	The class of the Powered Device (PD) defines the range of power a PD is drawing from the system. Class definitions: 0 - 0.44-16.2(watts) 1 - 0.44-4.2(watts) 2 - 0.44-7.4(watts) 3 - 0.44-16.2(watts) 4 - 0.44-31.2(watts) Power Device (PD) device class is always 4.
Detection Mode	Displays the Power Device (PD) Detection Mode.
Status	Displays the Power Device (PD) Powered Status.

2. Click **REFRESH** to refreshes the web page to show the latest PoE PD Port Status.

## 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 64
- [SNMP V3](#) on page 70

### 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 65
- [Trap Configuration](#) on page 66
- [Trap Flags](#) on page 68
- [Supported MIBs](#) on page 69



## 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.

Community Configuration					
Community Name	Client Address	Client IP Mask	Access Mode	Status	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0	Read-Only	Enable
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0	Read-Write	Enable

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**.

The screenshot shows a web interface titled "Trap Configuration". Below the title is a table with the following columns: Community Name, Version, Protocol, Address, and Status. The table contains one row with a checkbox in the first column, an empty text input for Community Name, a dropdown menu for Version set to "SNMP V1", a dropdown menu for Protocol set to "IPv4", an empty text input for Address, and a dropdown menu for Status set to "Disable".

	Community Name	Version	Protocol	Address	Status
<input type="checkbox"/>		SNMP V1	IPv4		Disable

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

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 **PoE** to enable or disable activation of PoE traps by selecting the corresponding radio button. The factory default is enabled. Indicates whether PoE traps will be sent.
7. Click **CANCEL** to cancel the configuration on the screen. Resets 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.

## 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
Broadcom-REF-MIB	Broadcom 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 SMIPv2
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	Broadcom 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	The Broadcom 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 - IPMROUTE-MIB	IPv4 Multicast Routing MIB
draft-ietf-magma-mgmd-mib-03	MGMD MIB, includes IGMpv3 and MLDv2.
RFC 5060 - PIM-STD-MIB	Protocol Independent Multicast MIB
RFC 5240 - PIM-BSR-MIB	Bootstrap Router mechanism for PIM routers
DVMRP-STD-MIB	Distance-Vector Multicast Routing Protocol MIB
IANA-RTPROTO-MIB	IANA IP Route Protocol and IP MRoute Protocol Textual Conventions
FASTPATH-NSF-MIB	The MIB module defines objects to configure Non Stop Forwarding.

The following table describes the SNMP Supported MIBs Status fields.

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 70

### User Configuration

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

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 72
- [LLDP-MED](#) on page 78

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 72
- [LLDP Interface Configuration](#) on page 73
- [LLDP Statistics](#) on page 73
- [LLDP Local Device Information](#) on page 75
- [LLDP Remote Device Information](#) on page 77
- [LLDP Remote Device Inventory](#) on page 78

### 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 > Global Configuration**. A screen similar to the following displays.

The screenshot shows the 'LLDP Global Configuration' page. At the top, there is a title bar with 'Global Configuration' and a help icon. Below the title bar, there are four rows of configuration fields, each with a label, a text input box, and a range in parentheses:

Transmit Interval	30	(5 to 32768 secs)
Transmit Hold Multiplier	4	(2 to 10 secs)
Re-Initialization Delay	2	(1 to 10 secs)
Notification Interval	5	(5 to 3600 secs)

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 > Interface Configuration**. A screen similar to the following displays.

**LLDP Interface Configuration**

**Interface Configuration**

1 All Go To Port

	Port	Link Status	Transmit	Receive	Notify	Transmit Management Information	Operational TLV(s)			
							System Name	System Description	System Capabilities	Port Description
<input type="checkbox"/>			<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	0/1	Up	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/2	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/3	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/4	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/5	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/6	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/7	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/8	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/9	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/10	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/11	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/12	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable

1 All Go To Port

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 > Statistics**. A screen similar to the following displays.

LLDP Statistics										
:: LLDP Statistics										
<b>Last Update</b>		0 Days 00:01:33								
<b>Total Inserts</b>		1								
<b>Total Deletes</b>		0								
<b>Total Drops</b>		0								
<b>Total Ageouts</b>		0								
:: LLDP Statistics										
Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV Unknowns	TLV MED	TLV 802.1	TLV 802.3
0/1	173	175	0	0	0	0	0	0	0	0
0/2	0	0	0	0	0	0	0	0	0	0
0/3	0	0	0	0	0	0	0	0	0	0
0/4	0	0	0	0	0	0	0	0	0	0
0/5	0	0	0	0	0	0	0	0	0	0
0/6	0	0	0	0	0	0	0	0	0	0
0/7	0	0	0	0	0	0	0	0	0	0
0/8	0	0	0	0	0	0	0	0	0	0
0/9	0	0	0	0	0	0	0	0	0	0
0/10	0	0	0	0	0	0	0	0	0	0
0/11	0	0	0	0	0	0	0	0	0	0
0/12	0	0	0	0	0	0	0	0	0	0

The following table describes the LLDP Statistics fields.

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.

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 > Local Device Information**. A screen similar to the following displays.

### LLDP Local Device Information

?

**LLDP Interface Selection**

Interface:  ▼

?

**Local Device Information**

<b>Chassis ID Subtype</b>	MAC Address
<b>Chassis ID</b>	00:09:02:07:09:09
<b>Port ID Subtype</b>	Local
<b>Port ID</b>	0/1
<b>System Name</b>	
<b>System Description</b>	12 port Gigabit Layer 2 POE Managed Switch with Static Routing
<b>Port Description</b>	
<b>System Capabilities Supported</b>	bridge, router
<b>System Capabilities Enabled</b>	bridge
<b>Management Address</b>	10.27.34.52
<b>Management Address Type</b>	IPv4

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.

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.

Field	Description
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 > Remote Device Information**. A screen similar to the following displays.



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

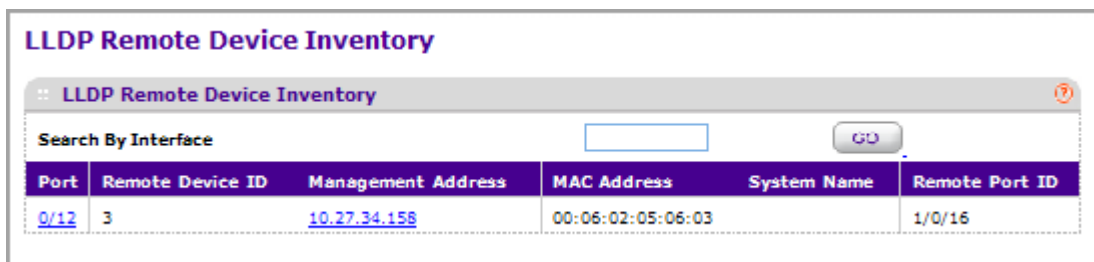
The following table describes the LLDP Remote Device Information fields.

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.

Field	Description
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.

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 79
- [LLDP-MED Interface Configuration](#) on page 79
- [LLDP-MED Local Device Information](#) on page 81

- [LLDP-MED Remote Device Information](#) on page 84
- [LLDP-MED Remote Device Inventory](#) on page 86

### 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.

The screenshot shows a web interface for 'LLDP-MED Global Configuration'. At the top, there's a title bar with the text 'LLDP-MED Global Configuration'. Below that is a sub-header 'Global Configuration' with a question mark icon. The main content area contains two fields: 'Fast Start Repeat Count' with a text input box containing the number '3' and a range '(1 to 10)' to its right, and 'Device Class' with a dropdown menu showing 'Network Connectivity'.

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.

Field	Description
Device Class	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.

**LLDP Interface Configuration**

Interface Configuration

1 All Go To Port

	Port	Link Status	Transmit	Receive	Notify	Transmit Management Information	System Name	System Description
<input type="checkbox"/>			<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	0/1	Up	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/2	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/3	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/4	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/5	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/6	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/7	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/8	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/9	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/10	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/11	Down	Enable	Enable	Disable	Enable	Enable	Enable
<input type="checkbox"/>	0/12	Down	Enable	Enable	Disable	Enable	Enable	Enable

1 All Go To Port

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.



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.

### LLDP-MED Local Device Information

**:: LLDP-MED Interface Selection** ?

Interface:  ▼

**:: Network Policies Information** ?

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

**:: Inventory Information** ?

<b>Hardware Revision</b>	0x0
<b>Firmware Revision</b>	1
<b>Software Revision</b>	10.14.19.6
<b>Serial Number</b>	23
<b>Manufacturer Name</b>	Broadcom Corporation
<b>Model Name</b>	GSM7212P
<b>Asset Id</b>	

**:: Location Information** ?

Sub Type	Location Information
Coordinate Based	
Civic Address	
ELIN	

**:: Extended PoE** ?

Device Type	Power Source	Power Priority	Power Value
PSE	Unknown	High	0 Watts

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.

Field	Description
<b>Network Policy Information: Specifies if network policy TLV is present in the LLDP frames.</b>	
	<p>Media Application Type</p> <p>Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, vidoesignalling.</p> <p>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.</p> <p>If a network policy TLV has been transmitted only then would this information be displayed</p>
<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.

#### LLDP-MED Remote Device Information

**:: LLDP-MED Interface Selection** ?

Interface:  ▼

Remote ID:

**:: Capability Information** ?

Supported Capabilities

Enabled Capabilities

Device Class

**:: Network Policies Information** ?

Media Application Type	VLAN ID	Priority	DSCP	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

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

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

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.

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.

LLDP-MED Remote Device Inventory				
Port	Management Address	MAC Address	System Model	Software Revision
0/12				

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

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 87
- *Advanced* on page 88

### Basic

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

- *Global Configuration* on page 87

### 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.

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 89
- [Interface Configuration](#) on page 90
- [ISDP Neighbor](#) on page 90
- [ISDP Statistics](#) on page 91



## 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.

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.

ISDP Interface Configuration		
:: Interface Configuration <span style="float: right;">?</span>		
1 All <span style="float: right;">Go To Port <input type="text"/> GO</span>		
	Port	Admin Mode
<input type="checkbox"/>		<input type="text"/> ▼
<input type="checkbox"/>	0/1	Enable
<input type="checkbox"/>	0/2	Enable
<input type="checkbox"/>	0/3	Enable
<input type="checkbox"/>	0/4	Enable
<input type="checkbox"/>	0/5	Enable
<input type="checkbox"/>	0/6	Enable
<input type="checkbox"/>	0/7	Enable
<input type="checkbox"/>	0/8	Enable
<input type="checkbox"/>	0/9	Enable
<input type="checkbox"/>	0/10	Enable
<input type="checkbox"/>	0/11	Enable
<input type="checkbox"/>	0/12	Enable
1 All <span style="float: right;">Go To Port <input type="text"/> GO</span>		

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 screenshot shows a web management interface titled "ISDP Neighbor". It features a search bar with a dropdown menu set to "Device Id" and a "GO" button. Below the search bar is a table with the following columns: Device ID, Interface, Address, Capability, Platform, Port ID, Hold Time, Advertisement Version, Entry Last Changed Time, and Software Version. The table contains six rows of data representing different ISDP neighbors.

Device ID	Interface	Address	Capability	Platform	Port ID	Hold Time	Advertisement Version	Entry Last Changed Time	Software Version
2ER1084000005	1/0/13	10.27.34.57	Router	XSM7224S	1/0/21	150	2	2 Days 01:17:07	3.23.15.39
049	1/0/22	10.27.15.7	Router	PCT6248	3/0/9	144	2	2 Days 01:17:04	3.2.0.7
2BW1044U00035	1/0/22	10.27.34.55	Router	GSM7252PS	1/0/41	166	2	2 Days 01:17:15	2.1.15.44
2ER1094H0000F	1/0/22	10.27.34.58	Router	XSM7224S	2/0/22	180	2	2 Days 01:17:23	3.16.16.32
GSM7352Sv2	1/0/22	10.27.34.62	Router	GSM7352Sv2	1/0/23	174	2	2 Days 01:17:20	1.24.19.31

The following table describes the ISDP Neighbor fields.

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 a window titled "ISDP Statistics" with a list of metrics and their corresponding values:

Metric	Value
ISDP Packets Received	60333
ISDP Packets Transmitted	13196
ISDPv1 Packets Received	0
ISDPv1 Packets Transmitted	0
ISDPv2 Packets Received	60333
ISDPv2 Packets Transmitted	13196
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

The following table describes the ISDP Statistics fields.

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.

## Timer Schedule

From Timer Schedule link under the System tab, you can configure the Timer Schedule settings.

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

- [Timer Global Configuration](#) on page 93
- [Timer Schedule Configuration](#) on page 94

### Timer Global Configuration

Use the Timer Global Configuration page to configure the Timer Global Configuration settings.

To display the Timer Global Configuration page, click **System > Services > Timer Schedule > Basic > Global Configuration**. A screen similar to the following displays.

1. Use **Admin Mode** to **Enable** or **Disable** the Timer Control service. The default value is **Disable**
2. Use the **Timer Schedule Name** to specify the name of a timer schedule.

The following table describes the Timer Schedule non-configurable fields.

Field	Description
ID	Identification of the timer Schedule. Maximum number of schedules that can be created is 100.

3. Click **ADD** to add the new timer schedule with a specified name. The configuration changes take effect immediately.
4. Click **DELETE** to delete the selected timer schedules. The configuration changes take effect immediately.
5. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest values.

- Click **APPLY** to send the updated configuration to the switch. The configuration changes take effect immediately.

## Timer Schedule Configuration

Use the Timer Schedule Configuration page to configure the Timer Schedule Configuration settings.

To display the Timer Schedule Configuration page, click **System > Services > Timer Schedule > Advanced > Schedule Configuration**. A screen similar to the following displays.

**Timer Schedule Configuration**

**Timer Schedule Selection**

Timer Schedule Name

---

**Timer Schedule Configuration**

Time Start  (hh:mm)

Time End  (hh:mm)

Date Start

Date End  No End Date  End Date

Recurrence Pattern

Daily Mode  Every Weekday  Every Day(s)

- Use the **Timer Schedule Name** to select the timer schedule name for which data is to be displayed.
- Use the **Time Start** to set the time of the day in format (HH:MM) when the schedule operation is started. This field is the required field. If no time is specified, the schedule does not start running.
- Use the **Time End** to set the time of the day in format (HH:MM) when the schedule operation is terminated.
- Use the **Date Start** to set the schedule start date. If no date is specified, the schedule starts running immediately.
- Use the **Date End** to set the schedule termination date. If No End Date selected, the schedule operates indefinitely.
- Use the **Recurrence Pattern** to show with what period the event will repeat. If recurrence is not needed (a timer schedule should be triggered just once), then set 'Date Stop' as equal to 'Date Start'. There are the following possible values of recurrence:
  - Daily** - The timer schedule works with daily recurrence

- **Daily Mode** - Every WeekDay selection means that the schedule will be triggered every day from Monday to Friday. Every Day(s) selection means that the schedule will be triggered every defined number of days. If number of days is not specified, then the schedule will be triggered every day.
  - **Weekly** - The timer schedule works with weekly recurrence
    - **Every Week(s)** - Define the number of weeks when the schedule will be triggered. If number of weeks is not specified, then the schedule will be triggered every week.
    - **WeekDay** - Specify the days of week when the schedule should operate.
  - **Monthly** - The timer schedule works with monthly recurrence
    - **Monthly Mode** - Show the day of the month when the schedule will be triggered. Field Every Month(s) means that the schedule will be triggered every defined number of months.
7. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest values.
  8. Click **APPLY** to send the updated configuration to the switch. The configuration changes take effect immediately.

# 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 96
- [Spanning Tree Protocol](#) on page 112
- [Multicast](#) on page 127
- [MVR Configuration](#) on page 147
- [Address Table](#) on page 152
- [Ports](#) on page 158
- [Link Aggregation Groups](#) on page 161

## 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 97
- [Advanced](#) on page 99



## Basic

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

- [VLAN Configuration](#) on page 97

### 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**.

VLAN Configuration				
:: <b>Reset</b>				
Reset Configuration <input type="checkbox"/>				
:: <b>Internal VLAN Configuration</b>				
Internal VLAN Allocation Base <input type="text" value="4093"/>				
Internal VLAN Allocation Policy <input type="radio"/> Ascending <input checked="" type="radio"/> Descending				
:: <b>VLAN Configuration</b>				
	VLAN ID	VLAN Name	VLAN Type	Make Static
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>		Disable
<input type="checkbox"/>	1	default	Default	Disable

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.

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 97
- [VLAN Membership](#) on page 100
- [VLAN Status](#) on page 101
- [Port PVID Configuration](#) on page 103
- [MAC Based VLAN](#) on page 104
- [Protocol Based VLAN Group Configuration](#) on page 105
- [Protocol Based VLAN Group Membership](#) on page 106
- [IP Subnet Based VLAN](#) on page 107
- [Port DVLAN Configuration](#) on page 108
- [Voice VLAN Configuration](#) on page 108
- [GARP Switch Configuration](#) on page 110
- [GARP Port Configuration](#) on page 110

### VLAN Configuration

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

#### VLAN Configuration

**Reset** ?

Reset Configuration

**Internal VLAN Configuration** ?

Internal VLAN Allocation Base

Internal VLAN Allocation Policy  Ascending  Descending

**VLAN Configuration** ?

	VLAN ID	VLAN Name	VLAN Type	Make Static
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>		Disable <span style="font-size: small;">v</span>
<input type="checkbox"/>	1	default	Default	Disable

**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.

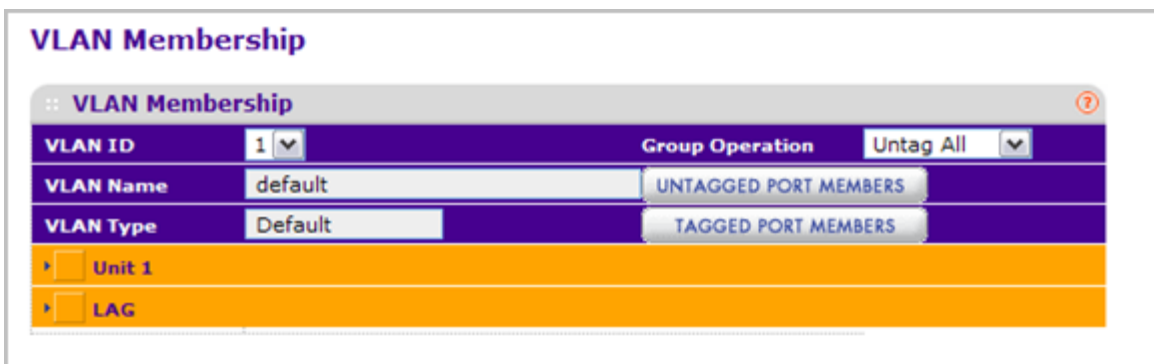
### Internal VLAN Configuration

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 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 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.

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**.

VLAN Status			
VLAN ID	VLAN Name	VLAN Type	Member Ports
1	default	Default	0/1 - 0/12, 3/1 - 3/12

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'.

## Web Management User Guide

Field	Definition
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**.

### Port PVID Configuration

:: PVID Configuration
?

1 **LAGS All**
Go To Interface

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

1 **LAGS All**
Go To Interface

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.

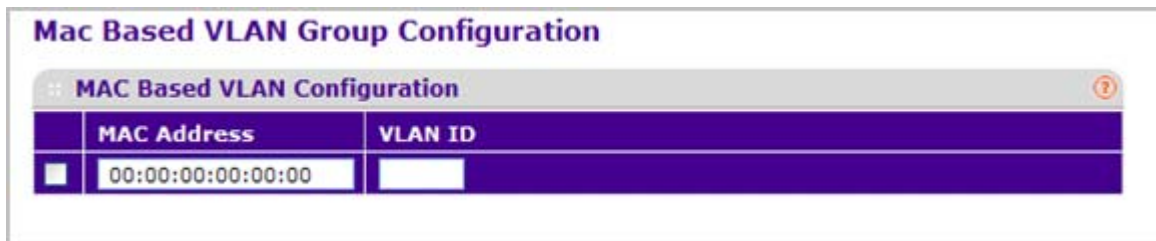
### MAC Based VLAN

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.

### 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**.

Protocol Based VLAN Group Configuration					
:: Protocol Based VLAN Group Configuration					
	Group ID	Group Name	Protocol	VLAN ID	Ports
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

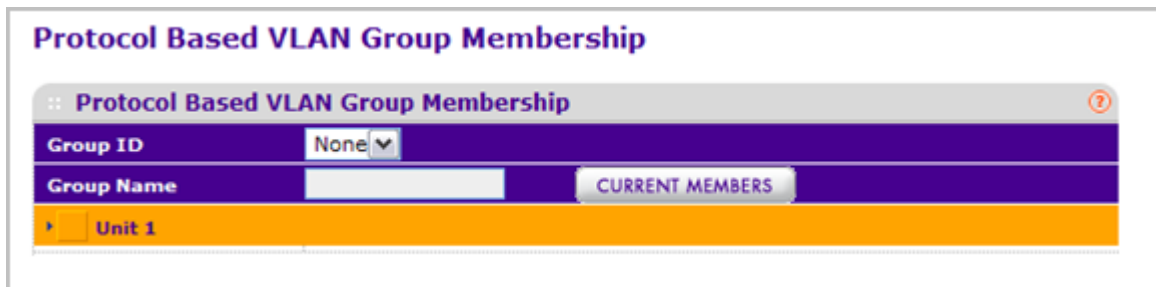
1. Use **Group Name** to assign a name to a new group. You may enter up to 16 characters.
2. Use **Protocol(s)** to select the protocols you want to be associated with the group. There are three configurable protocols: IP, IPX, ARP.
  - **IP** - IP is a network layer protocol that provides a connectionless 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.

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.

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.

## 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**.

**IP Subnet Based VLAN Configuration**

IP Subnet Based VLAN Configuration
?

	IP Address	Subnet Mask	VLAN ID
<input type="checkbox"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>

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**.

### Port DVLAN Configuration

**Global Configuration** ?

Global EtherType  ▼

**DVLAN Configuration** ?

**1 LAGS All** Go To Interface  GO

	Interface	Admin Mode
<input type="checkbox"/>		<input type="text" value=""/> ▼
<input type="checkbox"/>	0/1	Disable
<input type="checkbox"/>	0/2	Disable
<input type="checkbox"/>	0/3	Disable
<input type="checkbox"/>	0/4	Disable
<input type="checkbox"/>	0/5	Disable
<input type="checkbox"/>	0/6	Disable
<input type="checkbox"/>	0/7	Disable
<input type="checkbox"/>	0/8	Disable
<input type="checkbox"/>	0/9	Disable
<input type="checkbox"/>	0/10	Disable
<input type="checkbox"/>	0/11	Disable
<input type="checkbox"/>	0/12	Disable

**1 LAGS All** Go To Interface  GO

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

## 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**.

**Voice VLAN Configuration**

**Voice VLAN Global Admin** ?

Admin Mode  Disable  Enable

---

**Voice VLAN Configuration** ?

1 All Go To Interface  GO

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

1 All Go To Interface  GO

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.

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**.

### GARP Port Configuration

1 LAGS All Go To Interface

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

1 LAGS All Go To Interface

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 (centiseocs)** to specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseocs. Enter a number between 10 and 100 (0.1 to 1.0 seconds). The factory default is 20 centiseocs (0.2 seconds). An instance of this timer exists for each GARP participant for each port.
5. Use **Leave Time (centiseocs)** to specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseocs. 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 “CST Port Configuration” on page 3-119.

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 112
- [Advanced](#) on page 115

### Basic

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



- [STP Configuration](#) on page 113

## 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 shows the 'STP Configuration' web page. It is divided into two main sections: 'STP Configuration' and 'STP Status'.

**STP Configuration Section:**

- Spanning Tree Admin Mode:** Radio buttons for 'Disable' and 'Enable' (selected).
- Force Protocol Version:** Radio buttons for 'IEEE 802.1d', 'IEEE 802.1w', and 'IEEE 802.1s' (selected).
- Configuration Name:** Text input field containing '00-04-06-02-04-07'.
- Configuration Revision Level:** Text input field containing '0' (range: 0 to 65535).
- Forward BPDUs while STP Disabled:** Radio buttons for 'Disable' (selected) and 'Enable'.
- BPDUs Guard:** Radio buttons for 'Disable' (selected) and 'Enable'.
- BPDUs Filter:** Radio buttons for 'Disable' (selected) and 'Enable'.
- Configuration Digest Key:** Text input field containing '0xac36177f50283cd4b83821d8ab26de62'.
- Configuration Format Selector:** Text input field containing '0'.

**STP Status Section:**

MST ID	VID	FID
0	1	1

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 BPDUs 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 **BPDUs Guard** to specify whether the BPDUs guard feature is enabled. The STP BPDUs 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 BPDUs guard enabled will not be able to influence the overall STP topology. At the reception of BPDUs, the BPDUs 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.

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 115
- [CST Configuration](#) on page 117
- [CST Port Configuration](#) on page 119
- [CST Port Status](#) on page 121
- [MST Configuration](#) on page 122
- [MST Port Status](#) on page 124
- [STP Statistics](#) on page 126

### 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**.

#### STP Configuration

##### STP Configuration

Spanning Tree Admin Mode  Disable  Enable

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

Configuration Name

Configuration Revision Level  (0 to 65535)

Forward BPDU while STP Disabled  Disable  Enable

BPDU Guard  Disable  Enable

BPDU Filter  Disable  Enable

Configuration Digest Key

Configuration Format Selector

##### STP Status

MST ID	VID	FID
0	1	1

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.

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**.

### CST Configuration

#### CST Configuration

Bridge Priority	<input type="text" value="32768"/>	(0 to 61440)
Bridge Max Age (secs)	<input type="text" value="20"/>	(6 to 40)
Bridge Hello Time (secs)	<input type="text" value="2"/>	
Bridge Forward Delay (secs)	<input type="text" value="15"/>	(4 to 30)
Spanning Tree Maximum Hops	<input type="text" value="20"/>	(6 to 40)
Spanning Tree Tx Hold Count	<input type="text" value="6"/>	(1 to 10)

#### CST Status

Bridge Identifier	80:00:00:04:06:02:04:07
Time Since Topology Change	0 day 0 hr 30 min 22 sec
Topology Change Count	3
Topology Change	False
Designated Root	80:00:00:00:00:01:03:B8
Root Path Cost	60000
Root Port Identifier	80:16
Max Age (secs)	20
Forward Delay (secs)	15
Hold Time (secs)	6
CST Regional Root	80:00:00:04:06:02:04:07
CST Path Cost	0
Port Triggered TC	1/0/13

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.

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.

Field	Description
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**.

The screenshot shows the 'CST Port Configuration' page with a table of port settings. The table has columns for 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 Forwarding, BPDU Guard Effect, Auto Edge, Root Guard, Loop Guard, TCN Guard, Port Mode, and Port Forwarding State. The interface includes a 'Go To Interface' search bar and a 'LAGS All' indicator.

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 Forwarding	BPDU Guard Effect	Auto Edge	Root Guard	Loop Guard	TCN Guard	Port Mode	Port Forwarding State
0/1	128	Enable	20000	Enabled	2	20000	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Forwarding
0/2	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/3	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/4	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/5	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/6	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/7	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/8	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/9	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/10	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/11	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
0/12	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled

To configure CST port settings:

- Interface** - One of the physical or port channel interfaces associated with VLANs associated with the CST.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

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**.

### CST Port Status

Interface	Port ID	Port Forwarding State	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port	Topology Change Acknowledge	Edge Port	Point-to-Point MAC	CST Regional Root	CST Port Cost
0/1	80:01	Forwarding	Root	80:00:00:01:09:03:06:02	20000	80:00:00:06:02:05:06:03	80:0f	True	Disabled	True	80:00:00:06:02:05:06:03	0
0/2	80:02	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/3	80:03	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/4	80:04	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/5	80:05	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/6	80:06	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/7	80:07	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/8	80:08	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/9	80:09	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/10	80:0a	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/11	80:0b	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0
0/12	80:0c	Disabled	Disabled	80:00:00:09:02:07:09:09	0	80:00:00:09:02:07:09:09	00:00	False	Disabled	False	80:00:00:09:02:07:09:09	0

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

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.

Field	Description
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**.

MST ID	Priority	Bridge Identifier	Vlan Id	Time Since Topology Change	Topology Change Count	Topology Change	Designated Root	Root Path Cost	Root Port Identifier
0	32768	80:00:00:04:06:02:04:07	1	0 day 0 hr 35 min 4 sec	3	False	80:00:00:00:00:01:03:88	60000	80:16

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.
2. To delete an MST instance, select the check box next to the instance and click **DELETE**.
  3. 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.
  4. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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

Field	Description
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	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 Port Identifier	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 Status**.




---

**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\*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.

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.

## Web Management User Guide

Field	Description
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**.

The screenshot shows the 'STP Statistics' page with a table of interface statistics. The table has seven columns: Interface, STP BPDUs Received, STP BPDUs Transmitted, RSTP BPDUs Received, RSTP BPDUs Transmitted, MSTP BPDUs Received, and MSTP BPDUs Transmitted. The data rows show interfaces 0/1 through 0/12. Interface 0/1 has 36 RSTP BPDUs Transmitted and 6297 MSTP BPDUs Received. All other interfaces show 0 for all metrics.

Interface	STP BPDUs Received	STP BPDUs Transmitted	RSTP BPDUs Received	RSTP BPDUs Transmitted	MSTP BPDUs Received	MSTP BPDUs Transmitted
0/1	0	0	0	36	6297	0
0/2	0	0	0	0	0	0
0/3	0	0	0	0	0	0
0/4	0	0	0	0	0	0
0/5	0	0	0	0	0	0
0/6	0	0	0	0	0	0
0/7	0	0	0	0	0	0
0/8	0	0	0	0	0	0
0/9	0	0	0	0	0	0
0/10	0	0	0	0	0	0
0/11	0	0	0	0	0	0
0/12	0	0	0	0	0	0

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

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.

Field	Description
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 127
- [IGMP Snooping](#) on page 129
- [MLD Snooping](#) on page 140

## MFDB

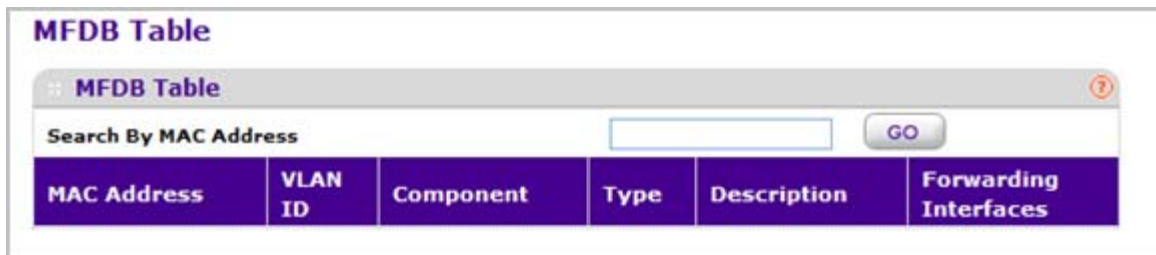
From the MFDB link, you can access the following pages:

- [MFDB Table](#) on page 128
- [MFDB Statistics](#) on page 129

## 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**.



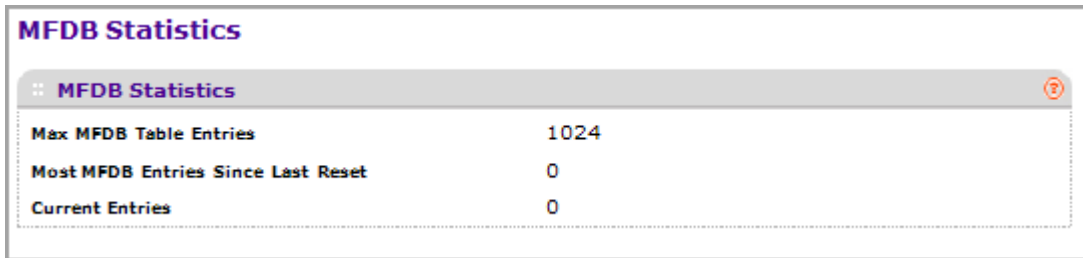
1. Use **Search by MAC Address** to enter a MAC Address whose MFDB table entry you want displayed. Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67. Then click on the “GO” button. If the address exists, that entry will be displayed. An exact match is required.

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**.



MFDB Statistics	
Max MFDB Table Entries	1024
Most MFDB Entries Since Last Reset	0
Current Entries	0

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 130
- [IGMP Snooping Interface Configuration](#) on page 132
- [IGMP VLAN Configuration](#) on page 133
- [Multicast Router Configuration](#) on page 135
- [Multicast Router VLAN Configuration](#) on page 135
- [IGMP Snooping Querier](#) on page 136
  - [IGMP Snooping Querier Configuration](#) on page 137
  - [IGMP Snooping Querier VLAN Configuration](#) on page 138

## 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**.

IGMP Snooping Configuration	
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Unknown Multicast Filtering	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Multicast Control Frame Count	0
IGMP Router-Alert check	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Interfaces Enabled for IGMP Snooping	
Data Frames Forwarded by the CPU	0
VLAN IDs Enabled for IGMP Snooping	

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.

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**.

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

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**.

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

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**.

	Interface	Multicast Router
<input type="checkbox"/>		<input type="text" value=""/>
<input type="checkbox"/>	0/1	Disable
<input type="checkbox"/>	0/2	Disable
<input type="checkbox"/>	0/3	Disable
<input type="checkbox"/>	0/4	Disable
<input type="checkbox"/>	0/5	Disable
<input type="checkbox"/>	0/6	Disable
<input type="checkbox"/>	0/7	Disable
<input type="checkbox"/>	0/8	Disable
<input type="checkbox"/>	0/9	Disable
<input type="checkbox"/>	0/10	Disable
<input type="checkbox"/>	0/11	Disable
<input type="checkbox"/>	0/12	Disable

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**.

### Multicast Router VLAN Configuration

?

**:: Multicast Router VLAN Configuration**

Interface  ▼

?

**:: Multicast Router VLAN Configuration**

	VLAN ID	Multicast Router
<input type="checkbox"/>	<input type="text"/>	<input type="text"/> ▼

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**.

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.
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.

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**.

	VLAN ID	Querier Election Participate Mode	Querier VLAN Address	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					

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.

## Web Management User Guide

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 140
- [MLD Snooping Interface Configuration](#) on page 141
- [MLD VLAN Configuration](#) on page 142
- [Multicast Router Configuration](#) on page 142
- [Multicast Router VLAN Configuration](#) on page 143
- [MLD Snooping Querier Configuration](#) on page 144
- [MLD Snooping Querier VLAN Configuration](#) on page 144

### 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.

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**.

### MLD Snooping Interface Configuration

1 LAGS All Go To Interface

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

1 LAGS All Go To Interface

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**.

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

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**.

**Multicast Router Configuration**

:: Multicast Router Configuration

1 LAGS All Go To Interface  GO

	Interface	Multicast Router
<input type="checkbox"/>		<input type="text"/> ▼
<input type="checkbox"/>	0/1	Disable
<input type="checkbox"/>	0/2	Disable
<input type="checkbox"/>	0/3	Disable
<input type="checkbox"/>	0/4	Disable
<input type="checkbox"/>	0/5	Disable
<input type="checkbox"/>	0/6	Disable
<input type="checkbox"/>	0/7	Disable
<input type="checkbox"/>	0/8	Disable
<input type="checkbox"/>	0/9	Disable
<input type="checkbox"/>	0/10	Disable
<input type="checkbox"/>	0/11	Disable
<input type="checkbox"/>	0/12	Disable

1 LAGS All Go To Interface  GO

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**.

**Multicast Router VLAN Configuration**

:: Multicast Router VLAN Configuration

Interface  ▼

:: Multicast Router VLAN Configuration

	VLAN ID	Multicast Router
<input type="checkbox"/>	<input type="text"/>	<input type="text"/> ▼

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.

- 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**.

- Use **Querier Admin Mode** to select the administrative mode for MLD Snooping for the switch. The default is disable.
- 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.
- Use **MLD Version** to specify the MLD protocol version used in periodic MLD queries.
- 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.
- 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.

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**.



MLD Snooping Querier VLAN Configuration								
MLD Snooping Querier VLAN Configuration								
	VLAN ID	Querier Election Participate Mode	Querier VLAN Address	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					

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, up on seeing other querier of same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
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.

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 is 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.

## Web Management User Guide

Field	Description
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.

## MVR Configuration

From the MVR Configuration link under the Switching tab, you can configure the MVR settings.

From the MVR Configuration link, you can access the following pages:

- [Basic](#) on page 147
- [Advanced](#) on page 148

### Basic

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

- [MVR Configuration](#) on page 147

### MVR Configuration

To display the MVR Configuration page, click **Switching > MVR > Basic > MVR Configuration**. A screen similar to the following displays.

### MVR Configuration

1. Use **MVR Running** to **Enable** or **Disable** the MVR feature. The factory default is **Disable**.
2. Use **MVR multicast** to specify the VLAN on which MVR multicast data will be received. All source ports belong to this VLAN. The value can be set in a range of 1 to 4093. The default value is 1.

Field	Definition
MVR Max Multicast Groups	Displays the maximum number of multicast groups that MVR supports.
MVR Current Multicast Groups	Displays current number of the MVR groups allocated.

3. Use **MVR Global query response time** to set the maximum time to wait for the IGMP reports membership on a receiver port. This time applies only to receiver-port leave

processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR querytime for an IGMP group membership report before removing the port from the multicast group membership. The value is equal to the tenths of second. The range is from 1 to 100 tenths. The factory default is 5 tenths or one-half.

4. Use **MVR Mode** to specify the MVR mode of operation. The factory default is compatible.

## Advanced

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

- [MVR Group Configuration](#) on page 148
- [MVR Interface Configuration](#) on page 149
- [MVR Group Membership](#) on page 150
- [MVR Statistics](#) on page 150

### MVR Group Configuration

To display the MVR Group Configuration page, click **Switching > MVR > Advanced > MVR Group Configuration**. A screen similar to the following displays.

### MVR Group Configuration

MVR Group Configuration		
MVR Group IP	Status	Members
<input type="text"/>		

1. Use the **MVR Group IP** to specify the IP Address for the new MVR group.
2. Click **ADD** to add a new MVR group.
3. Click **DELETE** to delete a selected MVR group.
4. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Field	Definition
Status	Displays the status of the specific MVR group.
Members	Displays the list of ports that participate in the specific MVR group.

## MVR Interface Configuration

To display the MVR Interface Configuration page, click **Switching > MVR > Advanced > MVR Interface Configuration**. A screen similar to the following displays.

### MVR Interface Configuration

	Interface	Admin Mode	Type	Immediate Leave	Status
<input type="checkbox"/>					
<input type="checkbox"/>	0/1	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/>	0/2	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/3	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/>	0/4	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/5	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/6	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/7	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/8	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/9	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/>	0/10	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/11	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/12	Disable	none	Disable	INACTIVE/InVLAN

1. Use **Interface** to specify the interface you want to configure.
2. Use **Admin Mode** to **Enable** or **Disable** MVR on a port. The factory default is **Disable**.
3. Use **Type** to configure the port as an MVR **receiver** port or a **source** port. The default port type is **none**.
4. Use **Immediate Leave** to **Enable** or **Disable** the **Immediate Leave** feature of MVR on a port. The factory default is **Disable**.
5. Click **REFRESH** to refresh the web page to show the latest MVR interface configuration.
6. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

Field	Definition
Status	Displays the status of the specific port.

## MVR Group Membership

To display the MVR Configuration page, click **Switching > MVR > Advanced > MVR Group Membership**. A screen similar to the following displays.

### MVR Group Membership



1. Use the **Group IP** to specify the IP multicast address of the MVR group for which you want to display or configure data.
2. Use the **Port List** to shows the configured list of members of the selected MVR group. You can use this port list to add the ports you selected to this MVR group.
3. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen.
4. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

## MVR Statistics

To display the MVR Configuration page, click **Switching > MVR > Advanced > MVR Statistics**. A screen similar to the following displays.

### Statistics

Mvr Statistics	
IGMP Query Received	0
IGMP Report V1 Received	0
IGMP Report V2 Received	0
IGMP Leave Received	0
IGMP Query Transmitted	0
IGMP Report V1 Transmitted	0
IGMP Report V2 Transmitted	0
IGMP Leave Transmitted	0
IGMP Packet Receive Failures	0
IGMP Packet Transmit Failures	0

1. Click **REFRESH** to refresh the web page to show the latest MVR statistics.

## Web Management User Guide

Field	Definition
IGMP Query Received	Displays the number of received IGMP Queries.
IGMP Report V1 Received	Displays the number of received IGMP Reports V1.
IGMP Report V2 Received	Displays the number of received IGMP Reports V2.
IGMP Leave Received	Displays the number of received IGMP Leaves.
IGMP Query Transmitted	Displays the number of transmitted IGMP Queries.
IGMP Report V1 Transmitted	Displays the number of transmitted IGMP Reports V1.
IGMP Report V2 Transmitted	Displays the number of transmitted IGMP Reports V2.
IGMP Leave Transmitted	Displays the number of transmitted IGMP Leaves.
IGMP Packet Receive Failures	Displays the number of IGMP packet receive failures.
IGMP Packet Transmit Failures	Displays the number of IGMP packet transmit failures.

## Address Table

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

- [Basic](#) on page 152
- [Advanced](#) on page 154

### Basic

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

- [Address Table](#) on page 152

### 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**.

The screenshot shows the 'Address Table' web interface. At the top, there is a search bar labeled 'Search By' with a dropdown menu set to 'VLAN ID' and a 'GO' button. Below the search bar, it indicates 'Total MAC Addresses: 43'. The main part of the interface is a table with the following data:

VLAN ID	MAC Address	Port	status
1	00:06:02:05:06:05	0/12	Learned
1	00:07:03:05:05:05	5/1	Management
1	00:0F:FE:00:8E:76	0/12	Learned
1	00:16:9C:E1:D8:00	0/12	Learned
1	00:19:E7:D3:82:2D	0/12	Learned
1	00:1A:A0:1A:94:FA	0/12	Learned
1	00:C0:05:01:98:05	0/12	Learned
1	00:E0:0C:BC:E5:60	0/12	Learned
1	C8:0A:A9:32:F3:63	0/12	Learned

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.

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 154
- [Address Table](#) on page 155
- [Static MAC Address](#) on page 157

### 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**.



**Dynamic Address Table**

**Dynamic Address Table** ⓘ

Address Aging Timeout (seconds)  (sec)

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**.

VLAN ID	MAC Address	Port	status
1	00:06:02:05:06:05	0/12	Learned
1	00:07:03:05:05:05	5/1	Management
1	00:0F:FE:00:8E:76	0/12	Learned
1	00:16:9C:E1:D8:00	0/12	Learned
1	00:19:E7:D3:82:2D	0/12	Learned
1	00:1A:A0:1A:94:FA	0/12	Learned
1	00:E0:0C:BC:E5:60	0/12	Learned
1	52:54:40:22:46:5C	0/12	Learned
1	C8:0A:A9:32:F3:63	0/12	Learned

- 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.

## Web Management User Guide

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	The status of this entry. The meanings of the values are: <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>

## Static MAC Address

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

**Static MAC Address Configuration**

**Port List**

Interface: 0/1

**Static MAC Address Table**

	Static MAC Address	VLAN ID
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

1. Use **Interface** to select the physical interface/LAGs for which you want to display data.
2. Use the **Static MAC Address** to input the MAC address to be deleted.
3. Select the **VLAN ID** associated with the MAC address.
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.
6. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

## 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 158
- [Port Description](#) on page 160

## 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**.

The screenshot shows the 'Port Configuration' page with a table of port settings. The table has columns for Port, Port Type, STP mode, Admin Mode, LACP Mode, Physical Mode, Physical Status, Link Status, Link Trap, Flow Control Mode, Maximum Frame Size (1518 to 9216), and ifindex. The rows correspond to ports G/1 through G/12. Port G/1 is the only one with a 'Link Up' status, while all others are 'Link Down'. The Physical Status for G/1 is '1000 Mbps', while others are 'Unknown'. The Maximum Frame Size is consistently '1518' for all ports.

Port	Port Type	STP mode	Admin Mode	LACP Mode	Physical Mode	Physical Status	Link Status	Link Trap	Flow Control Mode	Maximum Frame Size (1518 to 9216)	ifindex
<input type="checkbox"/> G/1	Normal	Enable	Enable	Enable	Auto	1000 Mbps	Link Up	Enable	Disable	1518	1
<input type="checkbox"/> G/2	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	2
<input type="checkbox"/> G/3	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	3
<input type="checkbox"/> G/4	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	4
<input type="checkbox"/> G/5	Normal	Enable	Disable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	5
<input type="checkbox"/> G/6	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	6
<input type="checkbox"/> G/7	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	7
<input type="checkbox"/> G/8	Normal	Enable	Disable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	8
<input type="checkbox"/> G/9	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	9
<input type="checkbox"/> G/10	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	10
<input type="checkbox"/> G/11	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	11
<input type="checkbox"/> G/12	Normal	Enable	Disable	Enable	Auto	Unknown	Link Down	Enable	Disable	1518	12

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.

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.

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.

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

- [LAG Configuration](#) on page 162
- [LAG Membership](#) on page 163

## 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**.

LAG Configuration										
LAG Name	Description	LAG ID	Admin Mode	Hash Mode	STP Mode	Static Mode	Link Trap	Configured Ports	Active Ports	LAG State
<input type="checkbox"/> <a href="#">ch1</a>		lag 1	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch2</a>		lag 2	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch3</a>		lag 3	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch4</a>		lag 4	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch5</a>		lag 5	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch6</a>		lag 6	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch7</a>		lag 7	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch8</a>		lag 8	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch9</a>		lag 9	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch10</a>		lag 10	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch11</a>		lag 11	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN
<input type="checkbox"/> <a href="#">ch12</a>		lag 12	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Disable			DOWN

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.
  - **Enhanced hashing mode** - Features MODULO-N operation based on the number of ports in the LAG, non-Unicast traffic and unicast traffic hashing using a common hash algorithm, excellent load balancing performance, and packet attributes selection based on the packet type:

- For L2 packets, source and destination MAC address are used for hash computation.
  - For L3 packets, source IP, destination IP address, TCP/UDP ports are used.
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.

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**.

### LAG Membership

:: LAG Membership ?

<b>LAG ID</b>	Lag 1 ▾	<b>LAG Name</b>	ch1
<b>LAG Description</b>	[Empty text box]		
<b>Admin Mode</b>	Enable ▾	<b>Link Trap</b>	Disable ▾
<b>STP Mode</b>	Enable ▾	<b>Static Mode</b>	Disable ▾
<b>Hash Mode</b>	Src/Dest MAC, VLAN, EType, incoming port ▾		

**Port Selection Table**

▶ Unit 1

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.
  - **Enhanced Hashing mode** - Features MODULO-N operation based on the number of ports in the LAG, non-Unicast traffic and unicast traffic hashing using a common hash algorithm, excellent load balancing performance, and packet attributes selection based on the packet type:
    - For L2 packets, source and destination MAC address are used for hash computation.
    - For L3 packets, source IP, destination IP address, TCP/UDP ports are used.
9. Use the **Port Selection Table** to select the ports as members of the LAG.

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

- [Routing Table](#) on page 166
- [IP](#) on page 171
- [VLAN](#) on page 186
- [ARP](#) on page 189
- [Router Discovery](#) on page 193

## 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 167
- [Advanced](#) on page 169

## Basic

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

- [Route Configuration](#) on page 167

### Route Configuration

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

The screenshot shows the 'Route Configuration' page with two main sections:

**Configure Routes**

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

### 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

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 169
- [Route Preferences](#) on page 171

### Route Configuration

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

The screenshot shows the 'Route Configuration' page. It features two main sections:

- Configure Routes:** A table with columns: Route Type, Network Address, Subnet Mask, Next Hop IP Address, Preference, and Identifier. Below the table is a row of input fields corresponding to these columns.
- Learned Routes:** A table with columns: Route Type, Network Address, Subnet Mask, Protocol, Next Hop Interface, Next Hop IP Address, Preference, and Metric.

### 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

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**.

## 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.

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 171
- [Advanced](#) on page 178

### Basic

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

- [IP Configuration](#) on page 171
- [Statistics](#) on page 173

### 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**.

### IP Configuration

:: IP Configuration ?

<b>Default Time to Live</b>	64	
<b>Routing Mode</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>ICMP Echo Replies</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
<b>ICMP Redirects</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<b>ICMP Rate Limit Interval</b>	<input style="width: 150px;" type="text" value="1000"/>	(0 to 2147483647 ms)
<b>ICMP Rate Limit Burst Size</b>	<input style="width: 150px;" type="text" value="100"/>	(1 to 200)
<b>Maximum Next Hops</b>	1	
<b>Maximum Routes</b>	64	
<b>Select to configure Global Default Gateway</b>	<input type="checkbox"/>	
<b>Global Default Gateway</b>	<input style="width: 150px;" type="text" value="0.0.0.0"/>	

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.

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	9835
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	9017
IpOutRequests	7956
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	60
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	1
IcmpInErrors	0
IcmpInDestUnreachs	0
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSrcQuenchs	0
IcmpInRedirects	0
IcmpInEchos	0
IcmpInEchoReps	1
IcmpInTimestamps	0
IcmpInTimestampReps	0
IcmpInAddrMasks	0
IcmpInAddrMaskReps	0
IcmpOutMsgs	1
IcmpOutErrors	0
IcmpOutDestUnreachs	0
IcmpOutTimeExcds	0

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.

## Web Management User Guide

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.
IcmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.

## Web Management User Guide

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.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.



## Web Management User Guide

Field	Description
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 178
- [IP Statistics](#) on page 179
- [IP Interface Configuration](#) on page 183
- [Secondary IP Address](#) on page 186

### 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**.

### IP Configuration

?

**IP Configuration**

Default Time to Live	64	
Routing Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
ICMP Echo Replies	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
ICMP Redirects	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
ICMP Rate Limit Interval	<input style="width: 150px;" type="text" value="1000"/>	(0 to 2147483647 ms)
ICMP Rate Limit Burst Size	<input style="width: 150px;" type="text" value="100"/>	(1 to 200)
Maximum Next Hops	1	
Maximum Routes	64	
Select to configure Global Default Gateway	<input type="checkbox"/>	
Global Default Gateway	<input style="width: 150px;" type="text" value="0.0.0.0"/>	

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 Ratelimiting 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.

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**.

The screenshot shows the 'IP Statistics' page with a title bar and a list of metrics. The metrics are listed in two columns: the metric name on the left and its corresponding value on the right. The values are as follows:

Metric	Value
IpInReceives	9884
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	9056
IpOutRequests	8002
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	60
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	1
IcmpInErrors	0
IcmpInDestUnreachs	0
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSrcQuenchs	0
IcmpInRedirects	0

## Web Management User Guide

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.

## Web Management User Guide

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.
IcmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.

## Web Management User Guide

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.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.

Field	Description
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**

IP Interface Configuration

1 VLANs All

Port	Description	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode	Link Speed
<input type="checkbox"/>			<input type="text" value="None"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="Disable"/>	<input type="text" value="Enable"/>	
<input type="checkbox"/>	Q/1		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/2		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/3		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/4		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/5		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/6		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/7		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/8		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/9		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/10		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/11		None	0.0.0.0	0.0.0.0	Disable	Enable	
<input type="checkbox"/>	Q/12		None	0.0.0.0	0.0.0.0	Disable	Enable	

1 VLANs All

Forward Net Directed Broadcasts	Active State	MAC Address	Encapsulation Type	Proxy Arp	Local Proxy Arp	Bandwidth	ICMP Destination Unreachables	ICMP Redirects	IP M
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	100000	Enable	Disable	1500
Disable		00:07:03:05:05:07	Ethernet	Enable	Disable	1000000	Enable	Disable	1500

Go To Interface

1. Use **Go To Interface** to enter the Interface in unit/slot/port format and click **Go**. The entry corresponding to the specified interface is selected.
2. Use **Port** to select the interface for which data is to be displayed or configured.
3. Use **Description** to enter the description for the interface.
4. Use **IP Address Configuration Method** to enter the method by which an IP address is configured on the interface. There are three methods: None, Manual, and DHCP. By default the method is None. Method 'None' should be used to reset the DHCP method.

---

**Note:** When the configuration method is changed from **DHCP** to **None** there will be a minor delay before the page refreshes.

---

5. Use **IP Address** to enter the IP address for the interface.
6. 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.
7. Use **Routing Mode** to enable or disable routing for an interface. The default value is enable.
8. 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.
9. 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.
10. 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.



11. Use **Proxy Arp** to disable or enable proxy Arp for the specified interface from the pull-down menu.
12. Use **Local Proxy Arp** to disable or enable Local Proxy ARP for the specified interface from the pull-down menu.
13. 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).
14. 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.
15. 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.
16. 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.

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.

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

## 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 187
- [VLAN Routing Configuration](#) on page 188

## 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**.

The screenshot shows the 'VLAN Routing Wizard' interface. At the top, there's a title bar with the text 'VLAN Routing Wizard' and a help icon. Below the title bar, there are several input fields: 'Vlan ID' (containing '0'), 'IP Address', and 'Network Mask'. Underneath these fields, there are two expandable sections: 'Unit 1' and 'LAG', each with a plus sign icon to its left, indicating they can be expanded to show more options.

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**.

The screenshot shows a web interface titled "VLAN Routing Configuration". Below the title is a table with the following columns: "VLAN ID", "Port", "MAC Address", "IP Address", and "Subnet Mask". The "VLAN ID" column contains a dropdown menu with a small square icon to its left. The "IP Address" and "Subnet Mask" columns contain text input fields. There is a small red question mark icon in the top right corner of the table area.

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.

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 189
- [Advanced](#) on page 190

### Basic

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

- [ARP Cache](#) on page 190

## 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**.

ARP Cache		
IP Address	Port	MAC Address
10.27.34.64	0/12	00:0F:FE:00:8E:76
10.27.34.58	0/12	C8:0A:A9:32:F3:63
10.27.34.1	0/12	00:16:9C:E1:D8:00

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 190
- [ARP Table Configuration](#) on page 192

### Static ARP Cache

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

ARP Static Configuration	
IP Address	MAC Address
<input type="text"/>	<input type="text"/>

ARP Cache				
Port	IP Address	MAC Address	Type	Age

## 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.

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**.

### ARP Table Configuration

**ARP Table Configuration** ?

<b>Age Time(secs)</b>	<input type="text" value="1200"/>	(15 to 21600)
<b>Response Time(secs)</b>	<input type="text" value="10"/>	(1 to 10)
<b>Retries</b>	<input type="text" value="10"/>	(0 to 10)
<b>Cache Size</b>	<input type="text" value="512"/>	(160 to 512)
<b>Dynamic Renew</b>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
<b>Total Entry Count</b>	0	
<b>Peak Total Entries</b>	0	
<b>Active Static Entries</b>	0	
<b>Configured Static Entries</b>	0	
<b>Maximum Static Entries</b>	16	
<b>Remove From Table</b>	<input type="text" value="None"/> <span style="float: right;">▼</span>	

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.

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.

## Router Discovery

To display the Router Discovery page, click **Routing > Router Discovery**.

The screenshot shows the 'Router Discovery Configuration' page. At the top, there is a 'Go To Interface' search bar with a 'GO' button. Below this is a table with the following columns: Interface, Advertise Mode, Advertise Address, Maximum Advertise Interval, Minimum Advertise Interval, Advertise Lifetime, and Preference Level. The table lists 13 interfaces (0/1 to 0/12), all with 'Advertise Mode' set to 'Disable', 'Advertise Address' set to '224.0.0.1', and varying 'Maximum Advertise Interval' and 'Minimum Advertise Interval' values. The 'Advertise Lifetime' is consistently 1800 and 'Preference Level' is 0 for all entries.

Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval	Minimum Advertise Interval	Advertise Lifetime	Preference Level
0/1	Disable	224.0.0.1	600	450	1800	0
0/2	Disable	224.0.0.1	600	450	1800	0
0/3	Disable	224.0.0.1	600	450	1800	0
0/4	Disable	224.0.0.1	600	450	1800	0
0/5	Disable	224.0.0.1	600	450	1800	0
0/6	Disable	224.0.0.1	600	450	1800	0
0/7	Disable	224.0.0.1	600	450	1800	0
0/8	Disable	224.0.0.1	600	450	1800	0
0/9	Disable	224.0.0.1	600	450	1800	0
0/10	Disable	224.0.0.1	600	450	1800	0
0/11	Disable	224.0.0.1	600	450	1800	0
0/12	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 from the pull-down menu. If you select enable, Router Advertisements will be transmitted from the selected interface.

3. Use **Advertise Address** 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 the IP Address to be used to advertise the router.
5. Use **Maximum Advertise Interval** to enter the maximum 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.
8. Use **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
9. Use **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.



# 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 197
- [Differentiated Services](#) on page 204

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 197
- [Advanced](#) on page 199

### Basic

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

- [CoS Configuration](#) on page 197

### 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 199
- [802.1p to Queue Mapping](#) on page 200 (Advanced)
- [IP DSCP to Queue Mapping](#) on page 201 (Advanced)
- [CoS Interface Configuration](#) on page 202 (Advanced)
- [Interface Queue Configuration](#) on page 203 (Advanced)

### CoS Configuration

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

The screenshot shows the 'CoS Configuration' page with a title bar and a help icon. Below the title bar, there are two main sections: 'Global' and 'Interface'. Each section has a radio button, a dropdown menu for selection, and a 'Trust Mode' dropdown menu. The 'Global' section is selected, and its 'Trust Mode' is set to 'trust dot1p'. The 'Interface' section is unselected, and its 'Trust Mode' is also set to 'trust dot1p'.

Configuration Type	Selection	Trust Mode
Global	All	trust dot1p
Interface	0/1	trust dot1p

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

### 802.1p to Queue Mapping

**Interface Selection** ?

Interface  ▼

**802.1p to Queue Mapping** ?

802.1p Priority	0	1	2	3	4	5	6	7
Queue	1 ▼	0 ▼	0 ▼	1 ▼	2 ▼	2 ▼	3 ▼	3 ▼

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**.

### IP DSCP to Queue Mapping

**:: Interface Selection** ?

Interface  ▼

**:: IP DSCP to Queue Mapping** ?

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 ▼

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**.

The screenshot shows the 'CoS Interface Configuration' page. At the top, there is a header with the title 'CoS Interface Configuration' and a help icon. Below the header, there is a section for 'LAGS All' with a 'Go To Interface' input field and a 'GO' button. The main content is a table with the following columns: 'Interface', 'Interface Trust Mode', and 'Interface Shaping Rate'. The table contains 12 rows, each representing an interface from 0/1 to 0/12. Each row has a checkbox on the left, the interface name, the trust mode (all are 802.1p), and the shaping rate (all are 0). At the bottom of the table, there is another 'Go To Interface' input field and a 'GO' button.

	Interface	Interface Trust Mode	Interface Shaping Rate
<input type="checkbox"/>	0/1	802.1p	0
<input type="checkbox"/>	0/2	802.1p	0
<input type="checkbox"/>	0/3	802.1p	0
<input type="checkbox"/>	0/4	802.1p	0
<input type="checkbox"/>	0/5	802.1p	0
<input type="checkbox"/>	0/6	802.1p	0
<input type="checkbox"/>	0/7	802.1p	0
<input type="checkbox"/>	0/8	802.1p	0
<input type="checkbox"/>	0/9	802.1p	0
<input type="checkbox"/>	0/10	802.1p	0
<input type="checkbox"/>	0/11	802.1p	0
<input type="checkbox"/>	0/12	802.1p	0

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**.

	Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
<input type="checkbox"/>		0			
<input type="checkbox"/>	0/1	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/2	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/3	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/4	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/5	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/6	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/7	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/8	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/9	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/10	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/11	0	0	Weighted	TailDrop
<input type="checkbox"/>	0/12	0	0	Weighted	TailDrop

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 205
- [Auto VoIP Configuration](#) on page 207
- [Basic](#) on page 207
- [Advanced](#) on page 209

## 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**.

The screenshot shows the 'Diffserv Wizard' configuration window. It has a title bar with the text 'Diffserv Wizard' and a help icon. The main area contains several configuration fields:

- Traffic Type:** A dropdown menu set to 'VOIP'.
- Committed Rate (Kbps):** A text input field containing the value '0'.
- Policing:** A checkbox that is checked.
- Outbound Priority:** A dropdown menu set to 'Medium'.

At the bottom of the window, there are two expandable sections, each with a right-pointing arrow:

- Unit 1**
- LAG**

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**.

	Interface	Auto VoIP Mode	Traffic Class
<input type="checkbox"/>	0/1	Disable	7
<input type="checkbox"/>	0/2	Disable	7
<input type="checkbox"/>	0/3	Disable	7
<input type="checkbox"/>	0/4	Disable	7
<input type="checkbox"/>	0/5	Disable	7
<input type="checkbox"/>	0/6	Disable	7
<input type="checkbox"/>	0/7	Disable	7
<input type="checkbox"/>	0/8	Disable	7
<input type="checkbox"/>	0/9	Disable	7
<input type="checkbox"/>	0/10	Disable	7
<input type="checkbox"/>	0/11	Disable	7
<input type="checkbox"/>	0/12	Disable	7

- Interface** - Specifies the Auto VoIP configurable interfaces.
- 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)

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 208

## 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**.

### DiffServ Configuration

:: DiffServ Configuration
?

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	36

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.



Field	Description
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 209
- [Class Configuration](#) on page 211
- [IPv6 Class Configuration](#) on page 214
- [Policy Configuration](#) on page 216
- [Service Interface Configuration](#) on page 220
- [Service Statistics](#) on page 220

### 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**.

**DiffServ Configuration**

DiffServ Configuration ?

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	36

To configure the global DiffServ mode:

1. Select the administrative mode for DiffServ:
  - **Enable.** Differentiated Services are active.
  - **Disable.** The DiffServ configuration is retained and can be changed, but it is not active.
2. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make changes to the page, click **APPLY** to apply the changes to the system.

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

Field	Description
<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.

Field	Description
<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**.

The screenshot shows a web interface titled "Class Name". Below the title is a search bar labeled "Class Name" with a question mark icon. Below the search bar is a table with two columns: "Class Name" and "Class Type". The "Class Name" column has a check box and a text input field. The "Class Type" column has a dropdown menu.

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.

**Class Name**

Class Name

	Class Name	Class Type
<input type="checkbox"/>	<a href="#">Class1</a>	All

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

**Class Configuration**

Class Information

Class Name:

Class Type:

DiffServ Class Configuration

Match Every

Reference Class

Class Of Service

VLAN  (0 to 4095)

Secondary Class of Service

Secondary VLAN  (0 to 4095)

Ethernet Type   (600 to ffff hex)

Source MAC Address  Mask

Destination MAC Address  Mask

Protocol Type   (0 to 255)

Source IP Address  Mask

Source L4 Port   (0 to 65535)

Destination IP Address  Mask

Destination L4 Port   (0 to 65535)

IP DSCP   (0 to 63)

Precedence Value  (0 to 7)

IP ToS Bit Value  Bit Mask

Class Summary

Match Criteria	Values
Match Every	Any
Reference Class	
Class Of Service	0
VLAN	
Secondary Class of Service	0
Secondary VLAN	
Ethernet Type	Appletalk
Source MAC	
Destination MAC	
Protocol Type	ICMP
Source IP	
Source L4 Port	domain
Destination IP	
Destination L4 Port	domain
IP DSCP	af11
Precedence Value	0
IP ToS	

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.

### IPv6 Class Configuration

Use the IPv6 Class Configuration page to add a new IPv6 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 > IPv6 Class Configuration**.

IPv6 Class Name	
Class Name	Class Type
<input type="checkbox"/> <input type="text"/>	<input type="text"/>

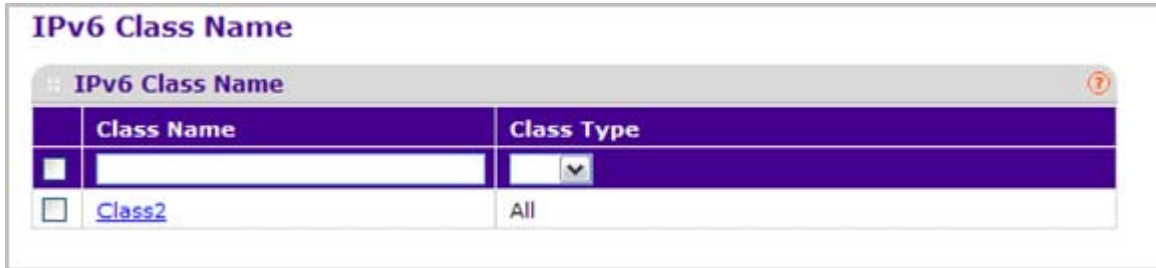
To configure a DiffServ class:

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.
 

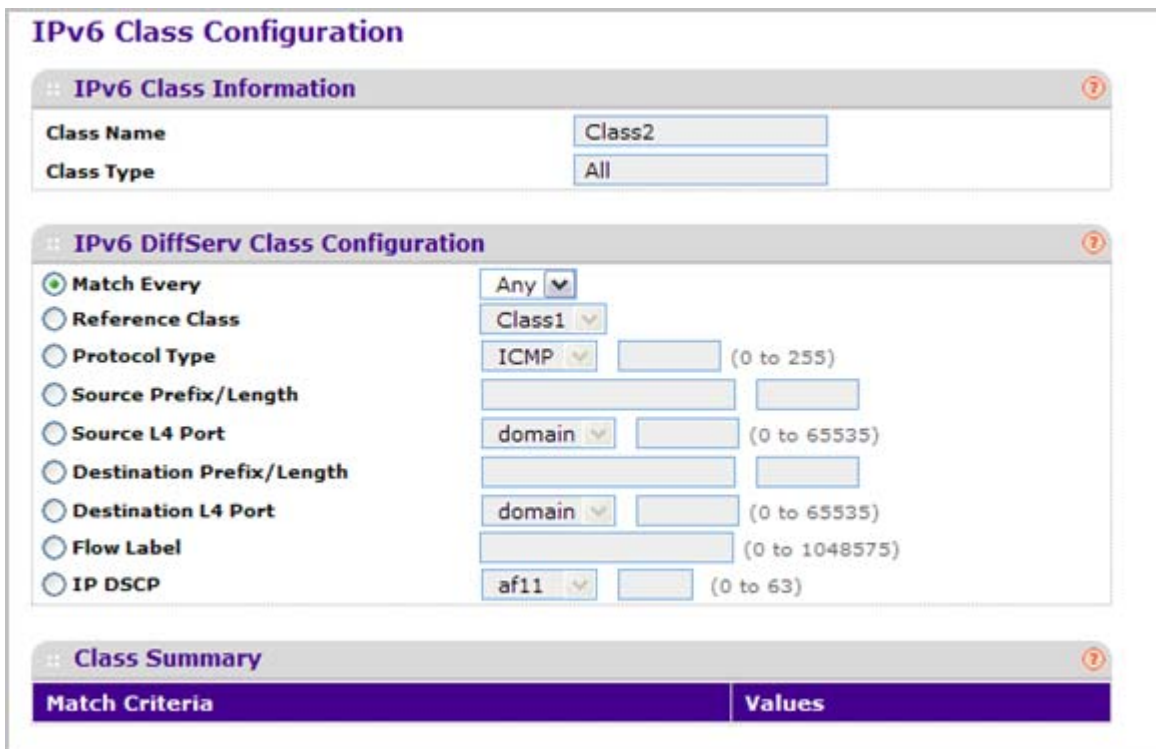
The switch supports only the **Class Type** value **All**, which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria. Only when a new class is created, this field is a selector field. After class creation 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:

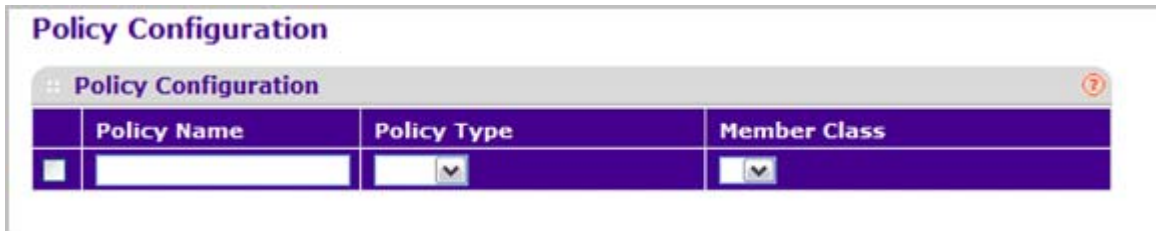
- **Match Every** - This adds to the specified class definition a match condition whereby all packets are considered to belong to the class.
  - **Reference Class** - This lists the class(es) that can be assigned as reference class(es) to the current class.
  - **Protocol Type** - This lists the keywords for the layer 4 protocols from which one can be selected. The list includes 'other' as an option for the remaining values.
  - **Source Prefix Length** - This is a valid Source IPv6 Prefix to compare against an IPv6 Packet. Prefix is always specified with the Prefix Length. Prefix can be entered in the range of ::0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and Prefix Length can be entered in the range of 0 to 128.
  - **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 Prefix/Length** - This is a valid Destination IPv6 Prefix to compare against an IPv6 Packet. Prefix is always specified with the Prefix Length. Prefix can be entered in the range of ::0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and Prefix Length can be entered in the range of 0 to 128.
  - **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.
  - **Flow Label** - This is a 20-bit number that is unique to an IPv6 Packet, used by end stations to signify Quality of Service handling in routers. Flow Label can be specified in the range of (0 to 1048575).
  - **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.
5. **Match Criteria** - Displays the configured match criteria for the specified class.
  6. **Values** - Displays the values of the configured match criteria.
  7. Click **CANCEL** to cancel the configuration on the screen. Resets 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.

### *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**.

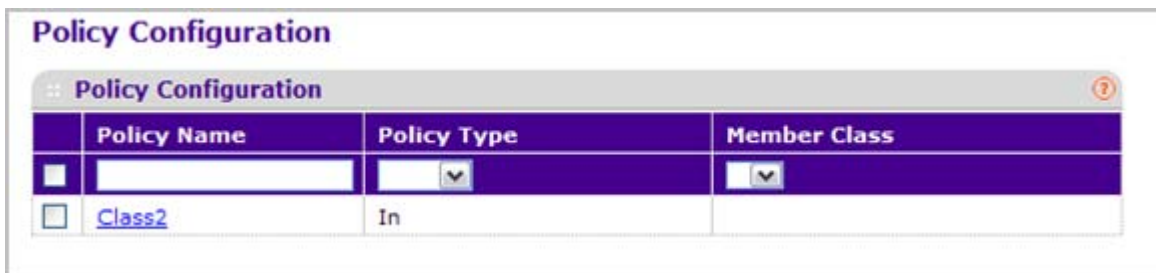




1. Use **Policy Name** to uniquely identify a policy using a case-sensitive alphanumeric string from 1 to 31 characters.
2. **Member Class** - This lists all existing DiffServ classes currently defined as members of the specified Policy, from which one can be selected. This list is automatically updated 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.

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.

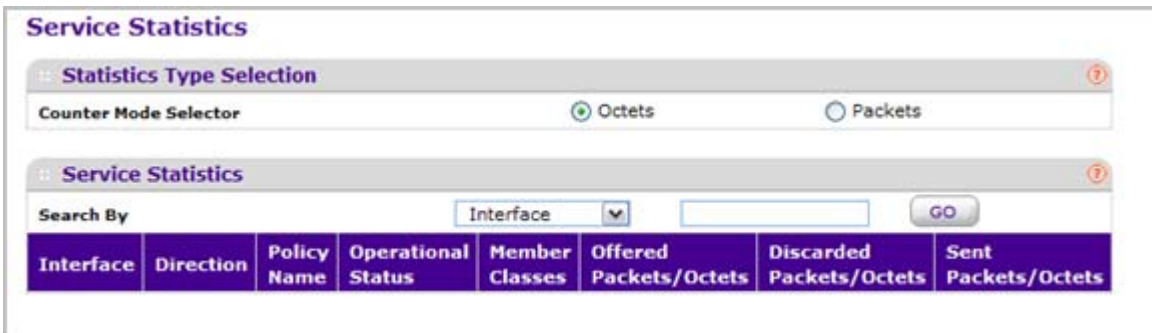
Field	Description
Direction	Shows that the traffic direction of this service interface is In.
Operational Status	Shows the operational status of this service interface, either Up or Down.

## 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**.



**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.

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.

## Web Management User Guide

Field	Description
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.



# 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 224
- [Configuring Management Access](#) on page 241
- [Port Authentication](#) on page 253
- [Traffic Control](#) on page 262
- [Control](#) on page 275
- [Configuring Access Control Lists](#) on page 288

## 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 224
- [Enable Password Configuration](#) on page 227
- [Line Password Configuration](#) on page 227
- [RADIUS](#) on page 228
- [Configuring TACACS+](#) on page 234
- [Authentication List Configuration](#) on page 236
- [Login Sessions](#) on page 240

### Local User

From the Local User link, you can access the following pages:

- [User Management](#) on page 225
- [User Password Configuration](#) on page 226



## 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**.

The screenshot shows the 'User Management' page with a 'Manage Users' section. It contains a table with the following columns: User Name, Edit Password, Password, Confirm Password, Access Mode, Lockout Status, and Password Expiration Date. The table lists two users: 'admin' and 'guest'. The 'admin' user has 'READ\_WRITE' access and 'FALSE' lockout status. The 'guest' user has 'READ\_ONLY' access and 'FALSE' lockout status. There is also a form for adding a new user with fields for User Name, Edit Password (set to 'Disable'), Password, Confirm Password, and Access Mode.

	User Name	Edit Password	Password	Confirm Password	Access Mode	Lockout Status	Password Expiration Date
<input type="checkbox"/>		Disable	*****	*****			
<input type="checkbox"/>	admin	Disable	*****	*****	READ_WRITE	FALSE	
<input type="checkbox"/>	guest	Disable	*****	*****	READ_ONLY	FALSE	

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.

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 a web interface titled "Password Configuration". It contains a table with four rows, each representing a configuration field. The first row is "Password Minimum Length" with a value of 8 and a range of (0 to 64). The second row is "Password Aging (days)" with a value of 0 and a range of (0 to 365). The third row is "Password History" with a value of 0 and a range of (0 to 10). The fourth row is "Lockout Attempts" with a value of 0 and a range of (0 to 5). Each field has a text input box and a range indicator to its right.

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.

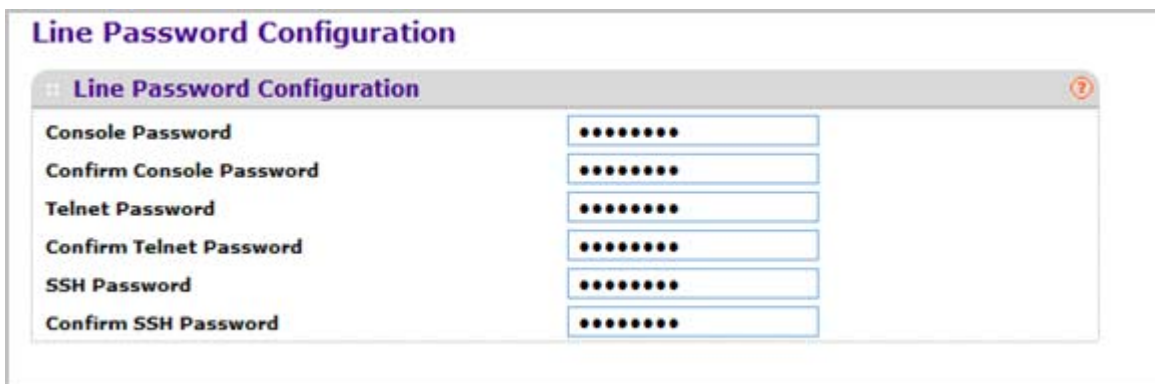
To display the Enable Password Configuration page, click **Security > Management Security > Enable Password**.



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:

- [Radius Configuration](#) on page 229
- [RADIUS Server Configuration](#) on page 230
- [Accounting Server Configuration](#) on page 232

## Radius 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 shows the 'Radius Configuration' page with the following settings:

Field	Value	Range
Current Server Address	[Blank]	
Number of Configured Authentication Servers	0	
Number of Configured Accounting Servers	0	
Number of Named Authentication Server Groups	0	
Number of Named Accounting Server Groups	0	
Max Number of Retransmits	4	(1 to 15)
Timeout Duration (secs)	5	(1 to 30)
Accounting Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Radius Attribute 4 Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	

The Current Server IP Address field is blank if no servers are configured (see “RADIUS Server Configuration” on page 6-230). 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.

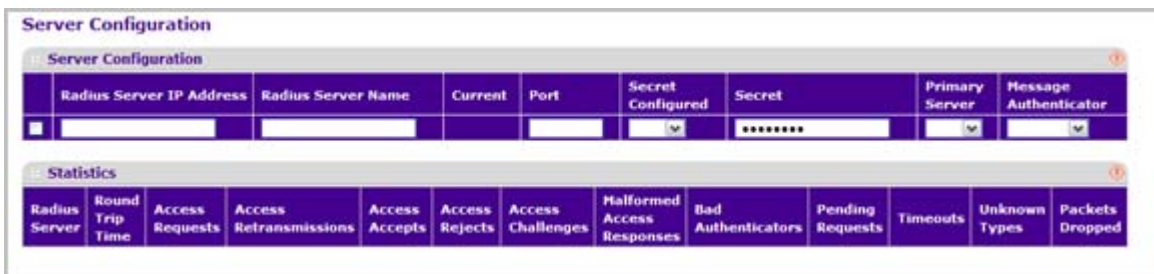
3. From the **Accounting Mode** menu, select whether the RADIUS accounting mode is enabled or disabled on the current server.
4. Use **RADIUS Attribute 4** to enable or disable RADIUS attribute 4. Default value is Disable.  
This is an optional field and can be seen only when RADIUS attribute 4 is enabled. It takes IP address value in the format (xx.xx.xx.xx).

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:

1. 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.
2. 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.
  3. 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.

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.

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.

Field	Description
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access-responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

### Accounting Server Configuration

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

To access the RADIUS Accounting Server **Configuration** page, click **Security > Management Security > RADIUS > Accounting Server Configuration**.

To configure the RADIUS accounting server:

1. In the **Accounting Server 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.

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.

Field	Description
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 234
- [TACACS+ Server Configuration](#) on page 235

### 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**.

The screenshot shows the 'TACACS Configuration' page. It features a title bar with the text 'TACACS Configuration' and a help icon. Below the title bar, there are two configuration fields:

- Key String:** A text input field with a value range of '(0 to 128)'.
- Connection Timeout:** A text input field with a value of '5' and a value range of '(1 to 30)'.

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

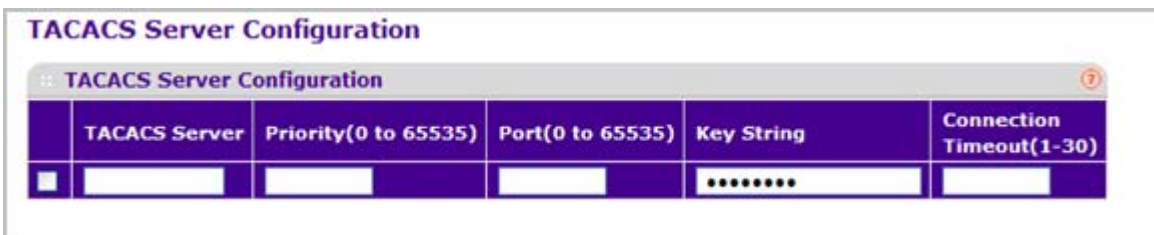
range is 0–128 characters. The key must match the key configured on the TACACS+ server.

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 236
- [Enable Authentication List](#) on page 237
- [Dot1x Authentication List](#) on page 238
- [HTTP Authentication List](#) on page 238
- [HTTPS Authentication List](#) on page 239

### 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**.

Login Authentication List			
List Name	1	2	3
<input type="checkbox"/> defaultList	Local		
<input type="checkbox"/> networkList	Local		

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. Click **ADD** to add a new login list to the switch.
6. 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. A 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**.

Enable Authentication List				
:: Enable Authentication List				
	List Name	1	2	3
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	enableList	None		

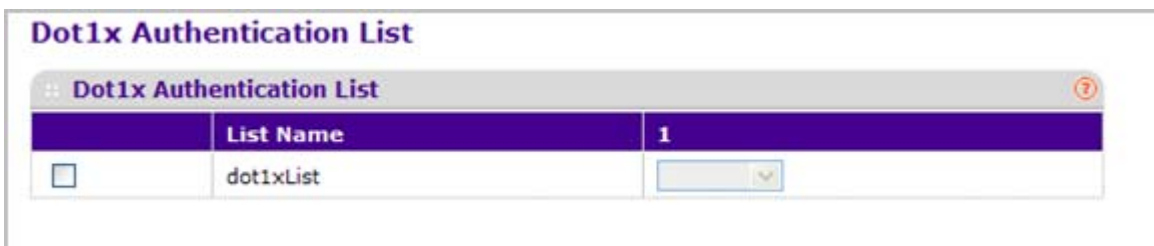
1. **List Name** - If you are creating a new enable list, enter the name you want to assign. It can be up to 15 alphanumeric characters long and is not case sensitive.
2. Use the dropdown menu to select the method that should appear first in the selected authentication login list. If you select a method 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. Click **ADD** to add a new login list to the switch.
6. 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**.

HTTP Authentication List				
:: HTTP Authentication List				
	List Name	1	2	3
<input type="checkbox"/>	httpList	Local		

- List Name** - Select the HTTP list name for which you want to configure data.
- 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.
- 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.
- Use the dropdown menu to select the method, if any, that should appear third 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**.

HTTPS Authentication List				
:: HTTPS Authentication List				
	List Name	1	2	3
<input type="checkbox"/>	httpsList	Local		

- 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.

## Login Sessions

To display the Login Sessions page, click **Security > Management Security > Login Sessions**.

The screenshot shows a web interface titled "Login Sessions". Below the title is a table with the following data:

ID	User Name	Connection From	Idle Time	Session Time	Session Type
11	admin	10.12.17.158	00:00:00	00:59:31	HTTP

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 241
- [HTTPS Configuration](#) on page 243
- [SSH](#) on page 246
- [Telnet](#) on page 249
- [Console Port](#) on page 251
- [Denial of Service](#) on page 252

### HTTP

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

- [HTTP Configuration](#) on page 241

#### *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.

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 243
- [Certificate Management](#) on page 244
- [Certificate Download](#) on page 245

### 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**.

HTTPS Configuration	
HTTPS Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
SSL Version 3	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
TLS Version 1	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
HTTPS Port	<input type="text" value="443"/> (1 to 65535)
HTTPS Session Soft Timeout (Minutes)	<input type="text" value="60"/> (1 to 60)
HTTPS Session Hard Timeout (Hours)	<input type="text" value="24"/> (1 to 168)
Maximum Number of HTTPS Sessions	<input type="text" value="16"/> (0 to 16)
Authentication List	HttpsListName

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.

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.

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 246
- [Host Keys Management](#) on page 247
- [Host Keys Download](#) on page 248

### SSH Configuration

To display the SSH Configuration page, click **Security > Access > SSH > SSH Configuration**.

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.

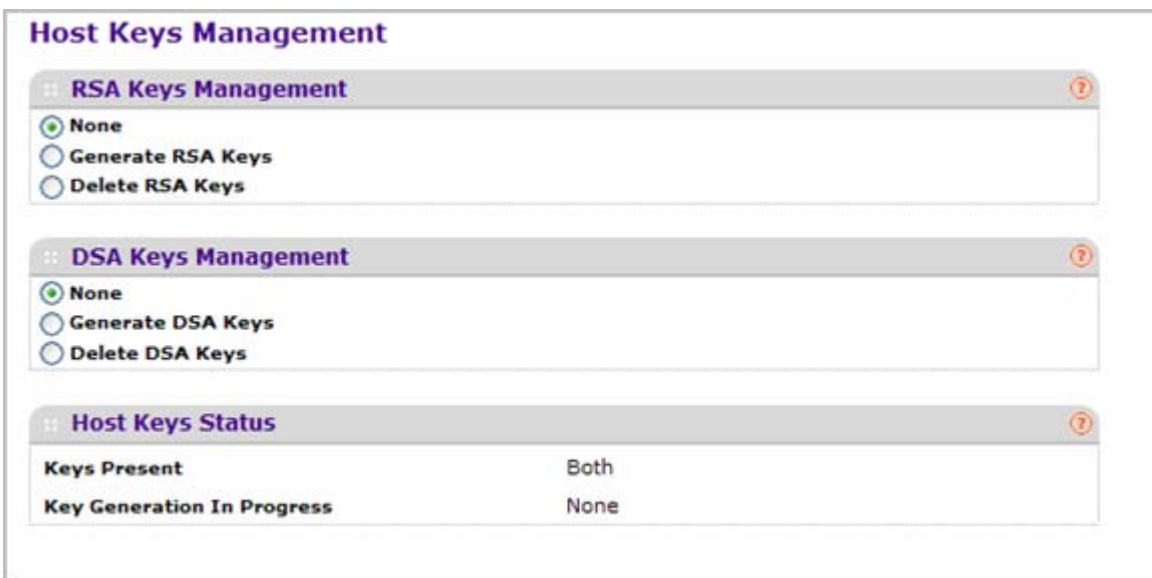
3. Use **SSH Version 2** to Enable or Disable Protocol Level 2 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.
4. Use **SSH Session Timeout** to configure the inactivity time-out value for incoming SSH sessions to the switch. The acceptable 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.

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.

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**.

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**.

The screenshot displays the TELNET configuration interface, organized into three main sections:

- Authentication List:** Includes a dropdown for 'Login Authentication List' (set to 'networkList') and a dropdown for 'Enable Authentication List' (set to 'enableList').
- Inbound Telnet:** Features a dropdown for 'Telnet Server Admin Mode' (set to 'Enable'), radio buttons for 'Allow new telnet sessions' (with 'Enable' selected), and input fields for 'Session Timeout' (5 minutes), 'Maximum Number of Sessions' (5), and 'Current Number of Sessions' (0).
- Outbound Telnet:** Features radio buttons for 'Allow new telnet sessions' (with 'Enable' selected), and input fields for 'Session Timeout' (5 minutes), 'Maximum Number of Sessions' (5), and 'Current Number of Sessions' (0).

### *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**.

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.

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**.

Configuration Item	Value	Range	State
Denial of Service Min TCP Header Size	20	(0 to 255)	Disable
Denial of Service ICMPv4			Disable
Denial of Service Max ICMPv4 Packet Size	512	(0 to 16376)	Disable
Denial of Service ICMPv6			Disable
Denial of Service Max ICMPv6 Packet Size	512	(0 to 16376)	Disable
Denial of Service First Fragment			Disable
Denial of Service ICMP Fragment			Disable
Denial of Service SIP=DIP			Disable
Denial of Service SMAC=DMAC			Disable
Denial of Service TCP FIN&URG&PSH			Disable
Denial of Service TCP Flag&Sequence			Disable
Denial of Service TCP Fragment			Disable
Denial of Service TCP Offset			Disable
Denial of Service TCP Port			Disable
Denial of Service TCP SYN			Disable
Denial of Service TCP SYN&FIN			Disable
Denial of Service UDP Port			Disable

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 than 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 254
- [Advanced](#) on page 255

## Basic

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

- [802.1X Configuration](#) on page 254

### 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 “Authentication List Configuration” on page 6-236.

---

- **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.

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 255
- [Port Authentication](#) on page 256
- [Port Summary](#) on page 259
- [Client Summary](#) on page 261

### 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.

- Use **Login** to select the login to apply to the specified user. All configured logins are displayed.

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.

The screenshot shows the 'Port Authentication' configuration page. At the top, there is a breadcrumb trail: 'Port Authentication'. Below it, there is a 'Go To Port' search box with a 'GO' button. The main content is a table with the following columns: Port, Control Mode, MAB, Quiet Period, Transmit Period, Guest VLAN ID, Guest VLAN Period, Unauthenticated VLAN ID, Supplicant Timeout, Server Timeout, Maximum Requests, PAE Capabilities, and Port Real-time status. The table contains 12 rows of data, all with 'Auto' control mode and 'Disable' MAB. At the bottom, there is another 'Go To Port' search box with a 'GO' button.

Port	Control Mode	MAB	Quiet Period	Transmit Period	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID	Supplicant Timeout	Server Timeout	Maximum Requests	PAE Capabilities	Port Real-time
<input type="checkbox"/> 0/1	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/2	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/3	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/4	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/5	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/6	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/7	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/8	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/9	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/10	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/11	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa
<input type="checkbox"/> 0/12	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disa

To configure 802.1X settings for the port:

- 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.
- 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.

## Port Summary

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

To access the Port Summary page, click **Security > Port Authentication > Advanced > Port Summary**.

Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Control Direction	Protocol Version	PAE Capabilities	Authenticator PAE State	Backend State	VLAN Assigned	VLAN Assigned Reason	Key Transmission Enabled	Session Timeout	Session Termination Action	Port Status	Port Method
0/1	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based
0/2	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based
0/3	Auto	Auto	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	Authorized	Port Based
0/4	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based
0/5	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based
0/6	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based
0/7	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based
0/8	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based
0/9	Auto	Auto	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	Authorized	Port Based
0/10	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based
0/11	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based
0/12	Auto	Auto	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	Authorized	Port Based

The following table describes the fields on the Port Summary page.

Field	Description
Port	Specifies the port whose settings are displayed in the current table row.
Control Mode	This field indicates the configured control mode for the port. Possible values are: <ul style="list-style-type: none"> <li>Force Unauthorized: The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized.</li> <li>Force Authorized: The authenticator PAE unconditionally sets the controlled port to authorized.</li> <li>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.</li> </ul>
Operating Control Mode	This field indicates the control mode under which the port is actually operating. Possible values are: <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>

## Web Management User Guide

Field	Description
Reauthentication Enabled	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.
Control Direction	This displays the control direction for the specified port. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator. This affects whether the unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames) or just in the incoming direction (disabling only the reception of incoming frames). This field is not configurable on some platforms.
Protocol Version	This field displays the protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1x specification. This field is not configurable.
PAE Capabilities	This field displays the port access entity (PAE) functionality of the selected port. Possible values are "Authenticator" or "Supplicant". This field is not configurable.
Authenticator PAE State	This field displays the current state of the authenticator PAE state machine. Possible values are: <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>
Backend State	This field displays the current state of the backend authentication state machine. Possible values are: <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>

Field	Description
Vlan Assigned	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.
Vlan Assigned Reason	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: <ul style="list-style-type: none"> <li>• “Radius”</li> <li>• “Unauth”</li> <li>• “Default”</li> <li>• “Not Assigned”</li> </ul>
Key Transmission Enabled	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.
Session Timeout	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.
Session Termination Action	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: <ul style="list-style-type: none"> <li>• “Default”</li> <li>• “Reauthenticate”</li> </ul> If the termination action is 'default' then at the end of the session, the client details are initialized. Otherwise re-authentication is attempted.
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**.

Port	User Name	Supplicant MAC Address	Session Time	Filter ID	VLAN ID	VLAN Assigned	Session Timeout	Termination Action
All								

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 263
- [Port Security](#) on page 265
- [Private Group](#) on page 270
- [Protected Ports Configuration](#) on page 272

- [Storm Control](#) on page 273

## MAC Filter

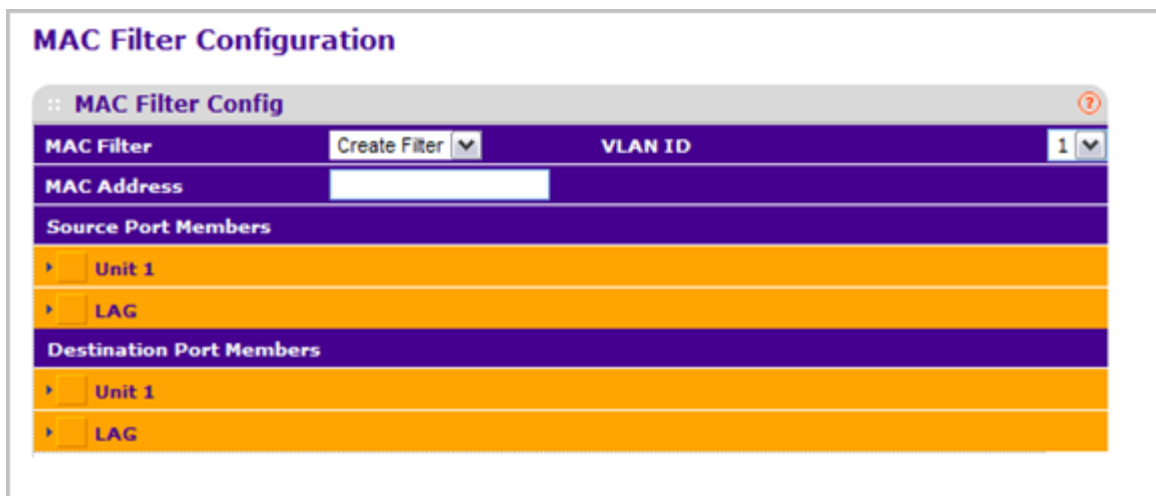
The MAC Filter folder contains links to the following features:

- [MAC Filter Configuration](#) on page 264
- [MAC Filter Summary](#) on page 265

## 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



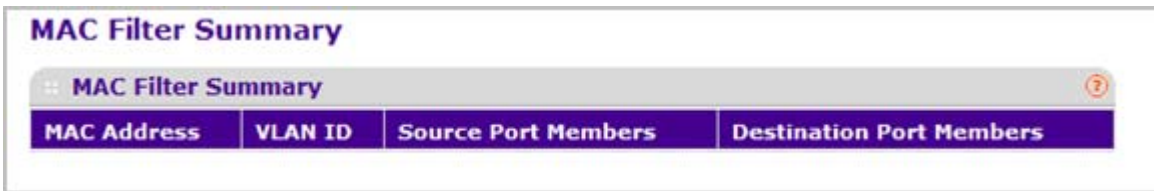
selected will be transmitted only out of ports that are in the list. Destination ports can be included only in the Multicast filter.

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:

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 266
- [Port Security Interface Configuration](#) on page 267
- [Dynamic MAC Address](#) on page 268
- [Static MAC Address](#) on page 269

## 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.

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**.

	Port	Security Mode	Max Allowed Dynamically Learned MAC	Max Allowed Statically Locked MAC	Violation Trap
<input type="checkbox"/>		<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
<input type="checkbox"/>	0/1	Disable	4096	48	Disable
<input type="checkbox"/>	0/2	Disable	4096	48	Disable
<input type="checkbox"/>	0/3	Disable	4096	48	Disable
<input type="checkbox"/>	0/4	Disable	4096	48	Disable
<input type="checkbox"/>	0/5	Disable	4096	48	Disable
<input type="checkbox"/>	0/6	Disable	4096	48	Disable
<input type="checkbox"/>	0/7	Disable	4096	48	Disable
<input type="checkbox"/>	0/8	Disable	4096	48	Disable
<input type="checkbox"/>	0/9	Disable	4096	48	Disable
<input type="checkbox"/>	0/10	Disable	4096	48	Disable
<input type="checkbox"/>	0/11	Disable	4096	48	Disable
<input type="checkbox"/>	0/12	Disable	4096	48	Disable

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**.

**Dynamic MAC Address Table**

**Port Security Settings**

Convert Dynamic Address to Static

Number Of Dynamic MAC Addresses Learned: 0

**Dynamic MAC Address Table**

Port List: 0/1

VLAN ID	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.

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**.

**Static MAC Address Configuration**

:: Port List ?

Interface  ▼

---

:: Static MAC Address Table ?

	Static MAC Address	VLAN ID
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="1"/> ▼

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 270
- [Private Group Membership](#) on page 271

### Private Group Configuration

To display the Private Group Configuration page, click **Security > Traffic Control > Private Group > Private Group Configuration**.

Private Group Configuration			
Private Group Configuration			
	Group Name	Group ID	Group Mode
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Community"/>

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.

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	This field identifies the mode of the Private Group you selected. The modes are: <ul style="list-style-type: none"> <li>• community</li> <li>• isolated</li> </ul> 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.

## 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 273
- [Storm Control Interface Configuration](#) on page 274

### 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**.

The screenshot shows the 'Port Configuration' page with a table for storm control settings. The table has columns for Port, Broadcast Storm (Recovery Mode, Recovery Level Type, Recovery Level), Multicast Storm (Recovery Mode, Recovery Level Type, Recovery Level), and Unicast Storm (Recovery Mode, Recovery Level Type, Recovery Level). Each row represents a port from 0/1 to 0/12. The 'Recovery Mode' column contains a checkbox and a pull-down menu. The 'Recovery Level Type' column contains a pull-down menu. The 'Recovery Level' column contains a text input field. The 'Recovery Mode' for Broadcast and Multicast Storm is 'Enable' and 'Disable' respectively. The 'Recovery Level Type' is 'Percent' for all. The 'Recovery Level' is '5' for all.

Port	Broadcast Storm			Multicast Storm			Unicast Storm		
	Recovery Mode	Recovery Level Type	Recovery Level	Recovery Mode	Recovery Level Type	Recovery Level	Recovery Mode	Recovery Level Type	Recovery Level
<input type="checkbox"/> 0/1	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/2	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/3	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/4	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/5	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/6	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/7	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/8	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/9	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/10	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/11	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 0/12	Enable	Percent	5	Disable	Percent	5	Disable	Percent	5

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.

Field	Description
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 275
- [IP Source Guard](#) on page 281
- [Dynamic ARP Inspection](#) on page 283

## DHCP Snooping

The DHCP Snooping folder contains links to the following features:

- [DHCP Snooping Global Configuration](#) on page 275
- [DHCP Snooping Interface Configuration](#) on page 277
- [DHCP Snooping Binding Configuration](#) on page 277
- [DHCP Snooping Persistent Configuration](#) on page 278
- [DHCP Snooping Statistics](#) on page 280

### *DHCP Snooping Global Configuration*

To display the DHCP Snooping Global Configuration page, click **Security > Control > DHCP Snooping > Global Configuration**.

### DHCP Snooping Global Configuration

**:: DHCP Snooping Global Configuration** ?

DHCP Snooping Mode  Disable  Enable

MAC Address Validation  Disable  Enable

**:: VLAN Configuration** ?

	VLAN ID	DHCP Snooping Mode
■	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/> ▼

### 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**.

Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
<input type="checkbox"/> 0/1	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/2	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/3	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/4	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/5	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/6	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/7	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/8	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/9	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/10	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/11	Disable	Disable	N/A	N/A
<input type="checkbox"/> 0/12	Disable	Disable	N/A	N/A

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**.

### DHCP Snooping Binding Configuration

:: Static Binding Configuration ?

	Interface	MAC Address	VLAN ID	IP Address
<input type="checkbox"/>	▼	□	▼	□

:: Dynamic Binding Configuration ?

Interface	MAC Address	VLAN ID	IP Address	Lease Time

### 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**.

The screenshot shows a web interface titled "DHCP Snooping Persistent Configuration". It features a header bar with the title and a help icon. Below the header, there are four configuration fields: "Store" with radio buttons for "Local" (selected) and "Remote"; "Remote IP Address" with a text box containing "0.0.0.0"; "Remote File Name" with an empty text box and a note "(1 to 32 alphanumeric characters)"; and "Write Delay" with a text box containing "300" and a note "(15 to 86400) seconds".

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**.

The screenshot shows the DHCP Snooping Statistics page. At the top, there is a header "DHCP Snooping Statistics" with a help icon. Below the header, there is a sub-header "LAGS All". The main content is a table with the following data:

Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs Received
0/1	0	0	0
0/2	0	0	0
0/3	0	0	0
0/4	0	0	0
0/5	0	0	0
0/6	0	0	0
0/7	0	0	0
0/8	0	0	0
0/9	0	0	0
0/10	0	0	0
0/11	0	0	0
0/12	0	0	0

At the bottom of the table, there is a sub-header "LAGS All".

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 281
- [IP Source Guard Binding Configuration](#) on page 282

### IP Source Guard Interface Configuration

To display the IP Source Guard Interface Configuration page, click **Security > Control > IP Source Guard > Interface Configuration**.

The screenshot shows the 'IP Source Guard Interface Configuration' page. At the top, there is a search bar labeled 'Go To Interface' with a 'GO' button. Below this is a table with the following columns: 'Interface', 'IPSG Mode', and 'IPSG Port Security'. The table contains 12 rows, each representing an interface from 0/1 to 0/12. Each row has a checkbox on the left, and the 'IPSG Mode' and 'IPSG Port Security' columns are currently set to 'Disable'. At the bottom of the table, there is another 'Go To Interface' search bar and a 'GO' button.

Interface	IPSG Mode	IPSG Port Security
<input type="checkbox"/> 0/1	Disable	Disable
<input type="checkbox"/> 0/2	Disable	Disable
<input type="checkbox"/> 0/3	Disable	Disable
<input type="checkbox"/> 0/4	Disable	Disable
<input type="checkbox"/> 0/5	Disable	Disable
<input type="checkbox"/> 0/6	Disable	Disable
<input type="checkbox"/> 0/7	Disable	Disable
<input type="checkbox"/> 0/8	Disable	Disable
<input type="checkbox"/> 0/9	Disable	Disable
<input type="checkbox"/> 0/10	Disable	Disable
<input type="checkbox"/> 0/11	Disable	Disable
<input type="checkbox"/> 0/12	Disable	Disable

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**.

### IP Source Guard Binding Configuration

**Static Binding Configuration**

	Interface	MAC Address	VLAN ID	IP Address	Filter Type
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**Dynamic Binding Configuration**

Interface	MAC Address	VLAN ID	IP Address	Filter Type
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

### Static Binding Configuration

1. **Interface** - Selects the interface to add a binding into the IPSPG 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 IPSPG static binding entry into the database.
6. Click **DELETE** to delete selected static entries from the database.

### Dynamic Binding Configuration

Field	Description
Interface	Displays the interface to add a binding into the IPSPG 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.

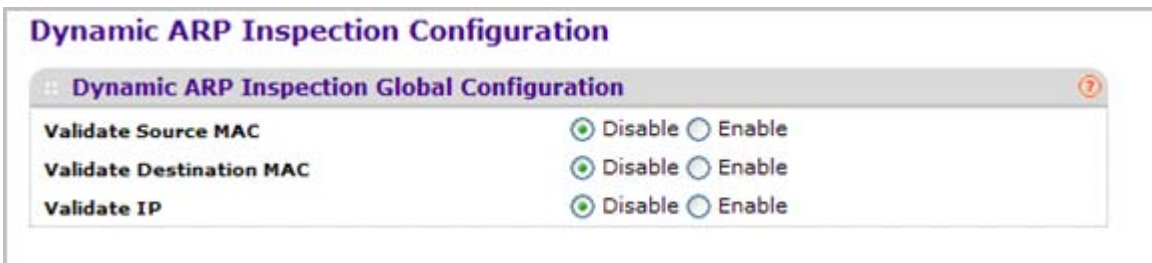
## Dynamic ARP Inspection

The Dynamic ARP Inspection (DAI) folder contains links to the following features:

- [DAI Configuration](#) on page 283
- [DAI VLAN Configuration](#) on page 283
- [DAI Interface Configuration](#) on page 285
- [DAI ACL Configuration](#) on page 285
- [DAI ACL Rule Configuration](#) on page 286
- [DAI Statistics](#) on page 286

### 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**.

**Dynamic ARP Inspection Configuration**

:: VLAN Configuration ?

	VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
<input type="checkbox"/>		<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
<input type="checkbox"/>	1	Disable	Enable		Disable

- VLAN ID** - Select the DAI Capable VLANs for which information has to be displayed or configured.
- 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.
- 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.
- 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.
- 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**.

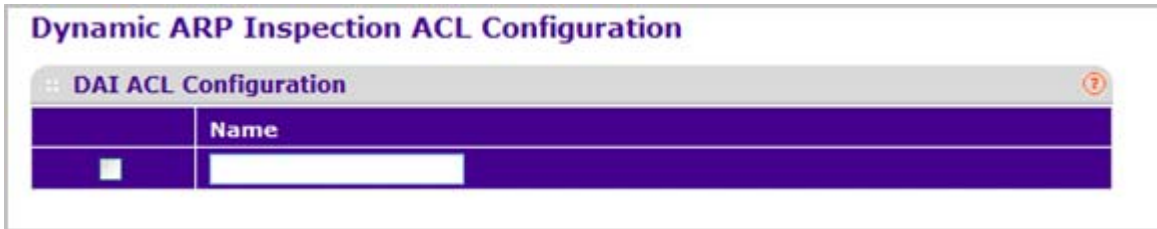
Interface	Trust Mode	Rate Limit(pps)	Burst Interval(secs)
<input type="checkbox"/> 0/1	Disable	15	1
<input type="checkbox"/> 0/2	Disable	15	1
<input type="checkbox"/> 0/3	Disable	15	1
<input type="checkbox"/> 0/4	Disable	15	1
<input type="checkbox"/> 0/5	Disable	15	1
<input type="checkbox"/> 0/6	Disable	15	1
<input type="checkbox"/> 0/7	Disable	15	1
<input type="checkbox"/> 0/8	Disable	15	1
<input type="checkbox"/> 0/9	Disable	15	1
<input type="checkbox"/> 0/10	Disable	15	1
<input type="checkbox"/> 0/11	Disable	15	1
<input type="checkbox"/> 0/12	Disable	15	1

1. **Interface** - Selects the physical interface for which data is to be configured.
2. Use **Trust Mode** 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**.

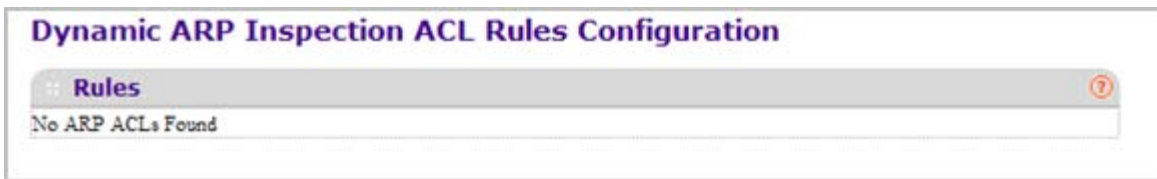


1. Use **Name** to create New ARP ACL for DAI.
2. Click **ADD** to add a new DAI ACL to the switch configuration.
3. Click **DELETE** to remove the currently selected DAI ACL from the switch configuration.

### 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.

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**.

**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

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.

## 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:

### ACL Wizard

the ACL Wizard helps a user to create a simple ACL and apply to the selected ports easily and quickly. Firstly you must select an ACL type with which you will create a ACL. Then add ACL rule to this ACL and at last apply this ACL on the selected ports. The ACL Wizard allows you only to create the ACL but doesn't allow you to modify it. If you want to modify it, please go to the ACL configuration page to do that.

To display the ACL Wizard, click **Security > ACL > ACL Wizard**.

**ACL Wizard**

**ACL Type Selection**

ACL Type:

**ACL Based on Destination MAC**

	Rule ID	Action	Match Every	Destination MAC	Destination MAC Mask	VLAN
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**Binding Configuration**

Direction:

**Port Selection Table**

<input type="checkbox"/>	Unit 1
<input type="checkbox"/>	LAG

1. Use **ACL Type** to specifies the ACL type you are using to create the ACL. You can select one type from 10 optional types:



- **ACL Based on Destination MAC** - To create a ACL based on the destination MAC address, destination MAC mask and VLAN.
  - **ACL Based on Source MAC** - To create a ACL based on the source MAC address, source MAC mask and VLAN.
  - **ACL Based on Destination IPv4** - To create a ACL based on the destination IPv4 address and IPv4 address mask.
  - **ACL Based on Source IPv4** - To create a ACL based on the source IPv4 address and IPv4 address mask.
  - **ACL Based on Destination IPv6** - To create a ACL based on the destination IPv6 prefix and IPv6 prefix length.
  - **ACL Based on Source IPv6** - To create a ACL based on the source IPv6 prefix and IPv6 prefix length.
  - **ACL Based on Destination IPv4 L4 Port** - To create a ACL based on the destination IPv4 layer4 port number.
  - **ACL Based on Source IPv4 L4 Port** - To create a ACL based on the source IPv4 layer4 port number.
  - **ACL Based on Destination IPv6 L4 Port** - To create a ACL based on the destination IPv6 layer4 port number.
  - **ACL Based on Source IPv6 L4 Port** - To create a ACL based on the source IPv6 layer4 port number.
2. Use **Rule ID** to enter a whole number in the range of 1 to 1023 that will be used to identify the rule.
  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 **Destination MAC** to specify 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.
  5. Use **Destination MAC Mask** to specify 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.
  6. Click **ADD** to add a new rule to the ACL based on destination MAC.
  7. Click **DELETE** to remove the currently selected Rule from the ACL based on destination MAC.
  8. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
  9. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

## Basic

The Basic folder contains links to the following features:

- [MAC ACL](#) on page 290

- [MAC Rules](#) on page 291
- [MAC Binding Configuration](#) on page 292
- [MAC Binding Table](#) on page 293

## 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 a 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**.

MAC ACL			
:: MAC ACL			
Current Number of ACL	<input type="text" value="0"/>		
Maximum ACL	<input type="text" value="100"/>		
MAC ACL Table			
<input type="checkbox"/>	Name	Rules	Direction
<input type="text"/>			

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**.



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 “MAC Binding Table” on page 6-293.
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**.

The screenshot shows the 'MAC Binding Configuration' page. It includes a 'Binding Configuration' section with the following fields:

- ACL ID**: A dropdown menu.
- Direction**: A dropdown menu set to 'Inbound'.
- Sequence Number**: A text input field containing '0', with a range indicator '(1 to 4294967295)'.

Below the configuration fields is a 'Port Selection Table' with two rows:

Port Selection Table
Unit 1
LAG

At the bottom of the page is an 'Interface Binding Status' table with the following columns:

Interface	Direction	ACL Type	ACL ID	Sequence Number
-----------	-----------	----------	--------	-----------------

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**.

Field	Description
Interface	Displays the interface of the ACL assigned.
Direction	Displays selected packet filtering direction for ACL.

Field	Description
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 295
- [IP Rules](#) on page 296
- [IP Extended Rules](#) on page 298
- [IPv6 ACL](#) on page 300
- [IPv6 Rules](#) on page 301
- [IP Binding Configuration](#) on page 303
- [IP Binding Table](#) on page 304
- [IP Binding Table](#) on page 304

## 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**.

IP ACL			
:: IP Configuration			
Current Number of ACL	<input type="text" value="5"/>		
Maximum ACL	<input type="text" value="100"/>		
:: IP ACL Table			
	IP ACL	Rules	Type
<input type="checkbox"/>	<input type="text"/>		
<input type="checkbox"/>	2	2	Basic IP ACL
<input type="checkbox"/>	102	1	Extended IP ACL
<input type="checkbox"/>	IP ACL 3	1	Named 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:

- 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.
- To delete an IP ACL, select the check box next to the IP ACL ID field, then click **DELETE**.

- 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**.

IP Rules									
ACL ID/NAME: 2									
Basic ACL Rule Table									
	Rule ID	Action	Logging	Assign Queue Id	Match Every	Mirror Interface	Redirect Interface	Source IP Address	Source IP Mask
<input type="checkbox"/>	10	Permit	Disable	0	False				
<input type="checkbox"/>	1022	Permit	Disable	0	False				

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**.

Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Keyword	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port	Service Type
1020	Permit	Disable	0			False									

To configure rules for an IP ACL:

- 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.
- 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**.

### IPv6 ACL

**IPv6 Configuration**

Current Number of ACL

Maximum ACL

**IPv6 ACL Table**

	IPv6 ACL	Rules	Type
<input type="checkbox"/>	<input style="width: 80%;" type="text"/>		IPv6 ACL
<input type="checkbox"/>	<a href="#">ipv6_acl 5</a>	1	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.

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 be 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 selecting one of the DSCP keywords 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**.

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.

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 **IP ACL Binding Table**.

To delete an IP ACL-to-interface binding, select the check box next to the interface and click **DELETE**.

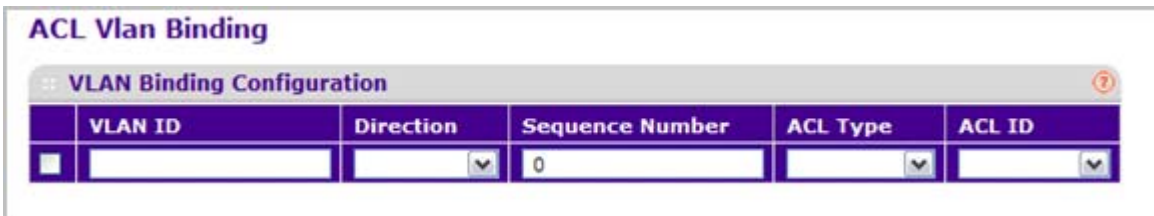


Field	Description
Interface	Displays selected interface.
Direction	Displays selected packet filtering direction for ACL.
ACL Type	Displays the type of ACL assigned to selected interface and direction.
ACL ID/Name	Displays the ACL Number (in the case of IP ACL) or ACL Name (in the case of Named IP ACL 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.

### VLAN Binding Table

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

To display the VLAN Binding Table, click **Security > ACL > Advanced > VLAN Binding Table**.



The following table describes the information displayed in the **ACL VLAN Binding Table**.

To delete a VLAN ACL-to-interface binding, select the check box next to the interface and click **DELETE**.

1. Use **Direction** to specify the packet filtering direction for ACL. Valid directions are Inbound and Outbound.
2. Use **ACL Type** to specify the type of ACL. Valid ACL Types include IP ACL, MAC ACL, and IPv6 ACL.
3. Use **ACL ID** to display all the ACLs configured, depending on the ACL Type selected.

## Web Management User Guide

Field	Description
VLAN ID	Specifies VLAN ID for ACL mapping.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this VLAN and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this VLAN and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user (i.e. the value is 0), a sequence number that is one greater than the highest sequence number currently in use for this VLAN and direction will be used. Valid range is (1 to 4294967295).



# 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 308
- [Logs](#) on page 321
- [Port Mirroring](#) on page 330
- [sFlow](#) on page 332

## 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 309
- [Port Detailed Statistics](#) on page 311
- [EAP Statistics](#) on page 317
- [Cable Test](#) on page 320

## 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**.

The screenshot shows the 'Port Statistics' page with a table of interface statistics. The table has columns for Interface, Total Packets received without Errors, Packets received with Errors, Broadcast Packets received, Packets transmitted without Errors, Transmit Packet Errors, Collision Frames, and Time since counters last cleared. The first row (0/1) shows 36116 total packets received without errors and 706 broadcast packets received. All other interfaces (0/2 to 0/12) show 0 for all error and collision metrics. The 'Time since counters last cleared' for all interfaces is '0 day 4 hr 54 min 33 sec'. There are 'LAGS All' and 'Go To Interface' buttons at the top and bottom of the table.

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"/> 0/1	36116	0	706	21573	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/2	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/3	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/4	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/5	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/6	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/7	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/8	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/9	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/10	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/11	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec
<input type="checkbox"/> 0/12	0	0	0	0	0	0	0 day 4 hr 54 min 33 sec

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.

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.

## Web Management User Guide

Field	Description
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 figure show some, but not all, of the fields on the Port Detailed Statistics page.)

The screenshot shows a web interface titled "Port Detailed Statistics". At the top, there is a header bar with the title and a help icon. Below the header, there are two dropdown menus: "Interface" set to "0/1" and "MST ID" set to "CST". The main content area is a list of configuration parameters and their values, followed by a list of traffic statistics, all with a value of 0.

Parameter	Value
Interface	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

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.

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.
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.



## Web Management User Guide

Field	Description
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1519-2047 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).
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).

## Web Management User Guide

Field	Description
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).
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.

## Web Management User Guide

Field	Description
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.
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).

## Web Management User Guide

Field	Description
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.
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.

Field	Description
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**.

Ports	PAE Capabilities	EAPOL				EAP							
		Frames Received	Frames Transmitted	Start Frames Received	Logoff Frames Received	Last Frame Version	Last Frame Source	Invalid Frames Received	Length Error Frames Received	Response/ID Frames Received	Response Frames Received	Request/ID Frames Transmitted	Request Frames Transmitted
<input type="checkbox"/> 0/1	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/2	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/3	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/4	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/5	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/6	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/7	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/8	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/9	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/10	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/11	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0
<input type="checkbox"/> 0/12	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0

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.

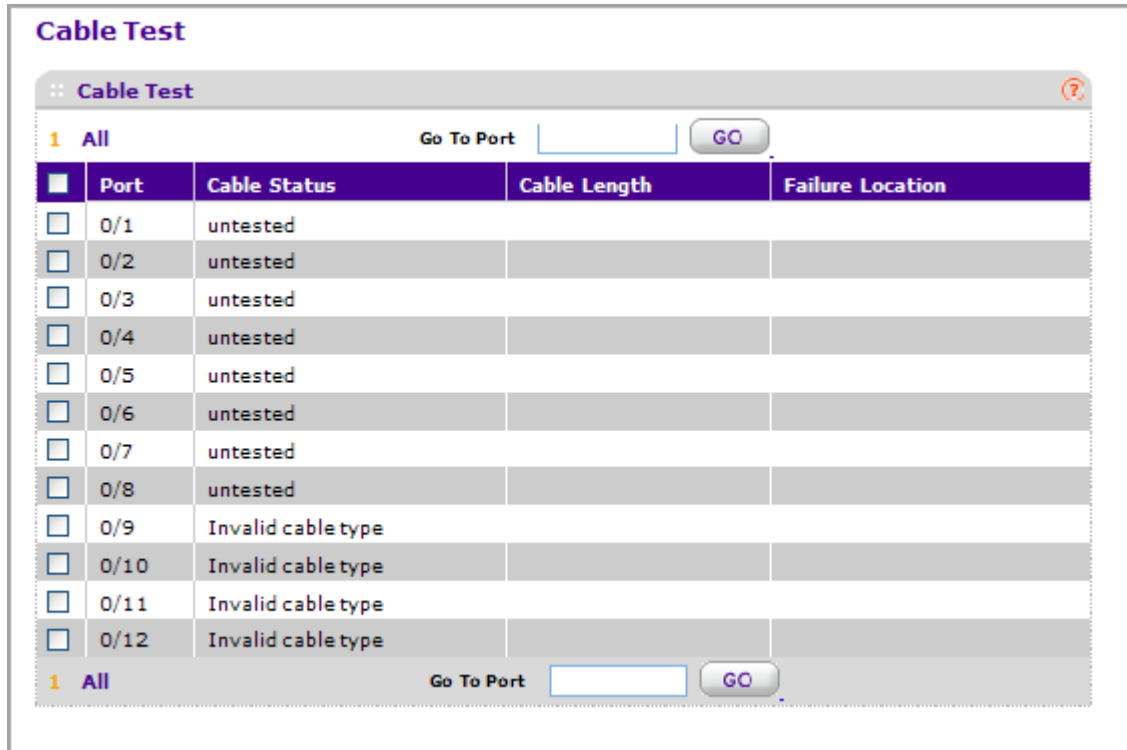
Field	Description
Port	Selects the port to be displayed. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port. All physical interfaces are valid.
PAE Capabilities	This displays the PAE capabilities of the selected port
EAPOL Frames Received	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.

## Web Management User Guide

Field	Description
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.

Field	Description
Cable Status	<p>This displays the cable status as Normal, Open or Short.</p> <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>



Field	Description
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 322
- [Command Log Configuration](#) on page 324
- [Console Log Configuration](#) on page 324
- [SysLog Configuration](#) on page 325
- [Trap Logs](#) on page 326
- [Event Logs](#) on page 328
- [Persistent Logs](#) on page 329

## Buffered Logs

To access the Buffered Logs page, click **Monitoring > Logs > Buffered Logs**.

**Buffered Logs**

Admin Status:  Disable  Enable

Behavior:

**Message Log**

Total number of Messages: 1292

Description
<14> JAN 03 23:40:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(2026) 1882 %% AutoInstall : Waiting for retry timeout
<14> JAN 03 23:40:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(3523) 1881 %% DHCP option resolved : TFTP IP address 10.9.11.20
<14> JAN 03 23:30:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(2026) 1752 %% AutoInstall : Waiting for retry timeout
<14> JAN 03 23:30:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(3523) 1751 %% DHCP option resolved : TFTP IP address 10.9.11.20
<14> JAN 03 23:20:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(2026) 1750 %% AutoInstall : Waiting for retry timeout
<14> JAN 03 23:20:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(3523) 1749 %% DHCP option resolved : TFTP IP address 10.9.11.20
<13> JAN 03 23:20:01 10.27.34.52-1 TRAPMGR[-1948147584]: traputil.c(614) 1748 %% Spanning Tree Topology Change: 0, Unit: 1
<13> JAN 03 23:20:01 10.27.34.52-1 TRAPMGR[-1948147584]: traputil.c(614) 1747 %% Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
<13> JAN 03 23:20:00 10.27.34.52-1 TRAPMGR[-1948147584]: traputil.c(614) 1746 %% Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
<13> JAN 03 23:19:59 10.27.34.52-1 TRAPMGR[-1948147584]: traputil.c(614) 1745 %% Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
<13> JAN 03 23:19:58 10.27.34.52-1 TRAPMGR[-1948147584]: traputil.c(614) 1744 %% Spanning Tree Topology Change: 0, Unit: 1
<13> JAN 03 23:19:58 10.27.34.52-1 TRAPMGR[-1948147584]: traputil.c(614) 1743 %% Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
<14> JAN 03 23:10:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(2026) 1742 %% AutoInstall : Waiting for retry timeout
<14> JAN 03 23:10:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(3523) 1741 %% DHCP option resolved : TFTP IP address 10.9.11.20
<14> JAN 03 23:00:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(2026) 1740 %% AutoInstall : Waiting for retry timeout
<14> JAN 03 23:00:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(3523) 1739 %% DHCP option resolved : TFTP IP address 10.9.11.20
<14> JAN 03 22:50:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(2026) 1738 %% AutoInstall : Waiting for retry timeout
<14> JAN 03 22:50:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(3523) 1737 %% DHCP option resolved : TFTP IP address 10.9.11.20
<14> JAN 03 22:40:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(2026) 1736 %% AutoInstall : Waiting for retry timeout
<14> JAN 03 22:40:43 10.27.34.52-1 AUTO_INST[-427012512]: auto_install_control.c(3523) 1735 %% DHCP option resolved : TFTP IP address 10.9.11.20
<13> JAN 03 22:36:00 10.27.34.52-1 TRAPMGR[-1948147584]: traputil.c(614) 1734 %% Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
<13> JAN 03 22:35:59 10.27.34.52-1 TRAPMGR[-1948147584]: traputil.c(614) 1733 %% Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22

### 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**.

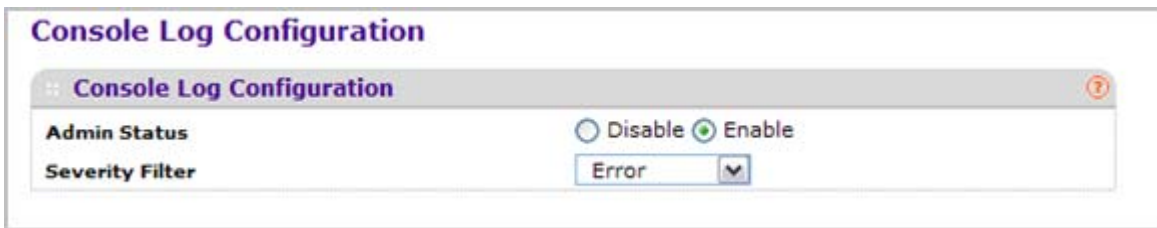


1. Use **Admin Mode** to enable/disable the operation of the CLI Command logging by selecting the corresponding radio button.

## 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**.

### Syslog Configuration

**Syslog Configuration** ?

**Admin Status**  Disable  Enable

**Local UDP Port**  (1 to 65535)

**Messages Received** 1752

**Messages Relayed** 0

**Messages Ignored** 0

**Host Configuration** ?

	Host Address	Status	Port	Severity Filter
<input type="checkbox"/>	<input type="text"/>		<input type="text"/>	<input type="text" value=""/>



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.

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**.

Trap Logs		
:: Trap Logs 		
<b>Number of Traps Since Last Reset</b>	376	
<b>Trap Log Capacity</b>	256	
<b>Number of Traps Since Log Last Viewed</b>	376	
:: Trap Logs 		
Log	System Up Time	Trap
0	2 days 23:19:51	Spanning Tree Topology Change: 0, Unit: 1
1	2 days 23:19:51	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
2	2 days 23:19:50	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
3	2 days 23:19:49	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
4	2 days 23:19:48	Spanning Tree Topology Change: 0, Unit: 1
5	2 days 23:19:48	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
6	2 days 22:35:50	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
7	2 days 22:35:49	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
8	2 days 22:35:48	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
9	2 days 22:35:47	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
10	2 days 22:35:47	Spanning Tree Topology Change: 0, Unit: 1
11	2 days 22:35:47	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
12	2 days 19:15:17	Spanning Tree Topology Change: 0, Unit: 1
13	2 days 19:15:17	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
14	2 days 19:15:16	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
15	2 days 19:15:15	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
16	2 days 19:15:14	Spanning Tree Topology Change: 0, Unit: 1
17	2 days 19:15:14	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
18	2 days 19:10:49	Spanning Tree Topology Change: 0, Unit: 1
19	2 days 19:10:49	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
20	2 days 19:10:48	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
21	2 days 19:10:47	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22

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.

## Web Management User Guide

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**.

Event Logs						
Entry	Type	Filename	Line	TaskID	Code	Time
1	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
2	EVENT>	unitmgr.c	5806	0	00000000	0 0 3 27
3	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
4	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
5	EVENT>	unitmgr.c	5806	0	00000000	0 0 31 42
6	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
7	EVENT>	unitmgr.c	5806	0	00000000	0 0 13 34
8	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
9	EVENT>	unitmgr.c	5806	0	00000000	0 0 2 4
10	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
11	EVENT>	unitmgr.c	5806	0	00000000	0 0 2 39
12	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
13	EVENT>	unitmgr.c	5806	0	00000000	0 0 5 36
14	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
15	EVENT>	unitmgr.c	5806	0	00000000	0 0 6 0
16	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
17	EVENT>	unitmgr.c	5806	0	00000000	0 0 2 47
18	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
19	EVENT>	unitmgr.c	5806	0	00000000	0 1 48 17
20	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
21	EVENT>	unitmgr.c	5806	0	00000000	0 0 12 10
22	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
23	EVENT>	unitmgr.c	5806	0	00000000	0 0 0 45
24	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
25	EVENT>	unitmgr.c	5806	0	00000000	0 0 1 48
26	EVENT>	bootos.c	220	0	AAAAAAAA	0 0 0 31
27	EVENT>	unitmgr.c	5806	0	00000000	0 0 3 40

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.

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**.

**Multiple Port Mirroring**

Status Table

1 LAGS All Go To Interface  GO

	Source Port	Destination Port	Session Mode	Direction	Mirroring Port
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Disable"/>	<input type="text" value=""/>	
<input type="checkbox"/>	0/1		Disable		
<input type="checkbox"/>	0/2		Disable		
<input type="checkbox"/>	0/3		Disable		
<input type="checkbox"/>	0/4		Disable		
<input type="checkbox"/>	0/5		Disable		
<input type="checkbox"/>	0/6		Disable		
<input type="checkbox"/>	0/7		Disable		
<input type="checkbox"/>	0/8		Disable		
<input type="checkbox"/>	0/9		Disable		
<input type="checkbox"/>	0/10		Disable		
<input type="checkbox"/>	0/11		Disable		
<input type="checkbox"/>	0/12		Disable		

1 LAGS All Go To Interface  GO

To configure Port Mirroring:

- 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.
- 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.
- 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.
- 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.
- Direction** - Specifies the direction of the Traffic to be mirrored from the configured mirrored port(s). Default value is Tx and Rx.
- 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.

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 332
- [Advanced](#) on page 333

### Basic

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

- [sFlow Agent](#) on page 332

### sFlow Agent

To display the sFlow Agent page, click **Monitoring** > **sFlow** > **Basic** > **sFlow Agent**.



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 333
- [sFlow Receiver Configuration](#) on page 333
- [sFlow Interface Configuration](#) on page 334

### sFlow Agent

To display the sFlow Agent page, click **Monitoring > sFlow > Advanced > sFlow Agent**.



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
<input type="checkbox"/> 1		0	1400	0.0.0.0	6343	5
<input type="checkbox"/> 2		0	1400	0.0.0.0	6343	5
<input type="checkbox"/> 3		0	1400	0.0.0.0	6343	5
<input type="checkbox"/> 4		0	1400	0.0.0.0	6343	5
<input type="checkbox"/> 5		0	1400	0.0.0.0	6343	5
<input type="checkbox"/> 6		0	1400	0.0.0.0	6343	5
<input type="checkbox"/> 7		0	1400	0.0.0.0	6343	5
<input type="checkbox"/> 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.

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**.

	Interface	Poller		Sampler		
		Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size
<input type="checkbox"/>	c/1	0	0	0	0	128
<input type="checkbox"/>	c/2	0	0	0	0	128
<input type="checkbox"/>	c/3	0	0	0	0	128
<input type="checkbox"/>	c/4	0	0	0	0	128
<input type="checkbox"/>	c/5	0	0	0	0	128
<input type="checkbox"/>	c/6	0	0	0	0	128
<input type="checkbox"/>	c/7	0	0	0	0	128
<input type="checkbox"/>	c/8	0	0	0	0	128
<input type="checkbox"/>	c/9	0	0	0	0	128
<input type="checkbox"/>	c/10	0	0	0	0	128
<input type="checkbox"/>	c/11	0	0	0	0	128
<input type="checkbox"/>	c/12	0	0	0	0	128

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 336
- [Reset](#) on page 337
- [Upload File From Switch](#) on page 339
- [Download File To Switch](#) on page 342
- [File Management](#) on page 347
- [Troubleshooting](#) on page 349

## Save Configuration


The **Save Configuration** menu contains links to the following options:

- [Save Configuration](#) on page 336
- [Auto Install Configuration](#) on page 337

## Save Configuration

To access the Save Configuration page, click **Maintenance > Save Config> Save Configuration**.

### Save Configuration

**Save Configuration** 

Saving all applied changes will cause all changes to configuration panels that were applied, but not saved, to be saved, thus retaining their new values across a system reboot.



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**.



The screenshot shows the 'Auto Install Configuration' page. It features a title bar with the text 'Auto Install Configuration' and a help icon. Below the title bar, there are five configuration items, each with a label and a control element:

AutoInstall Mode	Stop
AutoInstall Persistent Mode	Enabled
AutoSave Mode	Disabled
AutoInstall Retry Count	3 (1 to 3)
AutoInstall State	Waiting for restart timeout

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 338
- [Factory Default](#) on page 338
- [Password Reset](#) on page 339

## 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 11.

---

To access the Factory Defaults page, click **Maintenance** > **Reset** > **Factory Default**.

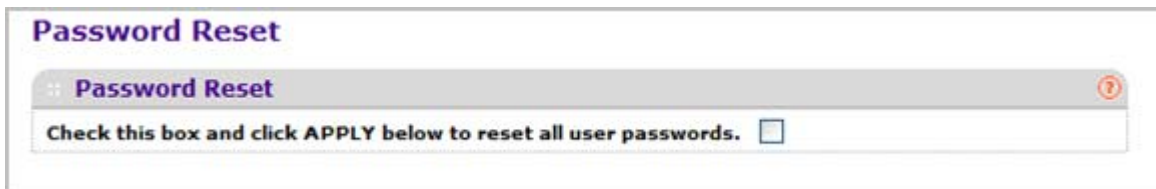
To reset the switch to the factory default settings:

1. Select the check box 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 340
- [HTTP File Upload](#) on page 341
- [USB File Upload](#) on page 342

## File Upload

To display the File Upload page, click **Maintenance > Upload > File Upload**.

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 HTTP File Upload page, click **Maintenance > Upload > USB 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.
  - **Text Configuration** to specify configuration in text mode when you want to retrieve the stored configuration. The factory default is **Archive**.
2. Use **USB File** to give 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. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. Click **APPLY** to send the updated configuration to the switch. Configuration changes take effect immediately.

## 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 343
- [HTTP File Download](#) on page 344

## 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).

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.

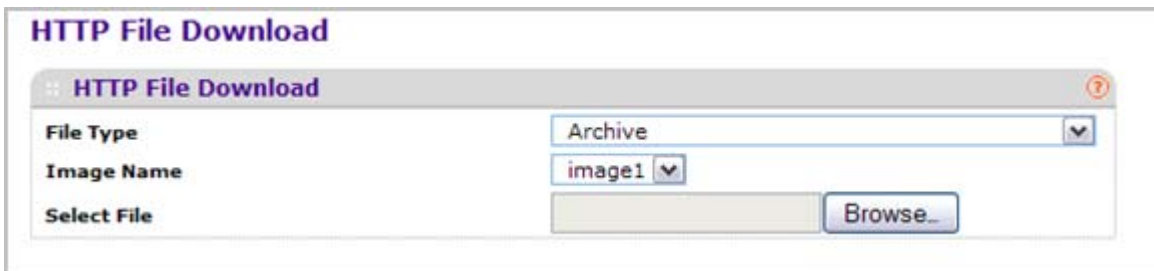
---

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**.



The screenshot shows a web interface titled "HTTP File Download". It contains a form with the following elements:

- File Type:** A dropdown menu currently showing "Archive".
- Image Name:** A dropdown menu currently showing "image1".
- Select File:** A text input field followed by a "Browse..." button.

A help icon (question mark) is located in the top right corner of the form area.



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)

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 from the switch to USB device.

To display the HTTP File Upload page, click **Maintenance > Download > USB File Upload**.

**Download File From USB**

:: **Download File From USB** ?

**File Type** Archive ▾

**Image Name** image1 ▾

**USB File**

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.
  - **Text Configuration** to specify configuration in text mode when you want to retrieve the stored configuration. The factory default is **Archive**.
2. Use **USB File** to give 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. Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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

## 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 347
- [Dual Image Configuration](#) on page 348

### Copy

To display the Copy page, click **Maintenance** > **File Management** > **Copy**.



Copy	
Source Image	<input checked="" type="radio"/> Image1 <input type="radio"/> Image2
Stack Member	1 ▼
Destination Image	<input checked="" type="radio"/> Image1 <input type="radio"/> Image2

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**.

Dual Image Configuration						
Unit	Image Name	Active Image	Next Active Image	Description	Version	Update Bootcode
<input type="checkbox"/>			<input type="checkbox"/>			True
<input type="checkbox"/>	1	image1	True	True	3.21.13.28	True
<input type="checkbox"/>	1	image2	False	False	9.0.0.10	True

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.

---

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 349
- [Ping IPv6](#) on page 350
- [Traceroute IPv4](#) on page 351
- [Traceroute IPv6](#) on page 352

### 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**.

**Ping Ipv4**

**Details** ⓘ

IP Address/Host Name

Count  (1 to 15)

Interval(secs)  (1 to 60)

Datagram Size  (0 to 65507)

Ping

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**.

The screenshot shows a web interface for configuring a ping to an IPv6 address. The title is "Ping IPv6". There is a "Ping" dropdown menu currently set to "Global". Below this is a text input field for "IPv6 Address/Host Name" with a placeholder "(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/)" and a note "Max 255 characters". The "Datagram Size" is set to "64" with a note "(48 to 2048)". At the bottom, there is a "Result" section with a scrollable area for displaying the output of the ping command.

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).

4. **Result** - Displays the result after the switch send a Ping IPv6 request to the specified IPv6 address.

## 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**.

TraceRoute Ipv4		
IP Address/Hostname	<input type="text"/>	(Max: 255 characters/x.x.x.x)
Probes Per Hop	<input type="text" value="3"/>	(1 to 10)
MaxTTL	<input type="text" value="30"/>	(1 to 255)
InitTTL	<input type="text" value="1"/>	(0 to 255)
MaxFail	<input type="text" value="5"/>	(0 to 255)
Interval(secs)	<input type="text" value="3"/>	(1 to 60)
Port	<input type="text" value="33434"/>	(1 to 65535)
Size	<input type="text" value="0"/>	(0 to 65507)

Results

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**.

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

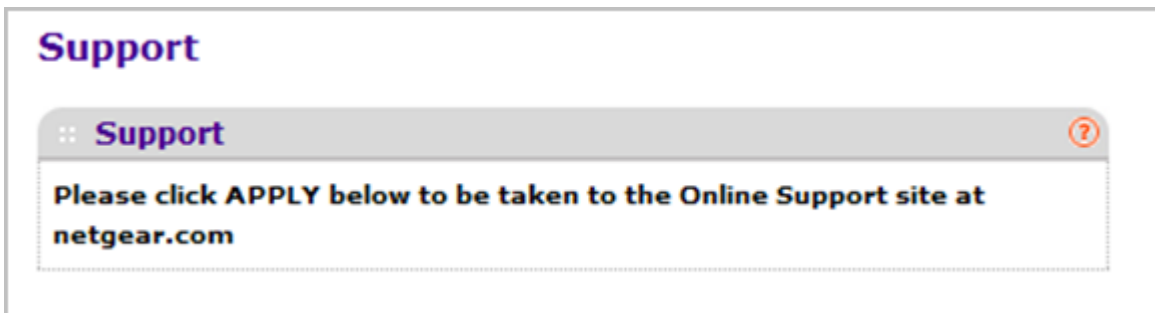
The Online Help includes the following pages:

- [Support](#) on page 354
- [User Guide](#) on page 355

## 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**.

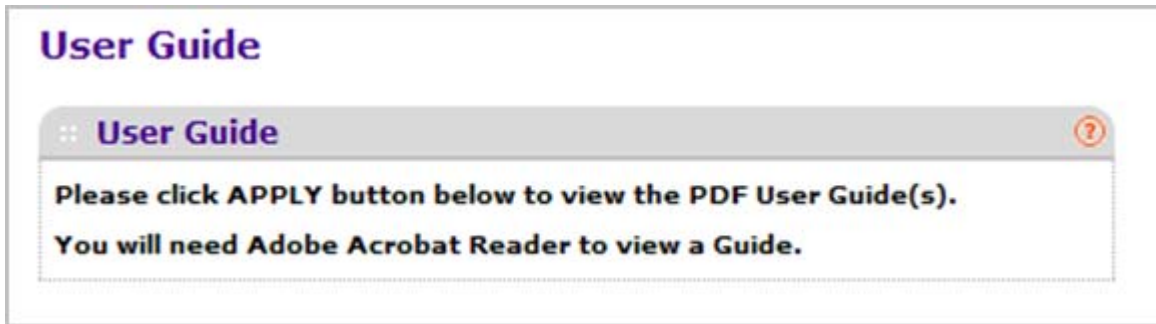


To connect to the NETGEAR support site for ProSafe® Managed Switches, click **APPLY**.

## 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 3. Default Settings**

<b>Feature</b>	<b>Default</b>
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	Eight characters
IPv6 management mode	Enabled
SNTP client	Enabled
SNTP server	Not configured
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
Auto Save	Disabled
sFlow	Enabled

**Table 3. Default Settings (Continued)**

<b>Feature</b>	<b>Default</b>
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
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
LLDP	Enabled
LLDP-MED	Disabled
MAC Table Address Aging	300 seconds (Dynamic Addresses)
DHCP Layer 2 Relay	Disabled

**Table 3. Default Settings (Continued)**

<b>Feature</b>	<b>Default</b>
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
IP Helper and UDP Relay	Enabled
Tunnel and Loopback Interfaces	None
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





# Configuration Examples

---

# B

This appendix contains information about how to configure the following features:

- *Virtual Local Area Networks (VLANs)* on page 361
- *Access Control Lists (ACLs)* on page 363
- *Differentiated Services (DiffServ)* on page 366
- *802.1X* on page 370
- *MSTP* on page 372

## 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 3-103.
- 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 137), 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 137) 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 3-103), 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 534).

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 536.

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 538).

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 540).

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 541).
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 543.

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 552).

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 554).

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.

NETGEAR® 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 425.

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 425.

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 429.

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 429.

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 433).

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 NETGEAR® 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:

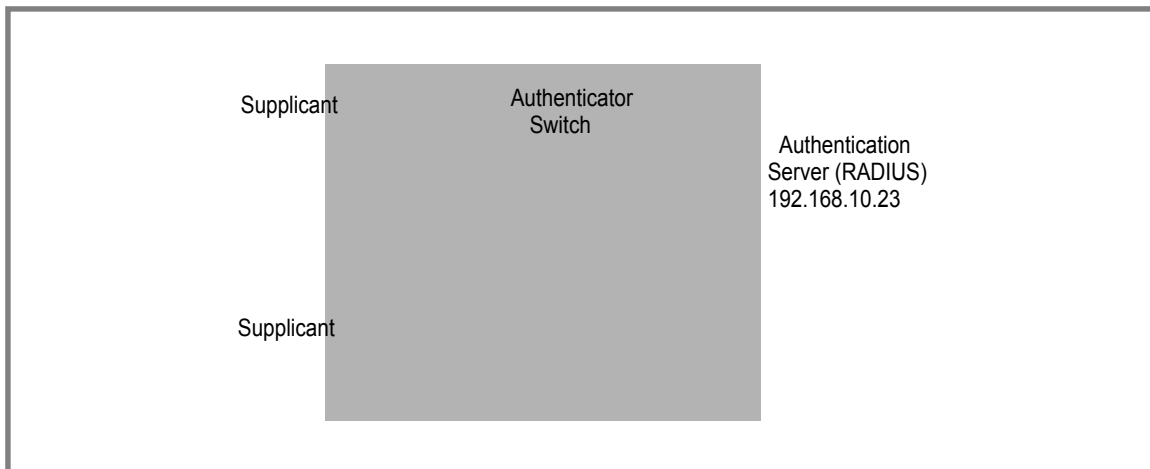
1. **Authenticator:** A Port that enforces authentication before allowing access to services available via that Port.
2. **Supplicant:** A Port that attempts to access services offered by the Authenticator.

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.

NETGEAR® 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 6-496 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 266).

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 443.

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 453).

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.

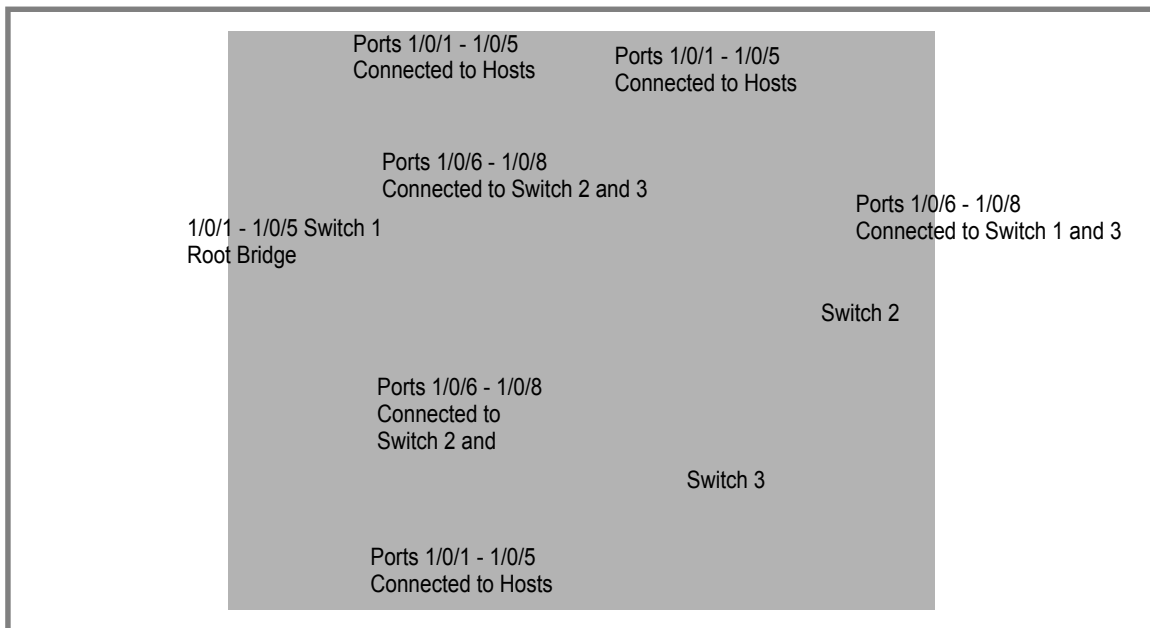
With this allocation we ensure that every VLAN is assigned to one and only one MSTI. The CIST is also an instance of spanning tree with a MSTID of 0.

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 137).
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 137).
3. From the STP Configuration screen, enable the Spanning Tree State option (see [STP Configuration](#) on page 158).

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 162).

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 164).
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 168.

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.





# Notification of Compliance



## NETGEAR Managed Stackable Switch

### Regulatory Compliance Information

Note: 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.

Note: 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.

### Europe – EU Declaration of Conformity



Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328 (2.4GHz), EN301 489-17, EN301 893 (5GHz), EN60950-1

For complete DoC, visit the NETGEAR EU Declarations of Conformity website at:  
[http://support.netgear.com/app/answers/detail/a\\_id/11621/](http://support.netgear.com/app/answers/detail/a_id/11621/)

### EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	<i>NETGEAR Inc.</i> tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede <i>NETGEAR Inc.</i> erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklart <i>NETGEAR Inc.</i> , dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab <i>NETGEAR Inc.</i> seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

## Web Management User Guide

English	Hereby, <i>NETGEAR Inc.</i> , declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente <i>NETGEAR Inc.</i> declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>NETGEAR Inc.</i> ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente <i>NETGEAR Inc.</i> déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente <i>NETGEAR Inc.</i> dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>NETGEAR Inc.</i> deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>NETGEAR Inc.</i> deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart <i>NETGEAR Inc.</i> dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, <i>NETGEAR Inc.</i> , jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, <i>NETGEAR Inc.</i> nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym <i>NETGEAR Inc.</i> oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	<i>NETGEAR Inc.</i> declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	<i>NETGEAR Inc.</i> izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>NETGEAR Inc.</i> týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	<i>NETGEAR Inc.</i> vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Svenska [Swedish]	Härmed intygar <i>NETGEAR Inc.</i> att denna Radiolan står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir <i>NETGEAR Inc.</i> yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	<i>NETGEAR Inc.</i> erklærer herved at utstyret <i>Radiolan</i> er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

## FCC Requirements for Operation in the United States

### FCC Information to User

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

### FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with 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 Web Management User Guide complies with Part 15 Subpart B of FCC CFR47 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.

### FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- 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.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

### Industry Canada

This device complies with RSS-210 of the Industry Canada 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.

### IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

### Caution:

The device for the band 5150-5250 MHz is only for indoor usage to reduce po-tential for harmful interference to co-channel mobile satellite systems.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

### NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

### Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utili-sation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

### Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

### GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to <ftp://downloads.netgear.com/files/GPLnotice.pdf>.

For GNU General Public License (GPL) related information, please visit [http://support.netgear.com/app/answers/detail/a\\_id/2649](http://support.netgear.com/app/answers/detail/a_id/2649).

### Interference Reduction Table

The table below shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

**Table 4.**

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

# Index

## Numerics

802.1X **228, 254, 255**  
example configuration **370**

## A

access control  
ACL example configuration **363**  
ACLs **288**  
authentication  
802.1X **253, 370**  
enable **14**  
port-based **253**  
RADIUS **228**  
SNMP **14**  
TACACS+ **234**

## C

certificate **245**  
compliance **378**  
Configuration  
802.1X **254, 255**  
Access Control Lists **288**  
Class **211, 214**  
Community **65**  
CoS **197**  
Differentiated Services **204**  
DNS **38**  
Dual Image **348**  
Dynamic Host **40**  
Global **130**  
IGMP Snooping **129**  
LAG **162**  
MAC Filter **264**  
Management Access **241**  
Policy **216**  
Port Security **266**  
Port VLAN ID **103**  
RADIUS  
Global **229**  
Secure HTTP **243**  
SNTP Server **35**  
Standard IP ACL Example **365**  
STP **112**  
TACACS+ **234**

Trap **66**  
VLAN **97**  
VLAN example **362**

CoS **197**

## D

defaults  
CoS **364**  
DES **14**  
Device View **12**  
DiffServ **204**  
DNS **38**  
download  
from a remote system **342**

## E

EAP **317**

## F

file management **347**  
firmware download **342**

## G

guest VLAN configuration **371**

## H

help, HTML-based **11**  
HTTP **241**  
management interface access **8**  
secure **241**  
using to download files **344**  
HTTPS **243**

## I

IEEE 802.11x **370**  
IEEE 802.1AB **71**  
IEEE 802.1D **112**  
IEEE 802.1Q **96, 112**

IEEE 802.1s **112**  
IEEE 802.1w **112**  
IEEE 802.1X **228**

IGMP **129**

interface

- LAG **161**
- logical **15**
- naming convention **14**
- physical **15**
- queue configuration **203**

IP DSCP **197**  
Mapping **201**

## L

LAG VLAN **161**  
LAGPDUs **161**  
LAGs **161**

- Membership **163**
- Static **161**

LLDP **71**  
LLDP-MED **71**

## M

MAC **129**

- filter summary **265**
- rules **291**

MD5 **31**  
MIBs **14**

## N

navigation **10**

## P

port

- authentication **253**
- summary **259**

## Q

QoS **196**

- 802.1p to Queue Mapping **200**

## R

RADIUS **224**

- server **228**

reboot **337**  
reset

- configuration to defaults **338**

switch **337**

RSTP **112**

## S

Simple Network Time Protocol **31**

SNMP

- traps **66**
- using **14**
- v1, v2 **64**

SNTP **31**

- server configuration **36**
- server status **37**

SSL **243**

storm control **273**

STP **112**

- example configuration **372**
- Status **113, 115**

Stratum

- 0 **31**
- 1 **31**
- 2 **31**

## T

T1 **31**  
T2 **31**  
T3 **31**  
T4 **31**  
TACACS+

- folder **234**
- settings **234**

technical support **2**  
time **31**

- levels **31**

trademarks **2**  
traffic control **262**  
trap

- flags **68**

## U

Unicast **31**  
upload configuration **339**

## V

VLAN **96**

- example configuration **361**
- guest **370**
- ID **96**
- managing **96**
- Port VLAN ID **103**



PVID **103**