NETGEAR®

M6100 Web Management User Guide

Software User Manual

September 2014
202-11439-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *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/general/contact/default.aspx*.

Contact your Internet service provider for technical support.

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.

See the regulatory compliance document before connecting the power supply.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11439-01	September 2014	First publication

Contents

Chapter 1 Getting Started

Chapter 2 Configuring System Information

Chapter 3 Configuring Switching Information

Chapter 4 Routing

Chapter 5 Configuring Quality of Service

Chapter 6 Managing Device Security

Chapter 7 Monitoring the System

Chapter 8 Maintenance

Chapter 9 Help

Getting Started

1

This chapter provides an overview of starting your NETGEAR M6100 Chassis switch and accessing the user interface. This chapter contains the following sections:

Switch Management Interface

The NETGEAR M6100 Chassis switch contains an embedded Web server and management software for managing and monitoring switch functions. M6100 Chassis switch functions as a simple switch without the management software. However, you can use the management software to configure more advanced features that can improve switch efficiency and overall network performance.

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

Web Access

To access the M6100 Chassis switch 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 M6100 Chassis switch 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 in *Figure 1* on page 10.

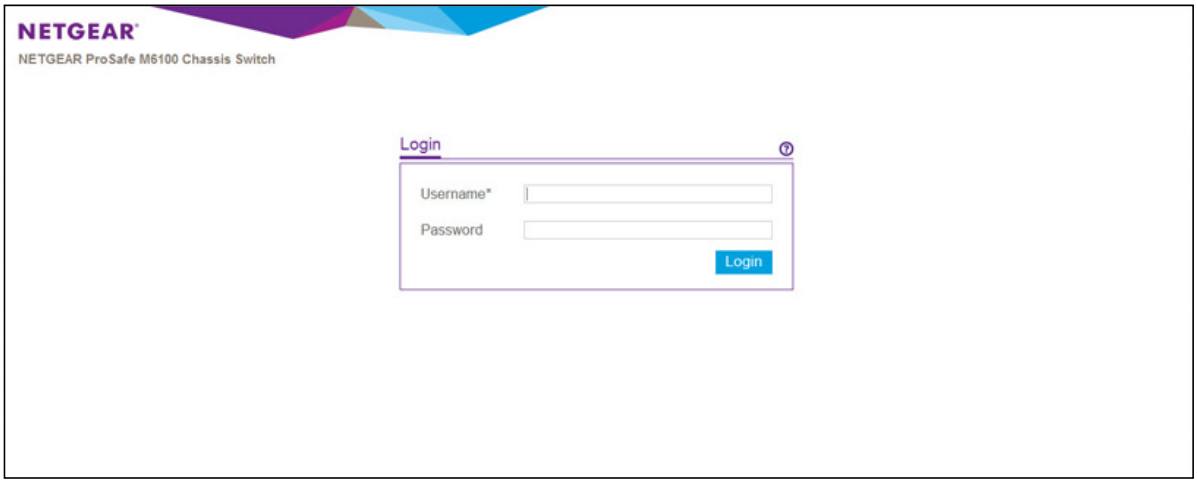


Figure 1. M6100 Web Interface

Understanding the User Interfaces

M6100 Chassis switch software includes a set of comprehensive management functions for configuring and monitoring the system by using one of the following methods:

- Web user interface
- Simple Network Management Protocol (SNMP)
- Command Line Interface (CLI)

Each of the standards-based management methods allows you to configure and monitor the components of the M6100 Chassis switch software. The method you use to manage the system depends on your network size and requirements, and on your preference.

The *Web Management User Guide* Software 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

Supported web browsers include:

- Internet Explorer 10.0, 11.0
- Mozilla Firefox 26
- Chrome 32

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.

Note: See *User Management* on page 396 for information about *admin* and *guest* user accounts.

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

Figure 2 below shows the layout of the Managed Switch Web interface.

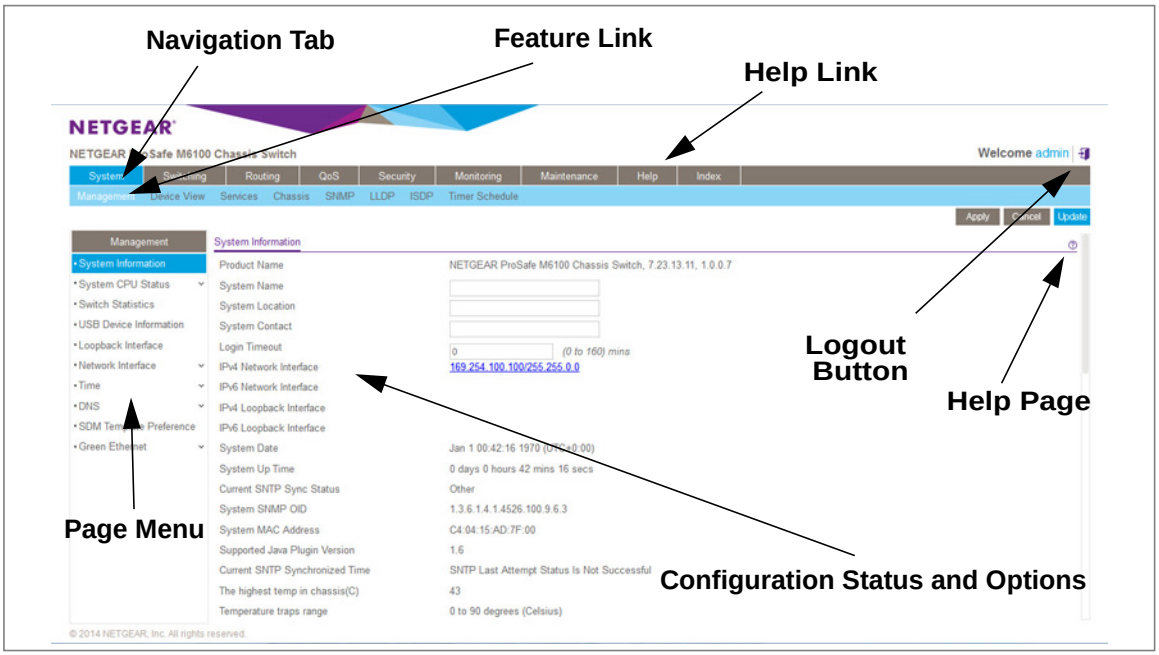


Figure 2. Layout of the Web Interface

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 *Figure 3, Submenu Links* on page 12 shows. When you click a menu item that includes

multiple configuration pages, the item becomes preceded by a down arrow symbol and expands to display the additional pages.

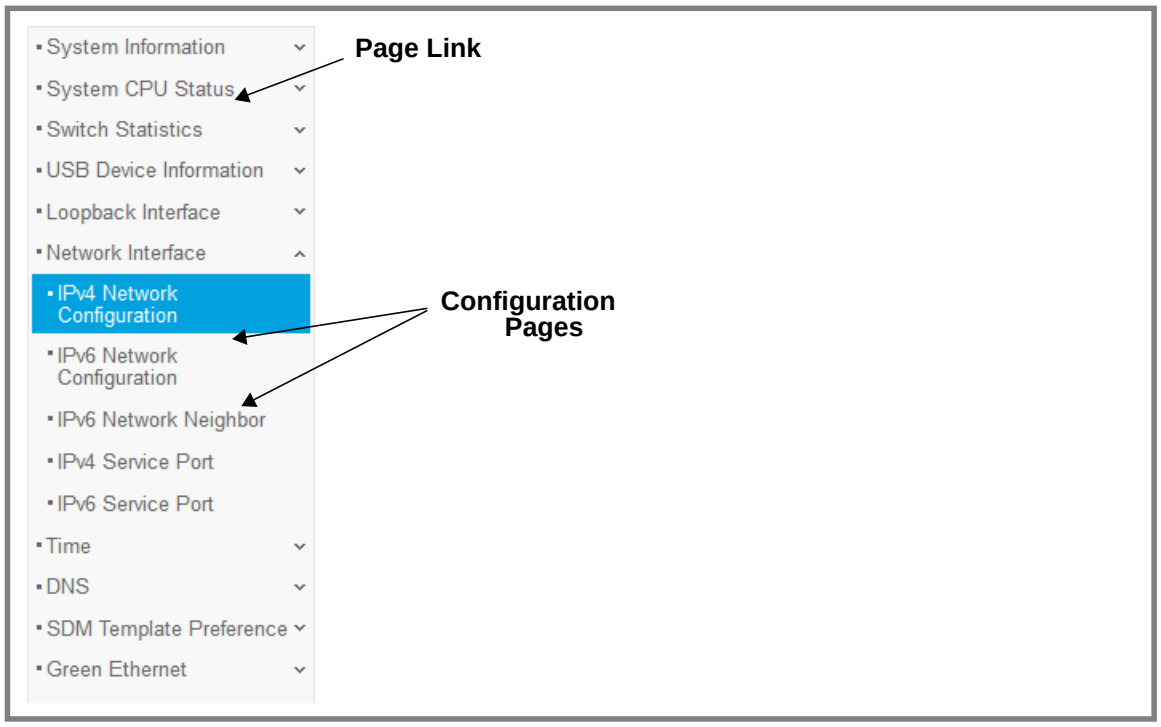


Figure 3. Submenu Links

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 menus.

Each page contains access to the HTML-based help that explains the fields and configuration options for the page. Each page, except the Index 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
Add	Clicking **Add** adds the new item configured in the heading row of a table.
Apply	Clicking the **Apply** button sends the updated configuration to the switch. Configuration changes take effect immediately.
Cancel	Clicking **Cancel** cancels the configuration on the screen and resets the data on the screen to the latest value of the switch.
Delete	Clicking **Delete** removes the selected item.

Table 1. Command Buttons

Button	Function
Update	Clicking the **Update** button updates the page with the latest information from the device.
Logout	Clicking the **Logout** button ends the session.

Device View

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

The Device View is available by selecting **System**> **Device View**.

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 that the link is disabled.
- Black indicates that no link is present.

The Device View of the switch is shown in *Figure 4* below.

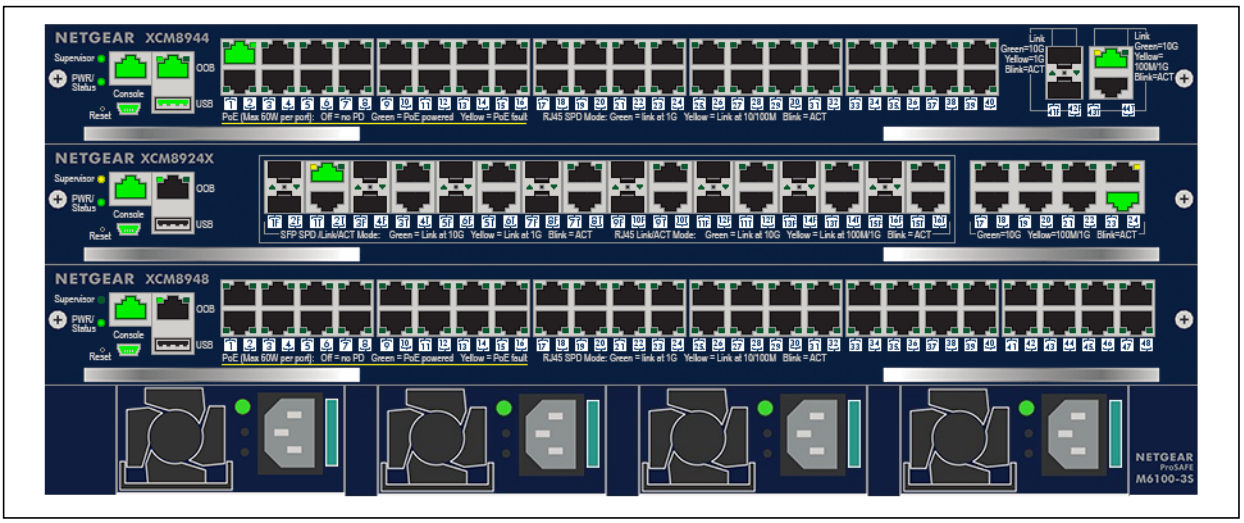


Figure 4. M6100 Device View

Click the port you want to view or configure to see a port menu that displays statistics and configuration options. Click the port 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, as shown in *Figure 5*. This menu contains the same option as the navigation tabs at the top of the page.

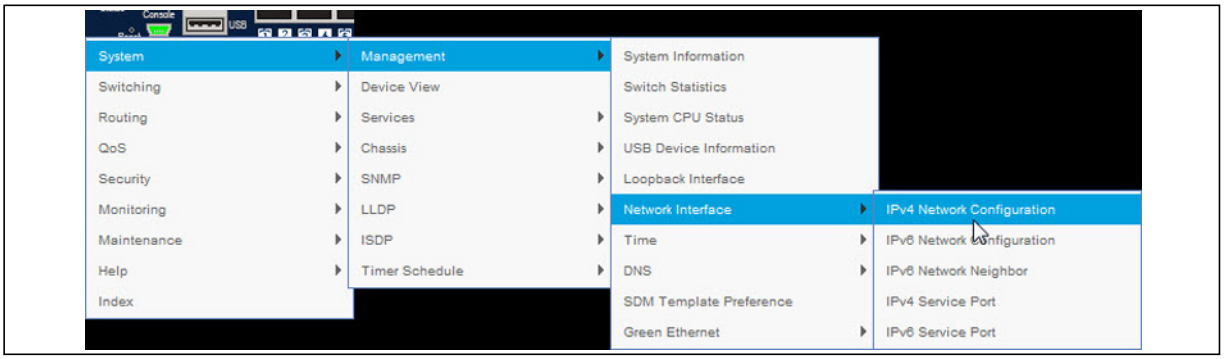


Figure 5. Device View Main Menu

Help Page Access

Every page contains a link to the online help , which contains information to assist in configuring and managing the switch. The online help pages are context sensitive. For example, if the IP Addressing page is open, the help topic for that page displays if you click Help.

User-Defined Fields

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

Table 2:

\	<
/	>
*	|
?	

Using SNMP

The M6100 Chassis switch software supports the configuration of SNMP groups and users that can manage traps that the SNMP agent generates.

M6100 Chassis switch uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. All private MIBs begin with a “-” prefix. The main object for interface configuration is in -SWITCHING-MIB, which is a private MIB. Some interface configurations also involve objects in the public MIB, IF-MIB.

SNMP is enabled by default. The **System** > **Management** > **System Information** Web page, which is the page that displays after a successful login, 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 SNMP V1 or SNMP V2, click **System** > **SNMP** > **SNMPv1/v2** and click the page that contains the information to configure.

Interface Naming Convention

The M6100 Chassis switch supports physical and logical interfaces. Interfaces are identified by their type and the interface number. The physical ports are gigabit interfaces and are numbered on the front panel. You configure the logical interfaces by using the software. *Table 3* describes the naming convention for all interfaces available on the switch.

Table 3. 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

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 55
- *Chassis* on page 79
- *PoE* on page 94
- *SNMP* on page 99
- *LLDP* on page 105
- *ISDP* on page 121
- *Timer Schedule* on page 126

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 17
- *Switch Statistics* on page 24
- *System CPU Status* on page 22
- *USB Device Information* on page 27
- *Loopback Interface* on page 29
- *Network Interface* on page 30
- *Time* on page 37
- *DNS* on page 43
- *SDM Template Preference* on page 45
- *Green Ethernet Configuration* on page 47

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.

Figure 6. System Information

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 255 alphanumeric characters. The factory default is blank.

d. **Login Timeout** - Specify how many minutes of inactivity should occur on a serial port connection before the switch closes the connection. Enter a number between 0 and 160: the factory default is 5. Entering 0 disables the timeout.

3. Click **Apply** to send the updated screen to the switch and cause the changes to take effect on the switch. These changes will not be retained across a power cycle unless a save is performed.

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

Table 4. System Information

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.
Current SNTP Sync Status	Displays the current SNTP sync status.
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.
Current SNTP Synchronized Time	Displays the SNTP Synchronized time.
The highest temp in chassis (C)	The general temperature of the switch in degrees Centigrade.
Temperature traps range	Identifies minimum and maximum of traps range.

Backplane Information

This screens displays the backplane information. The following table describes the information displayed.

Table 5. Backplane Information

Field	Description
Model Identifier	The model identifier
FPGA Version	The FPGA version
Serial Number	The serial number

Temperature Status

This screen shows the current temperature of the temperature sensors. The temperature is instant and can be updated with the latest information on the switch when the Update button is pressed. The maximum temperature of the temperature sensors depends on the actual hardware.

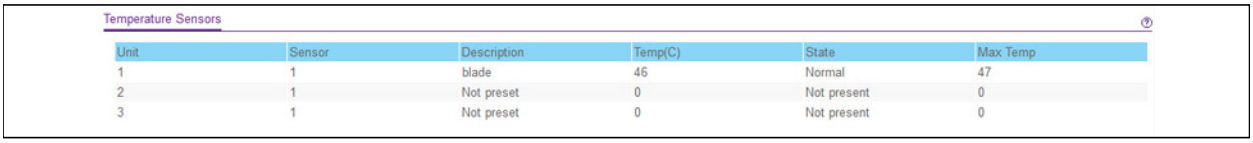


Figure 7. Temperature Status

The following table describes the non-configurable Temperature Status information.

Table 6. Temperature Status Information

Field	Description
Unit	The unit number in the chassis.
Sensor	The temperature sensor for the given unit.
Description	The description of the temperature sensor.
Temp (C)	The temperature of the specified unit in degrees Centigrade.
State	The unit temperature state.
Max Temp	The maximum temperature of CPU and MACs.

Click **Update** to update the page with the latest information on the switch.

FAN Status

This screen shows the status of the fans in all units. These fans remove the heat generated by the power, CPU and other chipsets, and allow the chipsets work normally. Fan status has three possible values: OK, Failure, and Not Present.

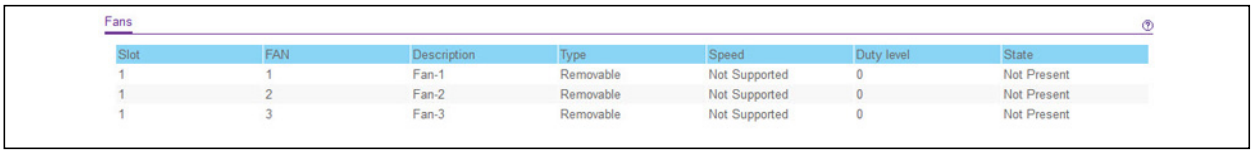


Figure 8. Fan Status

The following table describes the non-configurable Fan Status information.

Table 7. Fan Status

Field	Description
Slot	The slot number in the chassis.
Fan	The fan index used to identify the fan for the given chassis member.
Description	The description of the fan.
Type	Specifies whether the fan module is fixed or removable.
Speed	The fan speed.
Duty Level	The duty level of the fan.
State	Specifies whether the fan is running or stopped.

Click **Update** to update the page with the latest information on the switch.

Device Status

This screen shows the software version of each device.

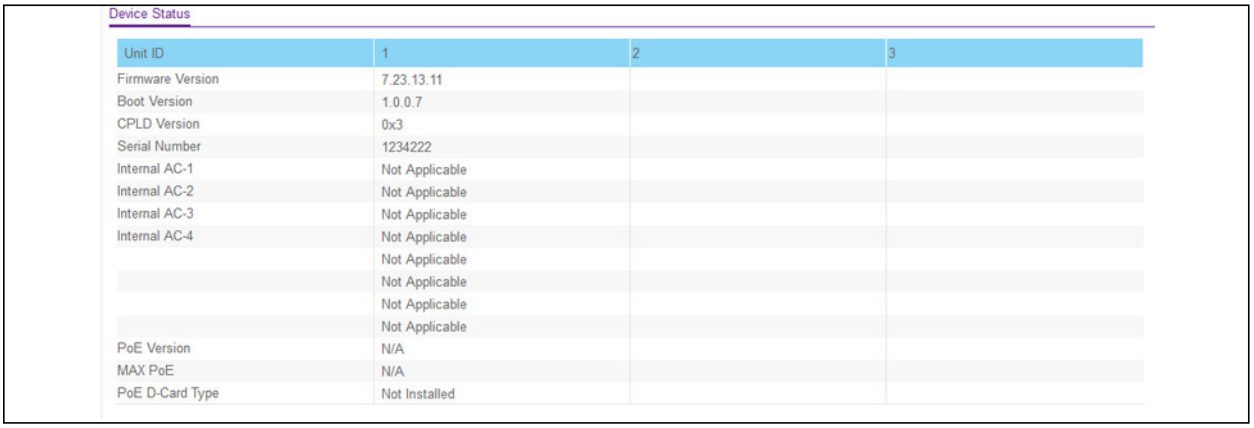


Figure 9. Device Status

The following table describes the non-configurable Device Status information.

Table 8. Device Status

Field	Description
Unit ID	The unit number in the chassis.
Firmware Version	The release.version.maintenance number of the code currently running on the switch. For example, if the release was 1, the version was 2 and the maintenance number was 4, the format would be '1.2.4'.
Boot Version	The version of the boot code which is in the flash memory to load the firmware into the memory.
CPLD Version	The version of the software for CPLD.
Serial Number	The serial number of this switch.

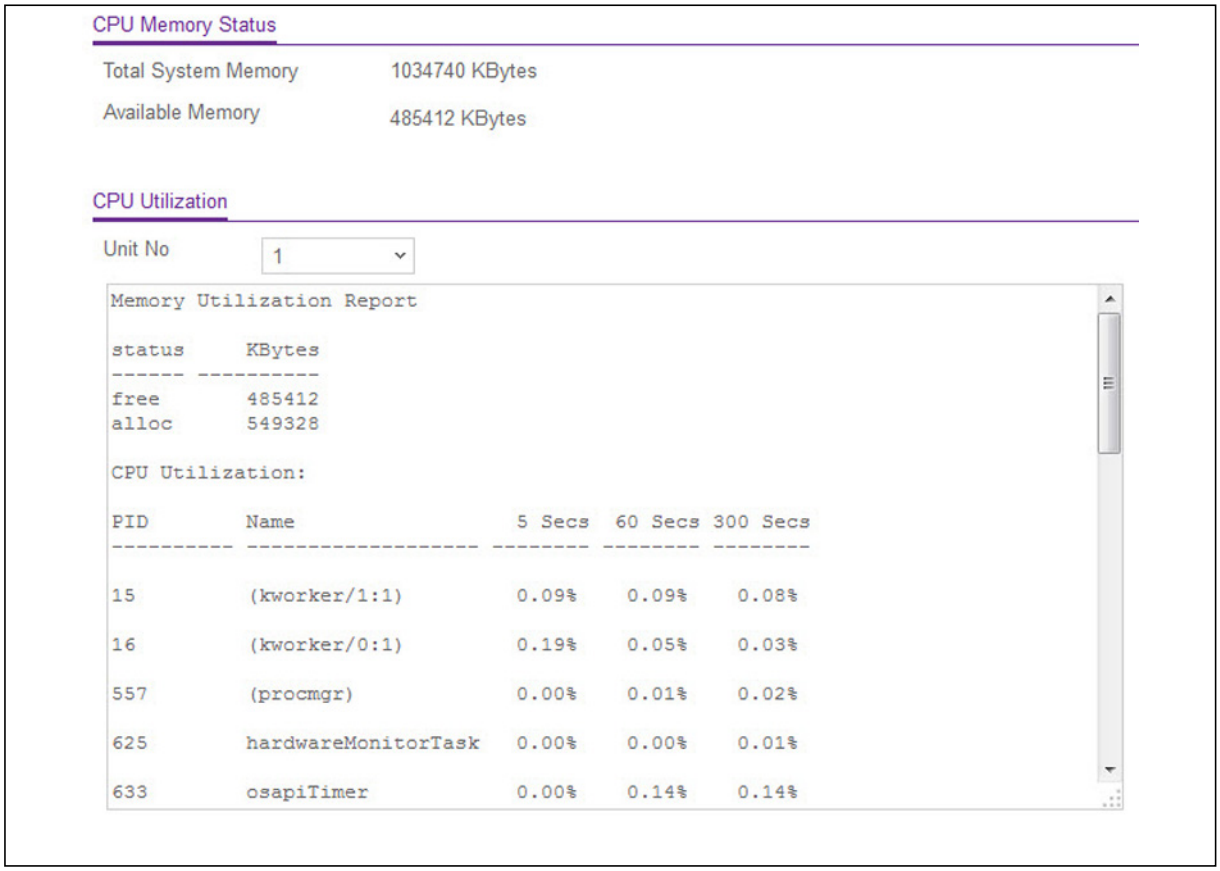
Field	Description
Internal AC-1, Internal AC-2, etc.	Indicates the status of the appropriate power module in each unit. Status can be any of the following: • Operational—Power module is present and functioning properly. • Powering—Main power is failed or disconnected but RPS provides power to the switch. • Not Present—Power module is not present in the slot. • Not powered—Power module is present but not connected to the power source. • Not powering—Power module is present and connected but the switch uses another power source. • Incompatible—Power module is present but incompatible. • Failed—Power module is present, but power cable is not plugged-in or a bad cable is plugged-in.
PoE Version	Version of the PoE controller FW image. N/A indicates that the Poe is not supported by the unit.
MAX PoE	Indicates the status of maximum PoE power available on the switch as follows: • ON—Indicates less than 10W of PoE power available for another device. • OFF—Indicates at least 10W of PoE power available for another device. • N/A—Indicates that PoE is not supported by the unit.
PoE D-Card Type	Indicates the type of the PoE daughter card plugged in. Possible values are: • XCM89P—PoE card supporting 802.3at standard (backward compatible with 802.3af). • XCM89UP—PoE card supporting UPOE pre-standard (backward compatible with 802.3af/802.3at). • Not Installed—PoE card is not plugged in.

Click **Update** to update the page with the latest information on the switch.

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 is displayed.



System CPU Status

The following table describes CPU Memory Status information.

Table 9. 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

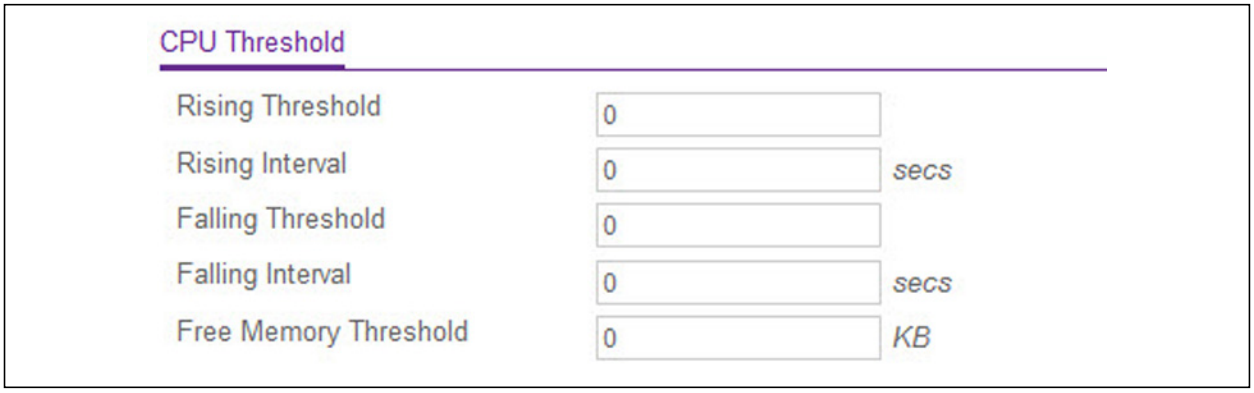
This page displays the CPU Utilization information, which contains the memory information, task-related information, and percentage of CPU utilization per task.

1. Select the Unit No. to display the CPU Utilization information.
2. Select All to display the CPU Utilization information for all units in a chassis.

CPU Threshold

The CPU Utilization Threshold notification feature allows you to configure thresholds that, when crossed, trigger a notification. The notification is done via SNMP trap and SYSLOG messages.

To display the CPU Threshold page, click **System** > **Management** > **System CPU Status** > **CPU Threshold**. A screen similar to the following is displayed.



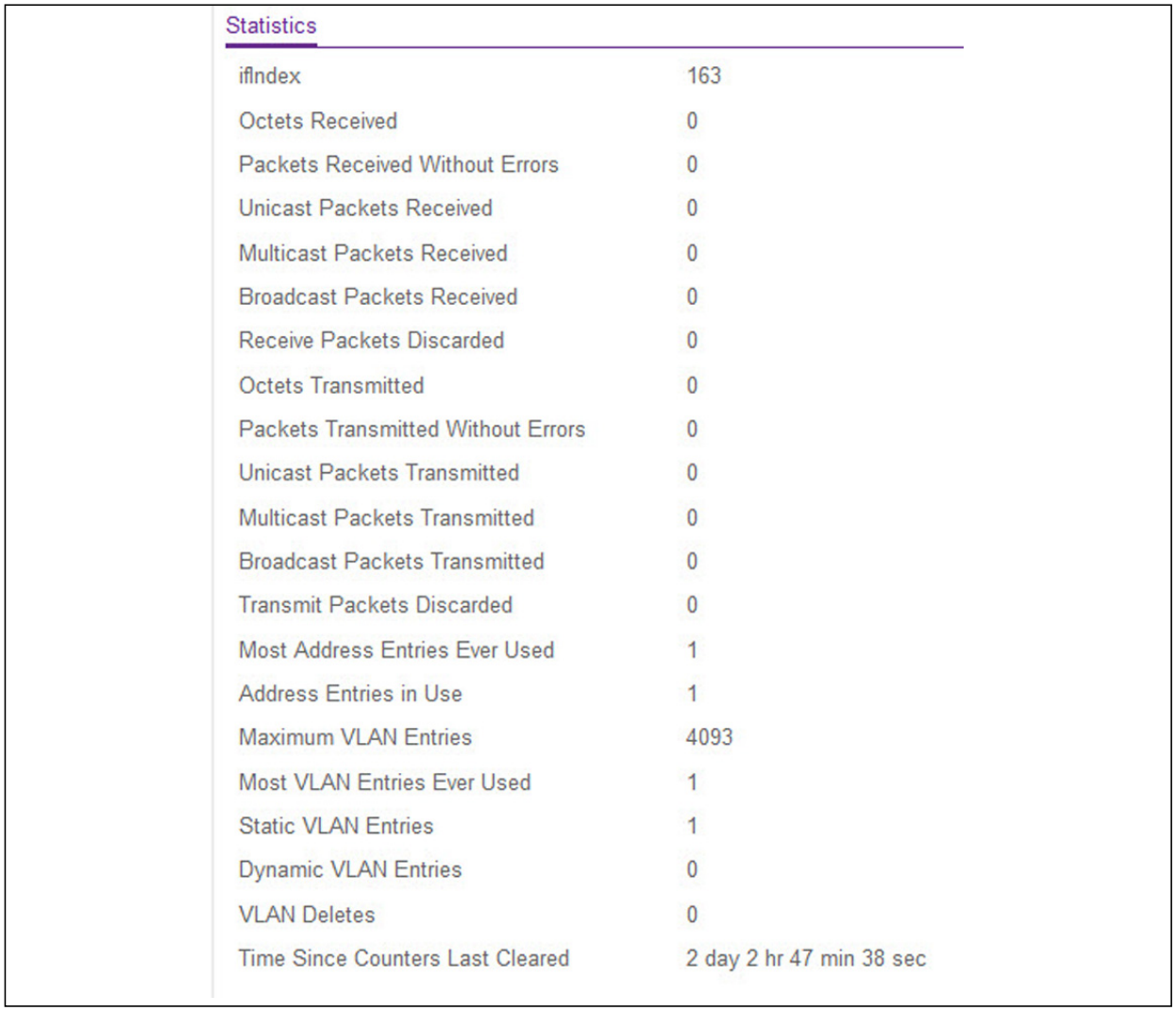
➢ **Use CPU Threshold page to configure thresholds**

1. Configure the **Rising Threshold** value. Notification is generated when the total CPU utilization exceeds this threshold value over the configured time period. The range is 1 to 100.
2. Configure the **Rising Interval** value. This utilization monitoring time period can be configured from 5 to 86400 seconds in multiples of 5 seconds.
3. Configure the **Falling Threshold**. Notification is triggered when the total CPU utilization falls below this level for a configured period of time. The falling utilization threshold must be equal to or less than the rising threshold value. The falling utilization threshold notification is made only if a rising threshold notification was done previously. Configuring the falling utilization threshold and time period is optional. If the Falling CPU utilization parameters are not configured, then it takes the same value as Rising CPU utilization parameters. The range is 1 to 100.
4. Configure the **Falling Interval**. The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds.
5. Configure the CPU **Free Memory Threshold** value in KB.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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 is displayed.



The following table describes Switch Statistics information.

Table 10. 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).
Packets Received Without Errors	The total number of packets (including broadcast packets and multicast packets) received by the processor.

Field	Description
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 that will 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 that will 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 that will 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.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.

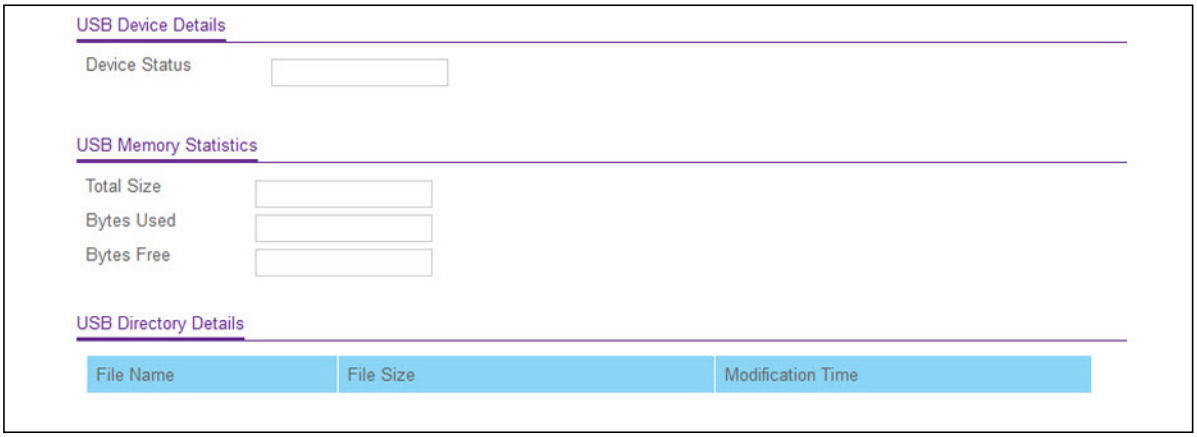
Field	Description
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
Dynamic VLAN Entries	The number of presently active VLAN 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.

USB Device Information

This page displays the USB device status.

To display the USB device information page, click **System** > **Management** > **USB Device Information**. A screen similar to the following is displayed.



USB Device Details

This screen displays the non-configurable USB device details shown in the following table.

Table 11. USB Device Details

Field	Description
Device Status	This field specifies the current status of the device. Status is: • **Active** if the device is USB plugged in and recognized by the switch. • **Inactive** if the device is not mounted. • **Invalid** if the device is not present or an invalid device is plugged in.

Click **Update** to update the page with the latest information on the switch.

USB Memory Statistics

This screen displays the memory statistics of the USB flash device.

The following table describes the non-configurable USB Memory Statistics information.

Table 12. USB Memory Statistics Information

Field	Description
Total Size	This field displays the USB flash device storage size in bytes.
Bytes Used	This field displays the size of memory used on the USB flash device.
Bytes Free	This field displays the size of memory free on the USB flash device.

Click **Update** to update the page with the latest information on the switch.

USB Directory Details

This screen displays the directory information of the USB flash device.

The following table describes the non-configurable USB Directory Details information.

Table 13. USB Directory Details Information

Field	Description
File Name	This field displays the Name of the file stored in the USB flash drive.

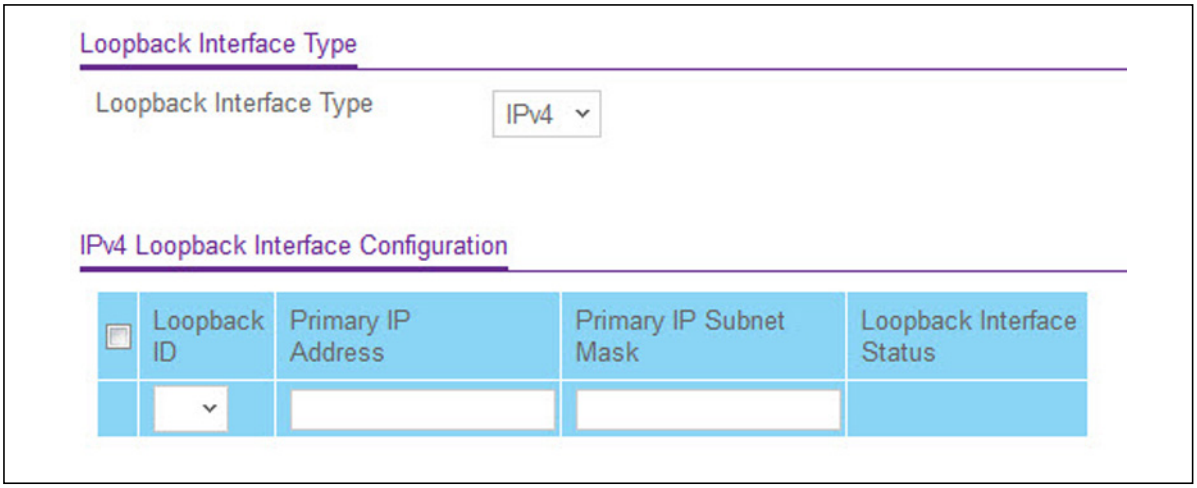
Field	Description
File Size	This field displays the Size of the file stored in the USB flash drive in bytes
Modification Time	This field displays the Last modification time of the file stored in the USB flash drive.

Click **Update** to update the page with the latest information on the switch.

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 is displayed.



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 is 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 is 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 is 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 is 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 is visible when IPv6 loopback is selected.

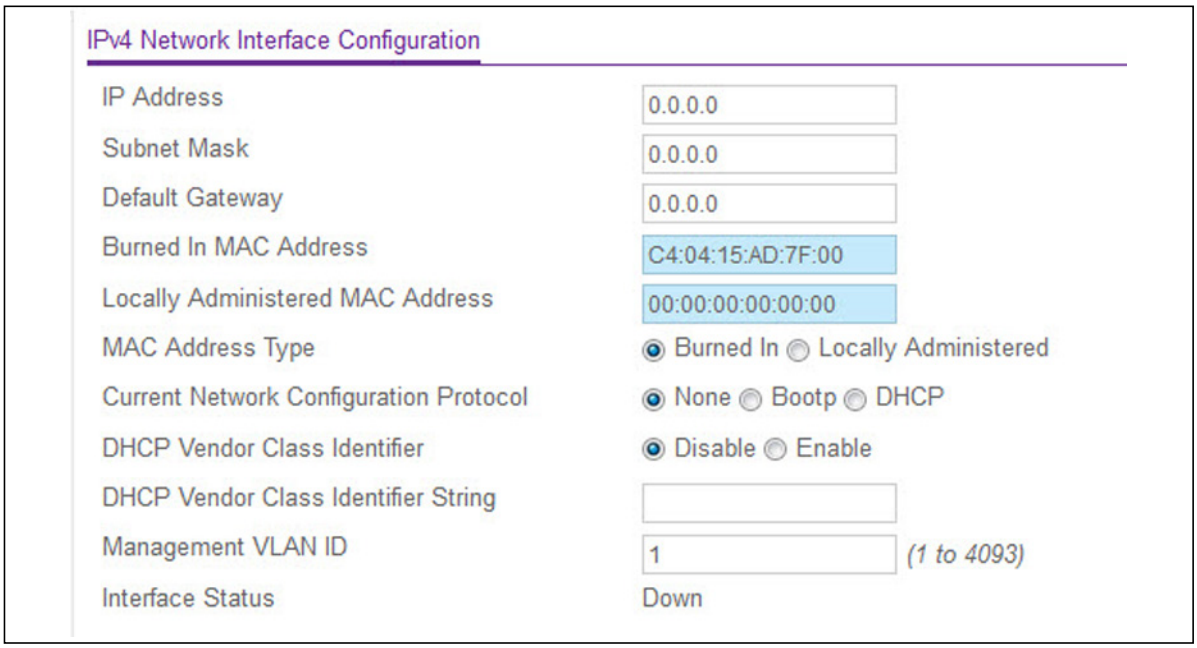
8. Use the **IPv6 Address** field to enter the IPv6 address in the format prefix/length. This option is visible when IPv6 loopback is selected.
9. Use the **EUI64** field to optionally specify the 64-bit extended unique identifier (EUI-64). This option is visible when IPv6 loopback is selected.

Network Interface

From the **System** > **Management** > **Network Interface** link, you can access the following pages:

IPv4 Network Configuration

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



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

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

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

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

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

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

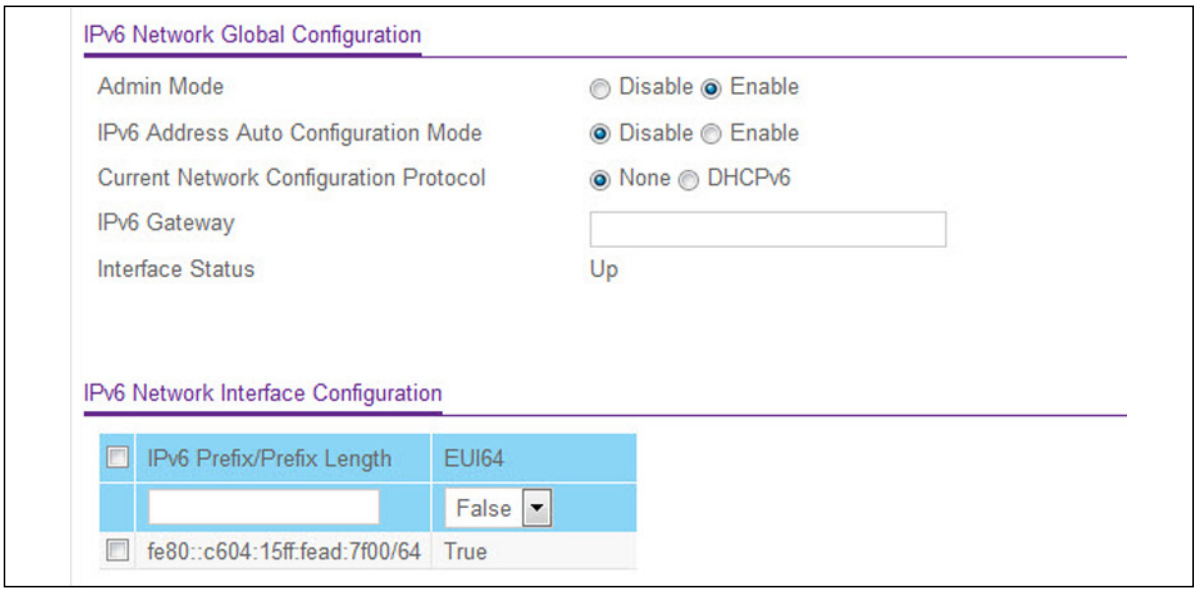
The following table describes IPv4 Network Configuration information.

Table 14. IPv4 Network Configuration Information

Field	Description
Burned In MAC Address	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 Configuration**. A screen similar to the following is displayed.



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

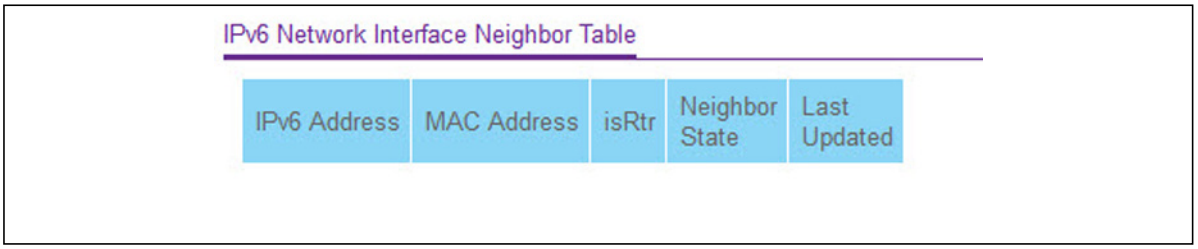
- Web-based management

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 is displayed.



The following table displays IPv6 Network Interface Neighbor Table information.

Table 15. 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.
Neighbor State	The state of the neighboring switch: • reachable(1) - The neighbor is reachable by this switch. • stale(2) - Information about the neighbor is scheduled for deletion. • delay(3) - No information has been received from neighbor during delay period. • probe(4) - Switch is attempting to probe for this neighbor. • unknown(6) - Unknown status.
Last Updated	The last sysUpTime that this neighbor has been updated.

IPv4 Service Port Configuration

Use this page to configure network information on the IPv4 Service Port. The service port is a dedicated Ethernet port for out-of-band management of the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.

To configure the IPv4 Service Port:

1. Click **System** > **Management** > **Network Interface > IPv4 Service Port**. The following screen is displayed.

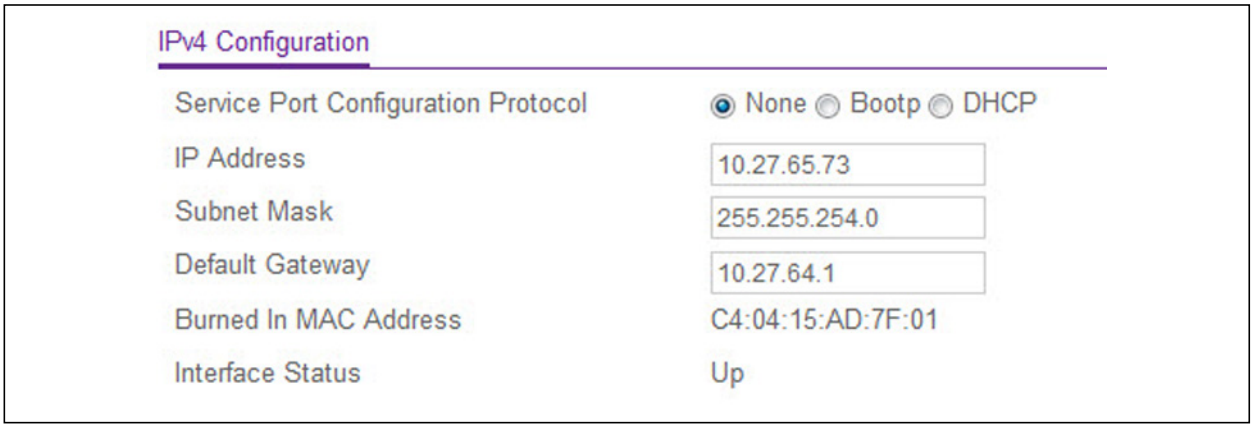


Figure 10. IPv4 Service Port

2. Using the Service Port Configuration Protocol field, specify how the device acquires network information on the service port by selecting one of the following:

- BootP—During the next boot cycle, the BootP client on the device broadcasts a BootP request in an attempt to acquire information from a BootP server on the network.
- DHCP—During the next boot cycle, the DHCP client on the device broadcasts a DHCP request in an attempt to acquire information from a DHCP server on the network.
- None—The device does not attempt to acquire network information dynamically.

3. In the IP address field, specify the IP address of the interface.
   - If the Service Port configuration Protocol is **None**, you can manually configure a static IP address.
   - If the Service Port configuration Protocol is **BootP** or **DHCP**, this field displays the IP address that was dynamically acquired (if any).
4. In the Subnet Mask field, specify the IP subnet mask for the interface.
   - If the Service Port configuration Protocol is **None**, you can manually configure a static subnet mask.
   - If the Service Port configuration Protocol is **BootP** or **DHCP**, this field displays the subnet mask that was dynamically acquired (if any).
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. Click **Update** to update the page with the latest information on the switch.

The following table describes the non-configurable fields on the Service Port Configuration page.

Table 16. IPv4 Service Port

Field	Description
Burned-in MAC Address	The burned-in MAC address used for out-of-band connectivity.
Interface Status	Indicates whether the link status is up or down.
DHCP Client Identifier	The identification code assigned to the client on a network. The DHCP server uses this code to identify this device.

IPv6 Service Port Configuration

Use this page to configure IPv6 network information on the Service Port. The service port is a dedicated Ethernet port for out-of-band management of the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.

To configure the IPv6 Service Port:

1. Click **System** > **Management** > **Network Interface > IPv6 Service Port**. The following screen is displayed.

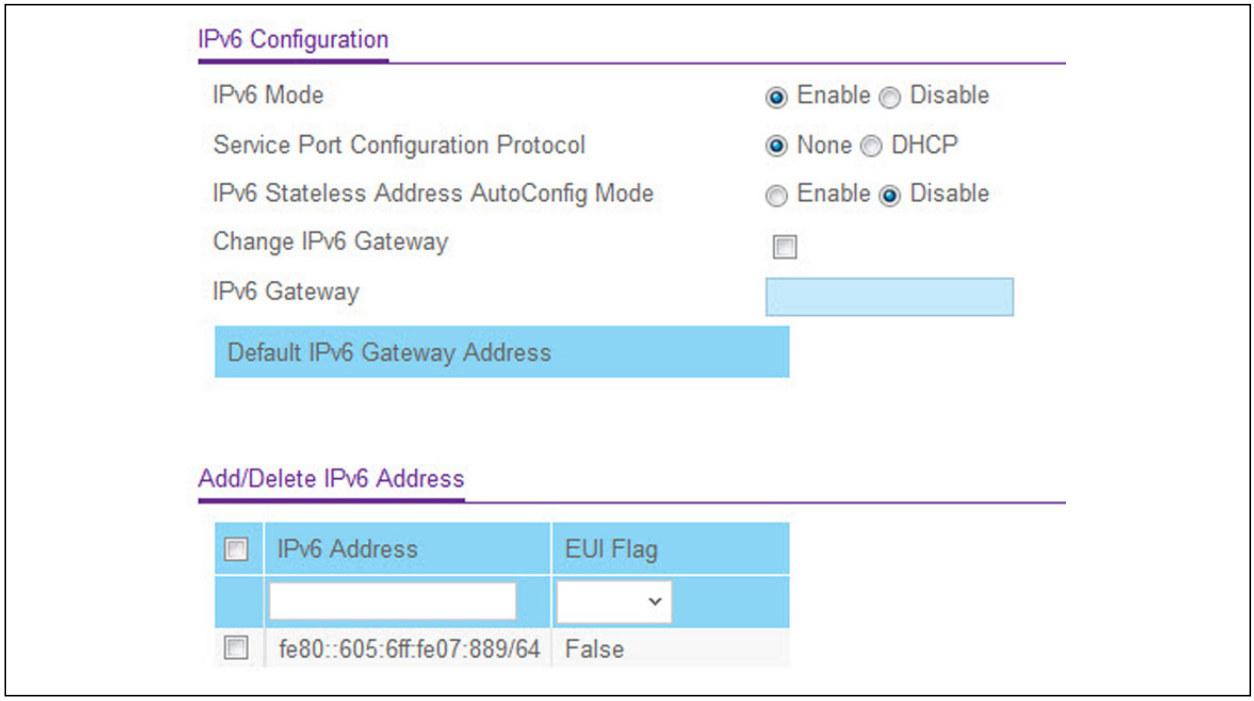


Figure 11. IPv6 Service Port

2. In the IPv6 Mode field, specify whether to enable or disable IPv6 administrative mode on the service port.
3. In the Service Port Configuration Protocol field, specify whether the device acquires network information from a DHCPv6 server. Selecting **None** disables the DHCPv6 client on the service port.
4. Use the IPv6 Stateless Address AutoConfig Mode field to set the IPv6 stateless address autoconfiguration mode on the service port.
   - **Enabled**—The service port can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages.
   - **Disabled**—The service port will not use the native IPv6 address autoconfiguration feature to acquire an IPv6 address.
5. The DHCPv6 Client DUID field displays the client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.
6. Check the Change IPv6 Gateway Address field to configure the IPv6 Gateway field.
7. Use the IPv6 Gateway field to specify the default gateway for the IPv6 service port interface.
8. The **Add/Delete IPv6 Address** table lists the manually configured static IPv6 addresses on the service port interface.
   a. In the IPv6 Address field, specify the IPv6 address to add or remove from the service port interface.

   b. Select the EUI Flag option to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or clear the option to omit the flag.
9. Click **Add** to add a new IPv6 address to the service port interface.
10. Click **Delete** to delete the selected IPv6 address.
11. Click **Update** to update the page with the latest information on the switch.
12. Click **Cancel** to cancel the configuration on the screen. This resets the data on the screen to the latest value of the switch.
13. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

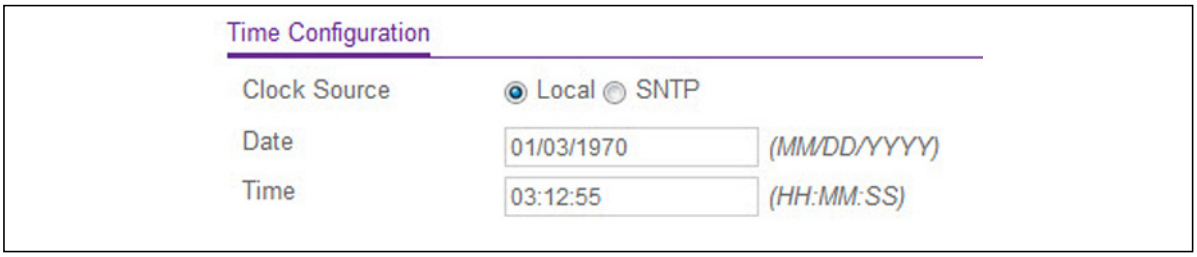
Time

M6100 Chassis switch software supports the Simple Network Time Protocol (SNTP). 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.

Time Configuration

Use the Time Configuration page to configure time locally or through SNTP.

To display the Time Configuration page, click **System** > **Management > Time** > **Time Configuration**. The following screen is displayed.



➢ **To configure the Time settings**

1. In the **Clock Source** field, select the option to configure time locally or through SNTP. The default is SNTP. The local clock can be set to SNTP only if the following two conditions are met:
   a. The SNTP server is configured.
   b. The SNTP last attempt status is successful.
2. Use the **Date** field to specify the current date in months, days, and years.
3. In the Time field, specify the current time in hours, minutes, and seconds.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Update** to update the page with the latest information on the switch.

SNTP Server Configuration

SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. M6100 Chassis switch software operates only as an SNTP client and cannot provide time services to other systems.

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

The following is an example of stratums:

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

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

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

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

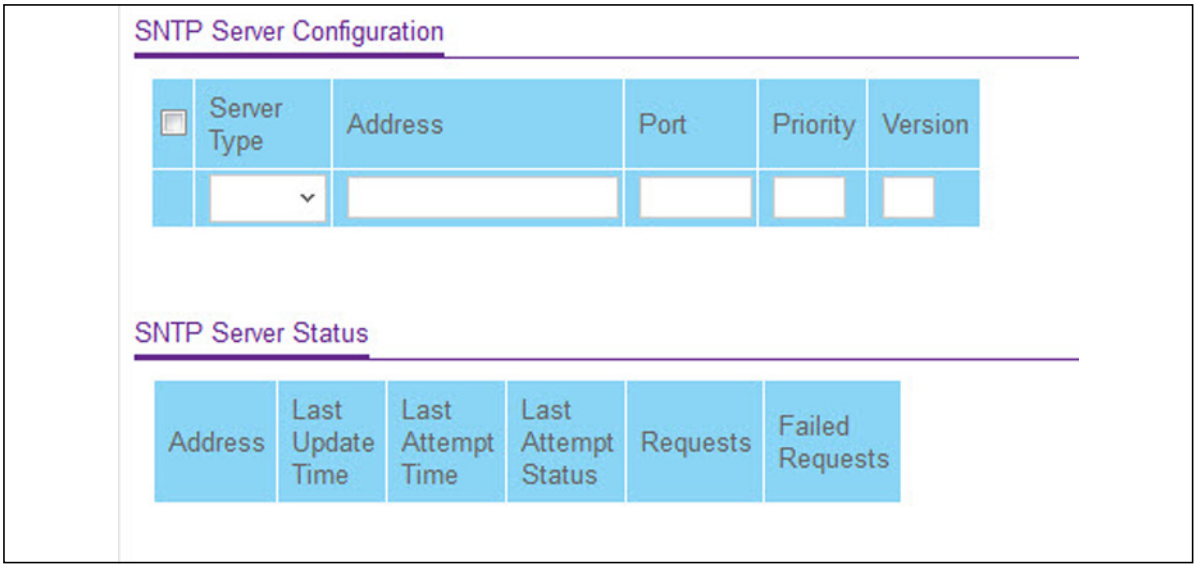
The device can poll Unicast server types for the server time.

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.

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**.



➢ **To configure a new SNTP Server:**

1. Use the **Server Type** field to specify the address type of the configured SNTP Server address. Possible values are:
   - IPv4
   - IPv6
   - DNS

   The default value is IPv4.
2. In the **Address** field, 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 an 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 an SNTP request is sent to it.
3. Enter a **Port** number on the SNTP server to which SNTP requests are sent. The valid range is 1 to 65535. The default value is 123.
4. 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. The valid range is 1 to 3. The default value is 1.
5. Specify the NTP **Version** running on the server. The range is 1 to 4. The default value is 4.
6. Click **Add** to add an SNTP Server entry. This sends the updated configuration to the switch. Configuration changes take effect immediately.
7. Repeat the previous steps to add additional SNTP servers. You can configure up to three SNTP servers.

8. 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, then click **Apply**. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. To remove an SNTP server entry, select the check box next to the configured server to remove, and then click **Delete**. The entry is removed, and the device is updated.
11. Click **Update** to update the page with the latest information on the switch.

SNTP Server Status

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

Table 17, SNTP Server Status displays SNTP Server Status information.

Table 17. SNTP Server Status

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

Field	Description
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.

Summer Time Configuration

Use this page to configure Summer Time Configuration information.

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

To configure the summer time configuration:

1. The summer time option is used to select one of the below four options.
   - **Disable** - This option is used to disable Summer Time.
   - **Recurring** - This option is used to enable Recurring Summer Time.
   - **Recurring EU** - This option is used to enable Recurring EU Summer Time.
   - **Recurring USA** - This option is used to enable Recurring USA Summer Time.
   - **Non Recurring** - This option is used to configure Non Recurring Summer Time.

The fields below are visible only when Summer Time is Recurring or Recurring EU or Recurring USA.

Table 18. Summer Time - Recurring

Field	Description
Begins At	The fields under this are used to configure the Start values of date and time. • Week - This field is used to configure start week. • Day - This field is used to configure start day. • Month - This field is used to configure start month. • Hours - This field is used to configure start hours. • Minutes - This field is used to configure start minutes.
Ends At	The fields under this are used to configure the End values of date and time. • Week - This field is used to configure end week. • Day - This field is used to configure end day. • Month - This field is used to configure end month. • Hours - This field is used to configure end hours. • Minutes - This field is used to configure end minutes.
Offset	This field is used to configure Recurring offset.
Zone	This field is used to configure Zone.

The fields below are visible only when Summer Time is Non Recurring.

Table 19. Summer Time - Non Recurring

Field	Description
Begins At	The fields under this are used to configure the Start values of date and time. • Week - This field is used to configure start week. • Day - This field is used to configure start day. • Month - This field is used to configure start month. • Hours - This field is used to configure start hours. • Minutes - This field is used to configure start minutes.
Ends At	The fields under this are used to configure the End values of date and time. • Week - This field is used to configure end week. • Day - This field is used to configure end day. • Month - This field is used to configure end month. • Hours - This field is used to configure end hours. • Minutes - This field is used to configure end minutes.
Offset	This field is used to configure Recurring offset.
Zone	This field is used to configure Zone.

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

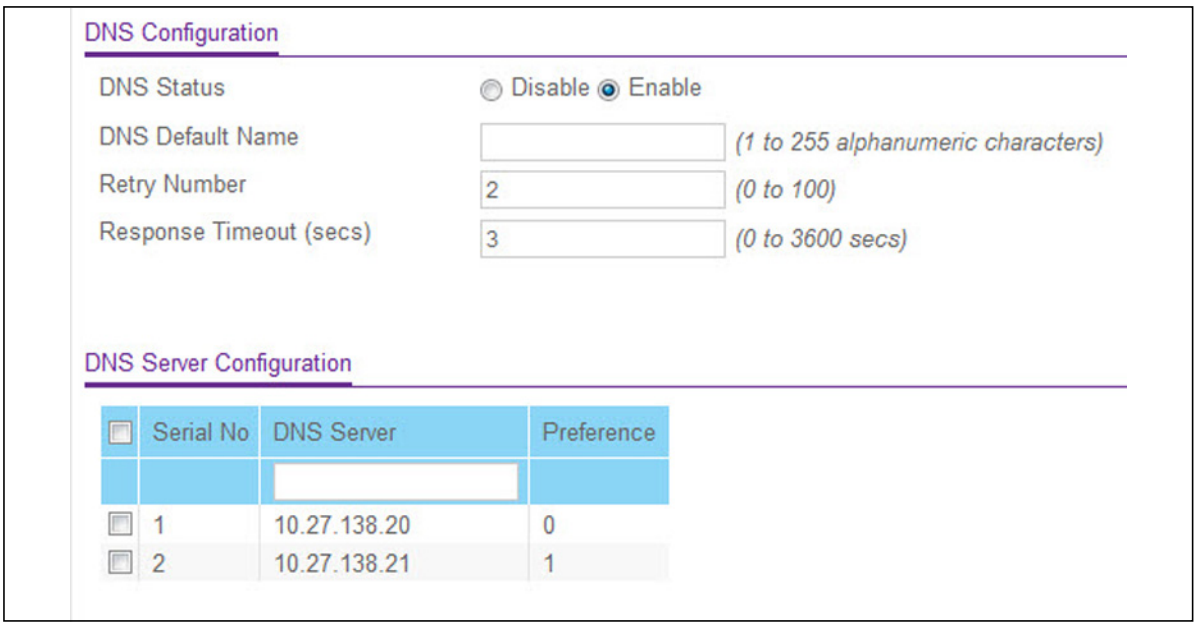
DNS

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

DNS Configuration

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

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



To configure the global DNS settings:

1. Specify whether to enable or disable the administrative status of the DNS Client.
   - **Enable** - Allow the switch to send DNS queries to a DNS server to resolve a DNS domain name. Default value is Enable.
   - **Disable** - Prevent the switch from sending DNS queries.
2. Enter the DNS default domain name to include in DNS queries. When the system is performing a lookup on an unqualified hostname, this field is provided as the domain name (for example, if default domain name is netgear.com and the user enters test, then test is changed to test.netgear.com to resolve the name). The length of the name should not be longer than 255 characters.
3. Use **Retry Number** to specify the number of times to retry sending DNS queries to DNS server. This number ranges from 0 to 100. The default value is 2.

4. Use **Response Timeout (secs)** to specify the amount of time, in seconds, to wait for a response to a DNS query. This timeout ranges from 0 to 3600. The default value is 3.
5. To specify the DNS server to which the switch sends DNS queries, enter an IP address in standard IPv4 dot notation in the **DNS Server Address** and click **Add**. The server appears in the list below. You can specify up to eight DNS servers. The precedence is set in the order created.
6. To remove a DNS server from the list, select the check box next to the server you want to remove and click **Delete**. If no DNS server is specified, the check box is global and will delete all the DNS servers listed.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Add** to add the specified DNS Server to the List of DNS Servers. Configuration changes take effect immediately.
10. Click **Delete** to delete the specified DNS Server from the list of DNS Servers. If no DNS Server is specified then it will delete all the DNS Servers

DNS Server Configuration

The following table displays DNS Server Configuration information.

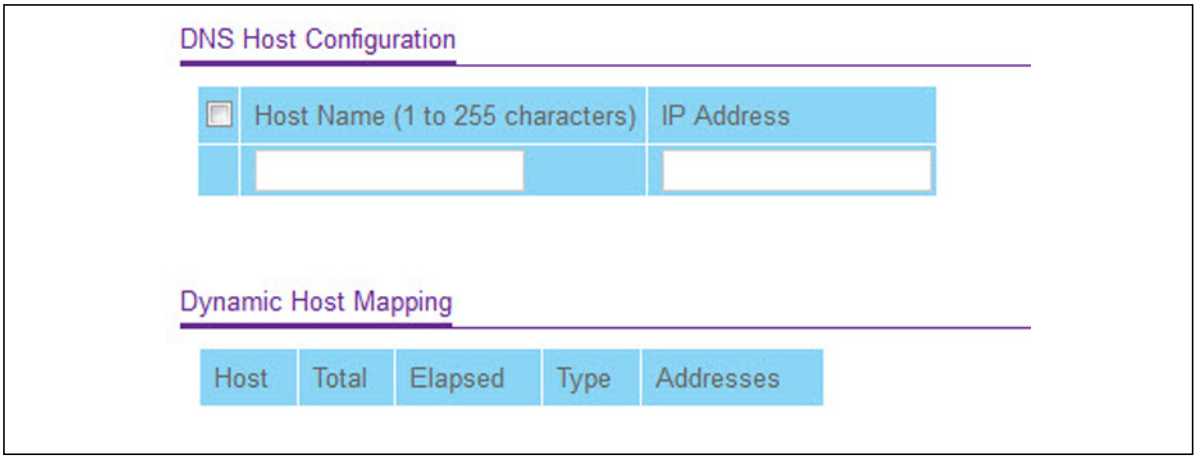
Table 20. DNS Server Configuration

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. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Clear** to clear all the dynamic host name entries from the list.

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

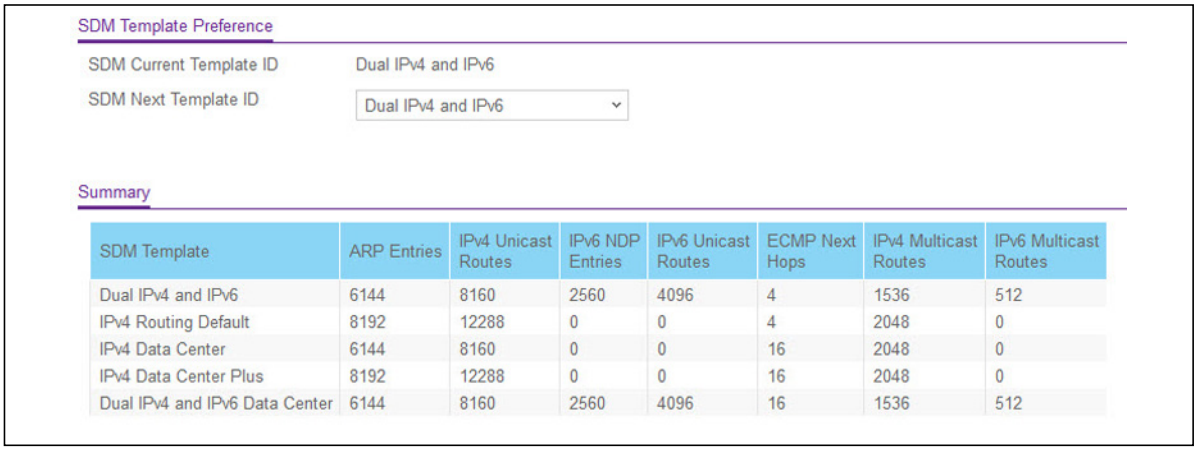
Table 21. DNS - Dynamic Host Mapping

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	8160	2560	4096	4	1536	512
IPv4 Routing Default	8192	12288	0	0	4	2048	0
IPv4 Data Center	6144	8160	0	0	16	2048	0
IPv4 Data Center Plus	8192	12288	0	0	16	2048	0
Dual IPv4 and IPv6 Data Center	6144	8160	2560	4096	16	1536	512

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:
   - Dual IPv4 and IPv6
   - IPv4 Routing Default
   - IPv4 Data Center
   - IPv4 Data Center Plus
   - Dual IPv4 and IPv6 Data Center

The following table displays Summary information.

Table 22. SDM Template Preference Summary

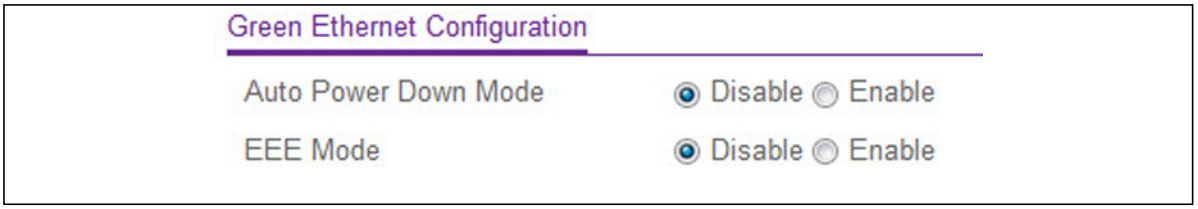
Field	Description
SDM Current Template ID	Displays the current active SDM Template. Possible values are: • Dual IPv4 and IPv6 • IPv4-routing Default • IPv4 Data Center
SDM Template	Identifies the Template. The possible values are: • Dual IPv4 and IPv6 • IPv4-routing Default • IPv4 Data Center
ARP Entries	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.

Field	Description
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.

Green Ethernet Configuration

You can use this page to configure the Green Ethernet settings for the switch.

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



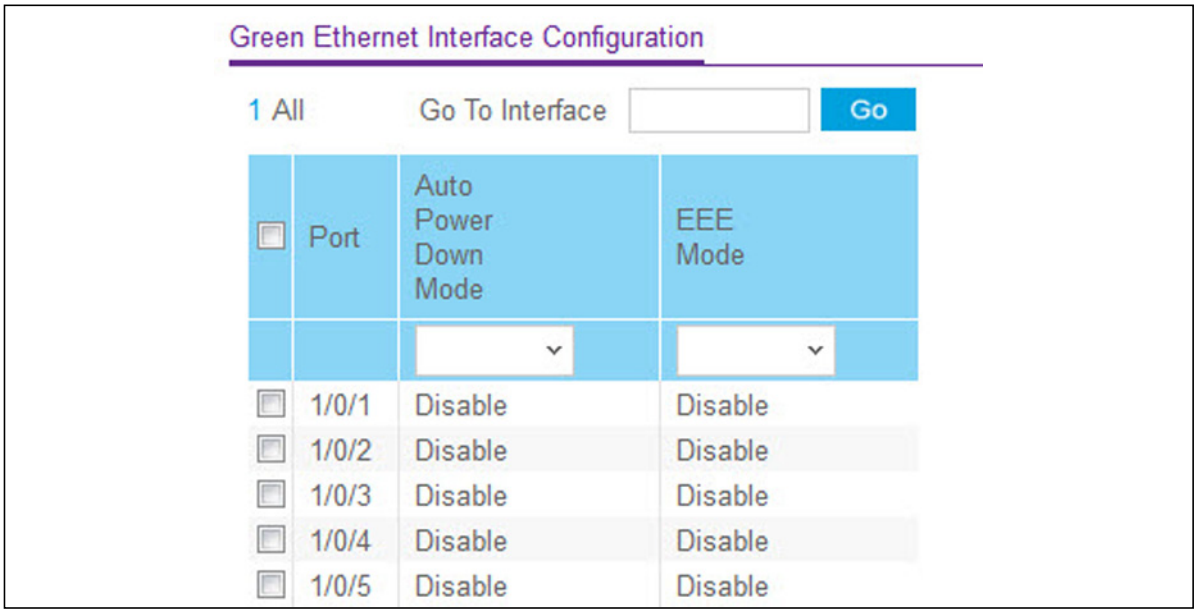
To configure the Green Ethernet settings:

1. Use the **Auto Power Down Mode** radio buttons to enable or disable this option. The factory default is enable. When the port link is down the PHY will automatically go down for short period of time, and then wakes up to check link pulses. This will allow performing auto-negotiation and saving power consumption when no link partner is present.
2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. Click **Apply** to update the configuration on the switch.

Green Ethernet Interface Configuration

Use this page to configure the Green Ethernet interface settings.

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



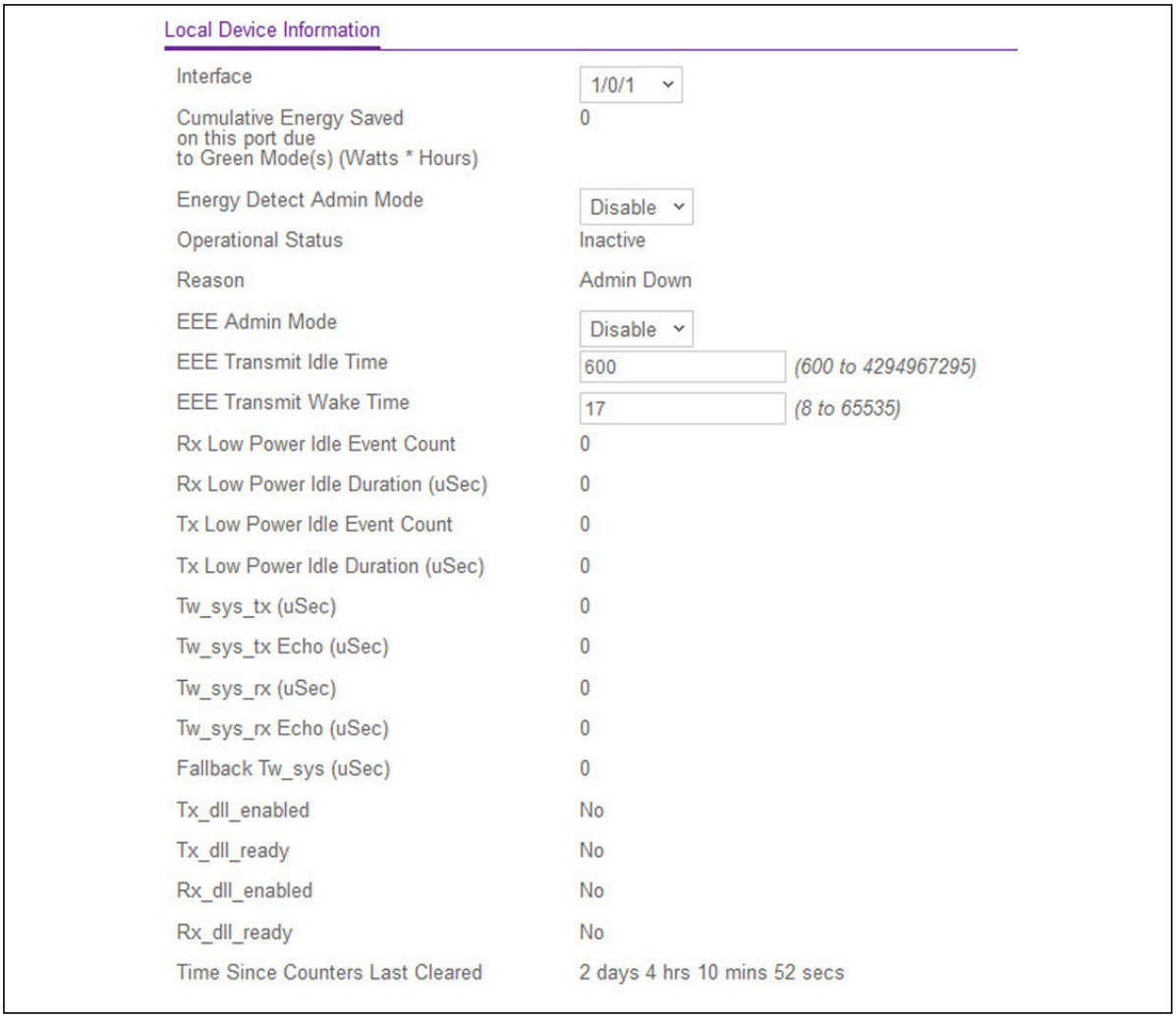
To configure the Green Ethernet interface settings:

1. Specify the **Go To Interface** by entering the Interface in unit/slot/port format and click on the **Go** button. The entry corresponding to the specified Interface, will be selected.
2. Select the **Port** for which data is to be displayed or configured.
3. Use the **Auto Power Down Mode** selection to enable or disable this option. The factory default is enable. When the port link is down the PHY will automatically go down for short period of time, and then wakes up to check link pulses. This will allow performing auto-negotiation and saving power consumption when no link partner is present.
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 update the configuration on the switch.

Green Ethernet Local and Remote Device Configuration

Use this page to configure the Green Ethernet Mode Local Device and Remote Device settings.

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



Configure Green Ethernet Local Device Details

➢ **To configure the green Ethernet local device information:**

1. Select the **Interface** for which data is to be displayed or configured.
2. Use the **Energy Detect Admin Mode** selection to enable or disable this option on the port. With energy detect mode enabled, when the port link is down, the PHY will automatically go down for short period of time, and then wakes up to check link pulses. This will allow performing auto-negotiation and saving power consumption when no link partner is present. The Default value is Disabled.
3. Use the **Short Reach Admin Mode** selection to enable or disable this option on the port. With short reach mode enabled, PHY is forced to operate in low power mode irrespective of the cable length. The Default value is Disabled.
4. Use the **EEE Admin Mode** selection to enable or disable this option on the port. With EEE mode enabled, Port transitions to Low power Mode during Link Idle condition. The Default value is Disabled.

Table 23, Green Ethernet Local Device Information describes the non-configurable fields.

Table 23. Green Ethernet Local Device Information

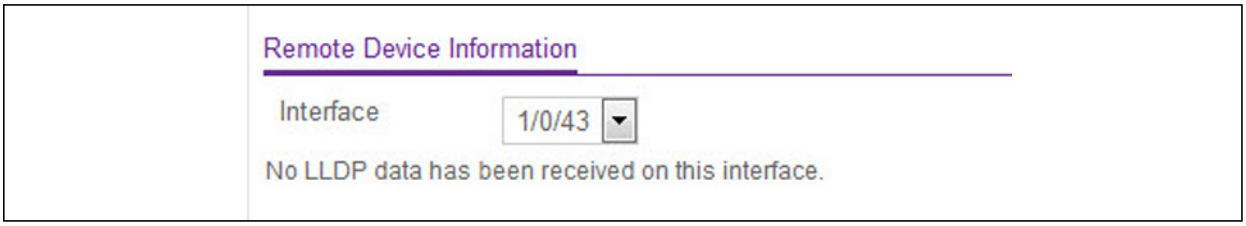
Field	Description
Cumulative Energy Saved on this port due to Green Mode(s) (Watts * Hours)	Cumulative Energy saved due to all Green Modes enabled on this port in (Watts * Hours).
Operational Status	Indicates whether Energy Detect Admin Mode is currently Operational (“Enabled”).
Reason	Reason for the current operational status of Energy Detect Admin Mode.
Operational Status	Indicates whether Short Reach Admin Mode is currently Operational(“Enabled”).
Reason	Reason for the current operational status of Short Reach Admin Mode.
Rx Low Power Idle Event Count	This field is incremented each time MAC RX enters LP IDLE state. Shows the total number of Rx LPI Events since EEE counters are last cleared.
Rx Low Power Idle Duration (uSec)	This field indicates duration of Rx LPI state in 10us increments. Shows the total duration of Rx LPI since the EEE counters are last cleared.
Tx Low Power Idle Event Count	This field is incremented each time MAC TX enters LP IDLE state. Shows the total number of Tx LPI Events since EEE counters are last cleared.
Tx Low Power Idle Duration (uSec)	This field indicates duration of Tx LPI state in 10us increments. Shows the total duration of Tx LPI since the EEE counters are last cleared.
Tw_sys_tx (uSec)	Integer that indicates the value of Tw_sys that the local system can support.
Tw_sys_tx Echo (uSec)	Integer that indicates the remote system's Transmit Tw_sys that was used by the local system to compute the Tw_sys that it wants to request from the remote system.
Tw_sys_rx (uSec)	Integer that indicates the value of Tw_sys that the local system requests from the remote system.
Tw_sys_rx Echo (uSec)	Integer that indicates the remote systems Receive Tw_sys that was used by the local system to compute the Tw_sys that it can support.
Fallback Tw_sys (uSec)	Integer that indicates the value of fallback Tw_sys that the local system requests from the remote system.

Table 23. Green Ethernet Local Device Information

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

5. Click **Clear** to clear the configuration, resetting all statistics for the selected interface to default values.
6. Click **Apply** to update the configuration on the switch.
7. Click **Update** to update the page with the latest information on the switch.

Configure Green Ethernet Remote Device Details



➢ **To configure the green Ethernet remote device information:**

1. Select the **Interface** for which data is to be displayed or configured.

Table 24, Green Ethernet Remote Device Information on page 51 describes the non-configurable fields.

Table 24. Green Ethernet Remote Device Information

Field	Description
Remote ID	Specifies the remote client identifier assigned to the remote system.
Remote Tw_sys_tx (uSec)	Integer that indicates the value of Tw_sys that the remote system can support.

Table 24. Green Ethernet Remote Device Information

Field	Description
Remote Tw_sys_tx Echo (uSec)	Integer that indicates the value Transmit Tw_sys echoed back by the remote system.
Remote Tw_sys_rx (uSec)	Integer that indicates the value of Tw_sys that the remote system requests from the local system.
Remote Tw_sys_rx Echo (uSec)	Integer that indicates the value of Receive Tw_sys echoed back by the remote system.
Remote Fallback Tw_sys (uSec)	Integer that indicates the value of fallback Tw_sys that the remote system is advertising.

Green Ethernet Statistics Summary

Use this page to view the Green Ethernet Statistics settings.

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

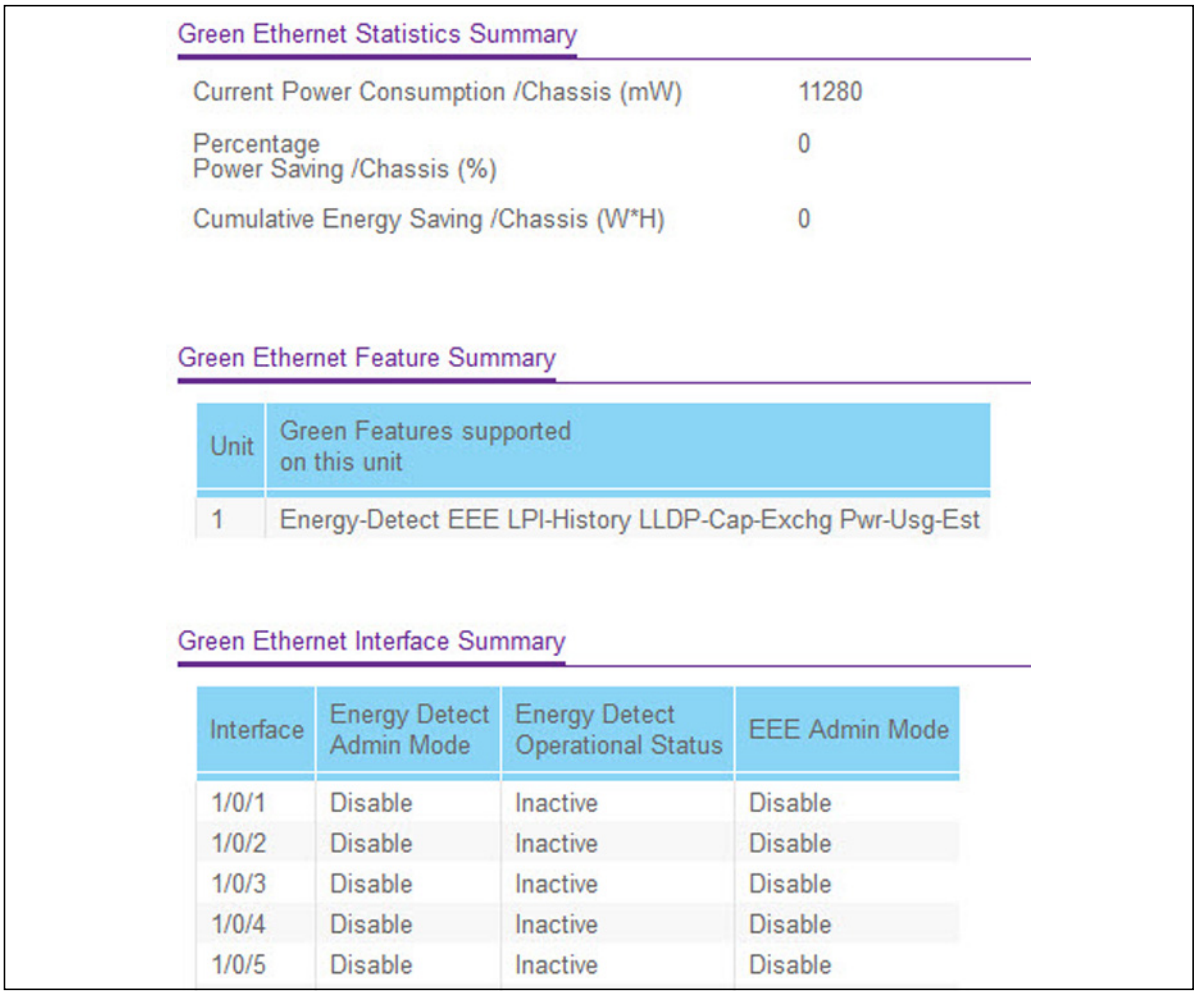


Table 25, Green Ethernet Statistics Summary on page 53 describes the non-configurable fields.

Table 25. Green Ethernet Statistics Summary

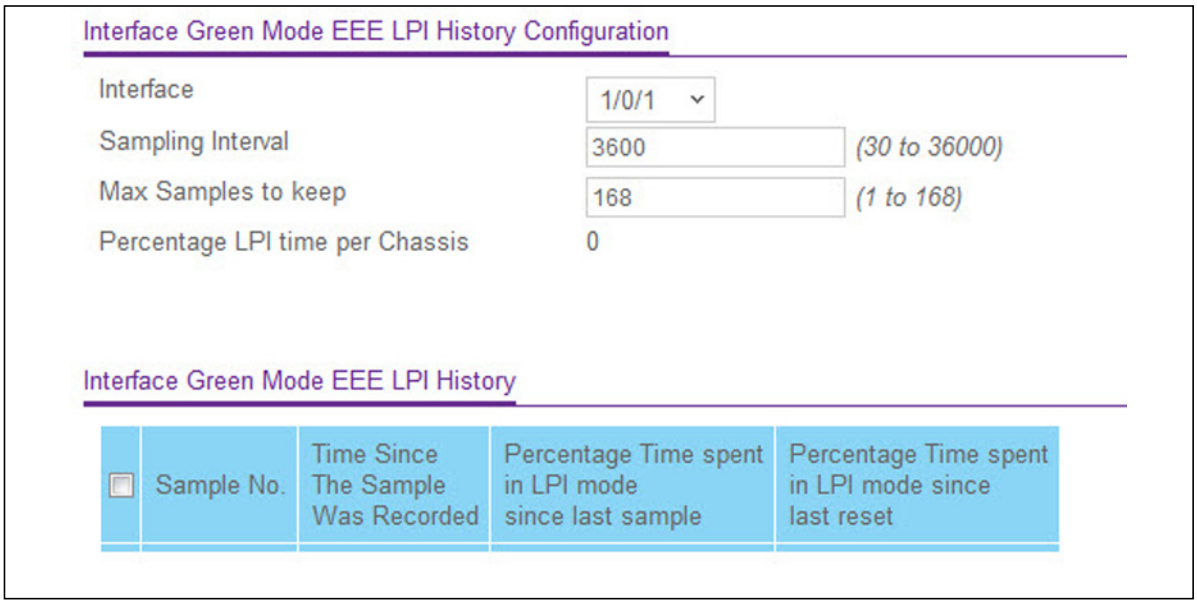
Field	Description
Current Power Consumption by all ports in Chassis (mWatts)	Estimated Power Consumption by all ports in chassis in mWatts.
Estimated Percentage Power Saving per chassis (%)	Estimated Percentage Power saved on all ports in chassis due to Green mode(s) enabled.
Cumulative Energy Saving per Chassis (Watts * Hours)	Estimated Cumulative Energy saved per Chassis in (Watts * Hours) due to all green modes enabled.
Unit	Displays the Unit ID.
Green Features supported on this unit	List of Green Features supported on the given unit which could be one or more of the following: Energy-Detect (Energy Detect), Short-Reach (Short Reach), EEE (Energy Efficient Ethernet), LPI-History (EEE Low Power Idle History), LLDP-Cap-Exchg (EEE LLDP Capability Exchange), Pwr-Usg-Est (Power Usage Estimates).
Interface	Interface for which data is displayed or configured.
Energy Detect Admin Mode	Enable / Disable Energy Detect Mode on the port. With this mode is enabled, when the port link is down the PHY automatically goes down for short period of time, and then wakes up to check link pulses. This will allow performing auto-negotiation and saving power consumption when no link partner is present.
Energy Detect Operational Status	Current operational status of the Energy Detect mode.
Short Reach Admin Mode	Enable / Disable Short Reach Admin Mode on the port. With short reach mode enabled, PHY is forced to operate in low power mode irrespective of the cable length.
Short Reach Operational Status	Current operational status of the Short Reach mode.
EEE Admin Mode	Enable / Disable Energy Efficient Ethernet Mode on the port. With EEE mode enabled, Port transitions to Low power Mode during Link Idle condition.

2. Click **Update** to update the page with the latest information on the switch.

Green Ethernet EEE LPI History

Use this page to configure the Green Ethernet Mode EEE LPI History settings.

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



To configure the port GreenMode EEE history:

1. Select the **Interface** for which data is to be displayed or configured.
2. The **Sampling Interval** is the Interval at which EEE LPI data needs to be collected. This is a global setting and is applied to all interfaces. The Range is (30 to 36000).The Default value is 3600.
3. The Max Samples is the number of samples to keep. This is a global setting and is applied to all interfaces. The Range is (1 to 168).The Default value is 168.

Table 26, Interface Green Mode EEE LPI History non-configurable fields.

Table 26. Interface Green Mode EEE LPI History

Field	Description
Percentage LPI time per Chassis	Time spent in LPI mode per chassis since EEE counters are last cleared.
Sample No.	Sample Index.
Time Since The Sample Was Recorded	Time Since The Sample Was Recorded. Each time the page is refreshed it shows a different time as it reflects the difference in current time and time at which the sample was recorded.

Table 26. Interface Green Mode EEE LPI History

Field	Description
Percentage Time spent in LPI mode since last sample	Percentage of time spent in LPI mode during the current measurement interval.
Percentage Time spent in LPI mode since last reset	Percentage of time spent in LPI mode since EEE LPI statistics are reset.

4. Click **Apply** to update the configuration on the switch.
5. Click **Update** to update the page with the latest information on the switch.

Device View

For Device View information, see *Device View* on page 13.

Services

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

- *DHCP Server* on page 55
- *DHCP Relay* on page 64
- *DHCP L2 Relay* on page 65
- *UDP Relay* on page 67
- *DHCPv6 Server* on page 70
- *DHCPv6 Relay* on page 78

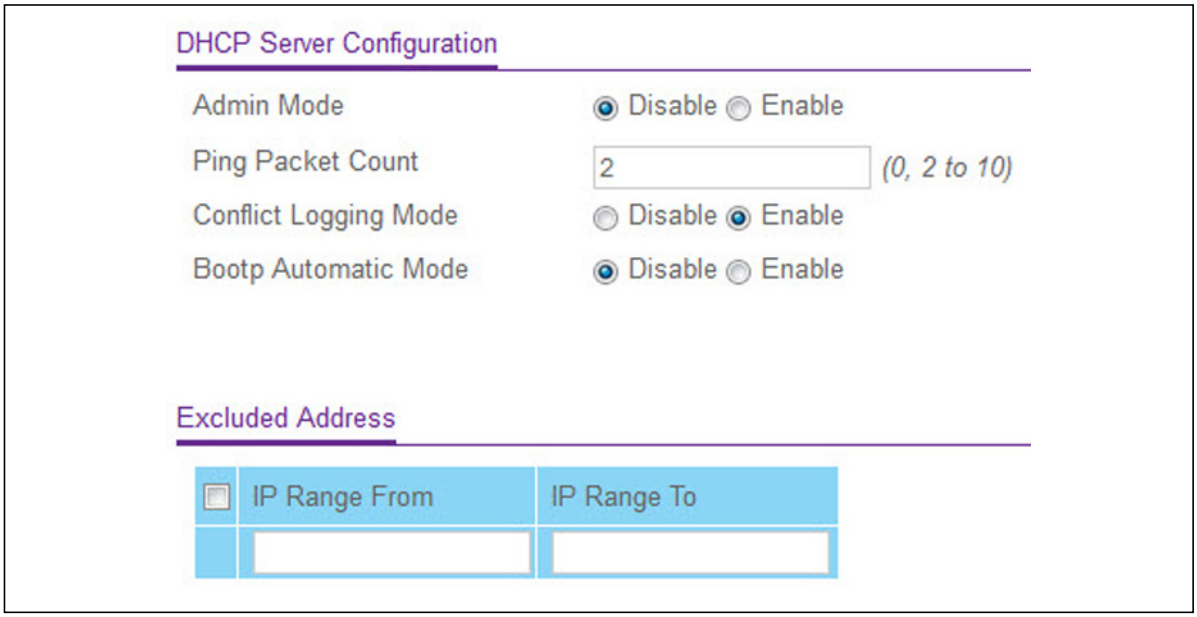
DHCP Server

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

- *DHCP Server Configuration* on page 55
- *DHCP Pool Configuration* on page 57
- *DHCP Pool Options* on page 60
- *DHCP Server Statistics* on page 60
- *DHCP Bindings Information* on page 62
- *DHCP Conflicts Information* on page 63

DHCP Server Configuration

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



To enable or disable DHCP service:

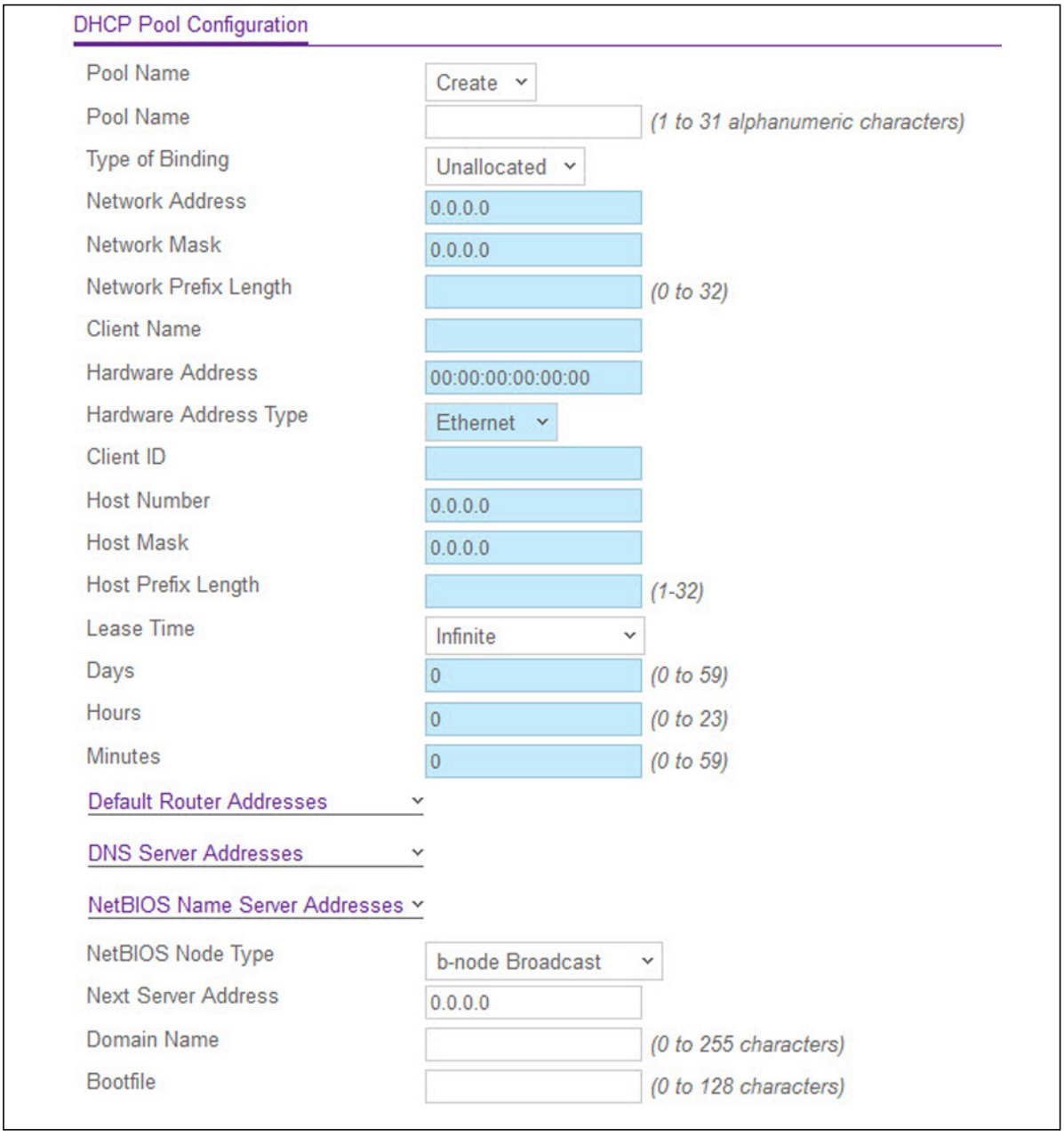
1. Use **Admin Mode** to specify whether the DHCP Service is to be Enabled or Disabled. Default value is Disable.
2. Use **Ping Packet Count** to specify the number of packets a server sends to a Pool address to check for duplication as part of a ping operation. Default value is 2. Valid Range is (0, 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 is displayed.



The following table describes the DHCP Pool Configuration fields.

Table 27. DHCP Pool Configuration

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. • Unallocated • Dynamic • Manual
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. The 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.

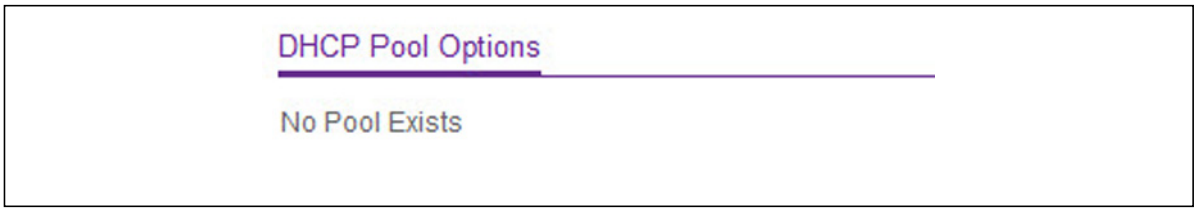
Field	Description
Host Mask	Specifies the subnet mask for a manual binding to a DHCP client. Either Host Mask or Prefix Length can be configured to specify the subnet mask but not both.
Host Prefix Length	Specifies the subnet mask for a manual binding to a DHCP client. Either Host Mask or Prefix Length can be configured to specify the subnet mask but not both. Valid Range is (0 to 32)
Lease Time	Can be selected as “Infinite” to specify lease time as Infinite or “Specified Duration” to enter a specific lease period. In case of dynamic binding infinite implies a lease period of 60 days and In case of manual binding infinite implies indefinite lease period. Default Value is “Specified Duration”.
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: • b-node Broadcast • p-node Peer-to-Peer • m-node Mixed • h-node Hybrid
Next Server Address	Specifies the Next Server Address for the pool.

Field	Description
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

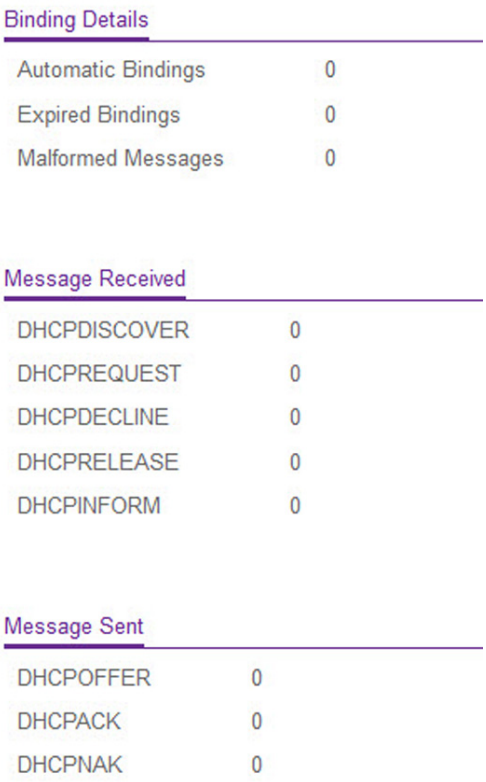
To display the DHCP Pool Options page, click **System** > **Services** > **DHCP Server**> **DHCP Pool Options**. A screen similar to the following is displayed.



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 is displayed.



The following table describes the DHCP Server Statistics fields.

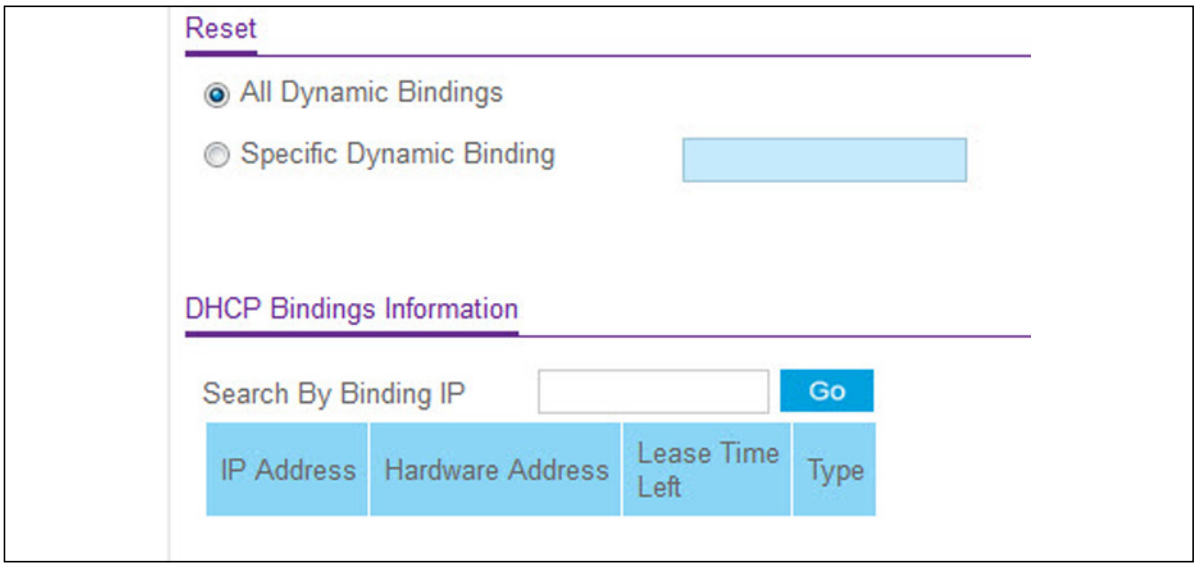
Table 28. DHCP Server Statistics

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 is displayed.



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

The following table describes the DHCP Bindings Information fields.

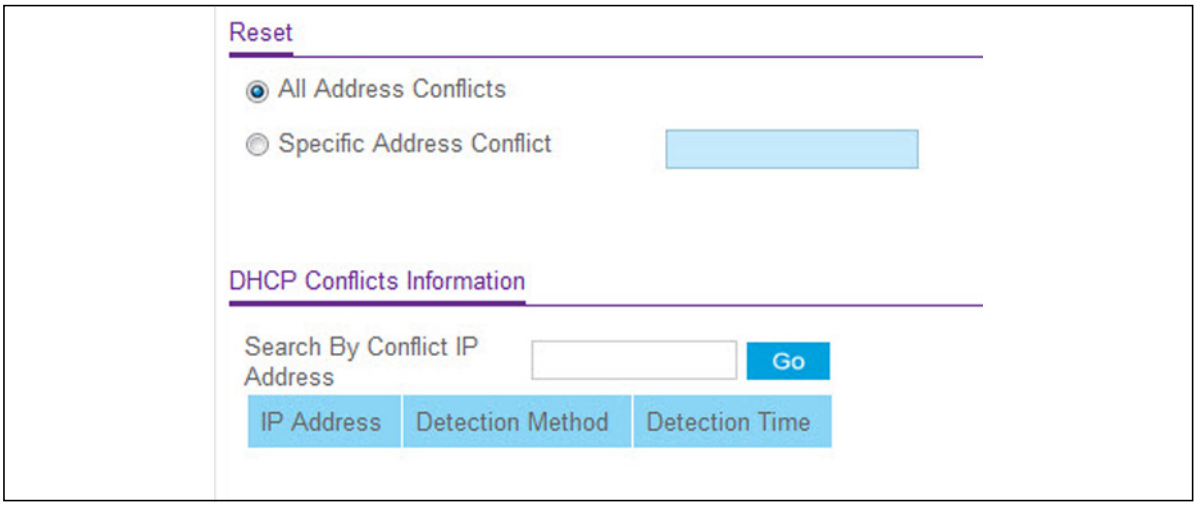
Table 29. DHCP Bindings Information

Field	Description
IP Address	Specifies the Client's IP Address.
Hardware Address	Specifies the Client's Hardware Address.

Field	Description
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 is displayed.



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

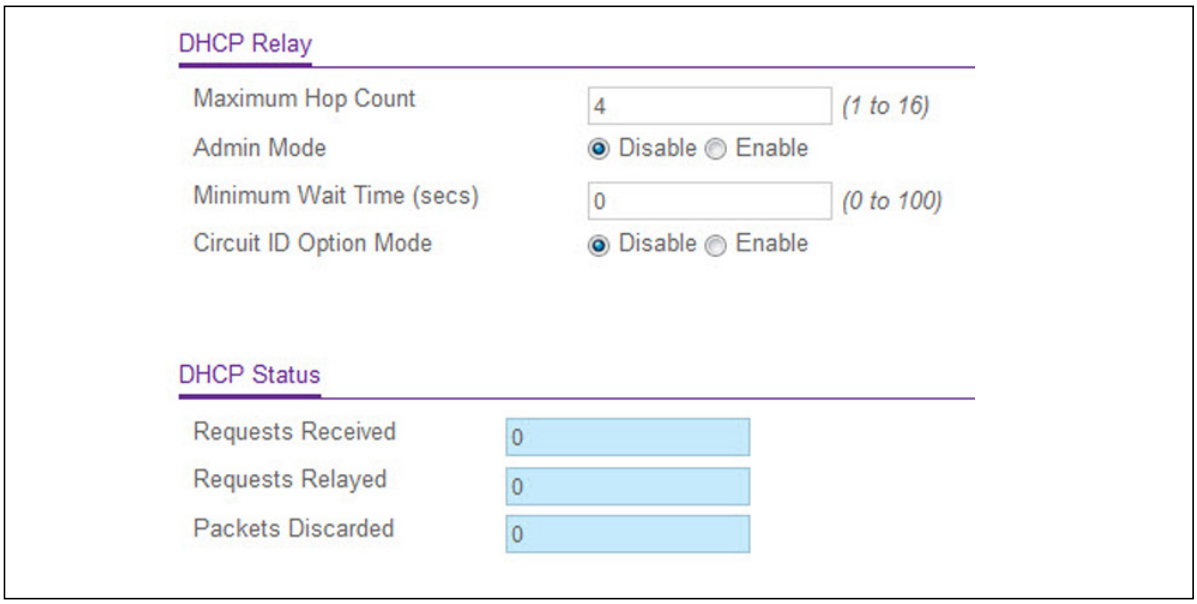
The following table describes the DHCP Conflicts Information fields.

Table 30. DHCP Conflicts Information

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 is displayed.



DHCP Relay Configuration

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

DHCP Relay Status

The following table describes the DHCP Relay Status fields.

Table 31. DHCP Relay Status

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

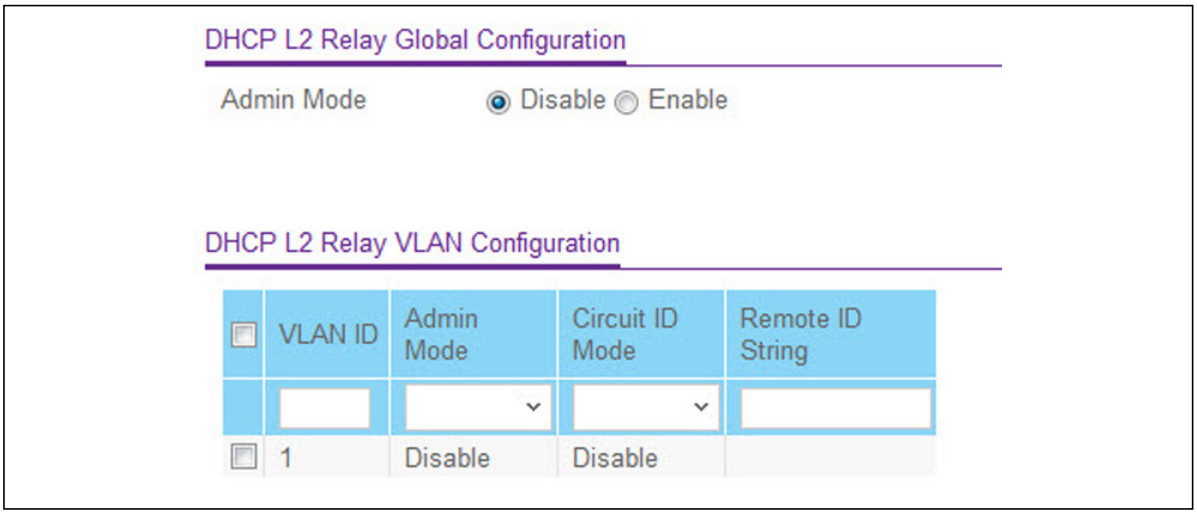
DHCP L2 Relay

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

- *DHCP L2 Relay Global Configuration* on page 65
- *DHCP L2 Relay Interface Configuration* on page 66
- *DHCP L2 Relay Interface Statistics* on page 66

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 is displayed.



DHCP L2 Relay Global Configuration

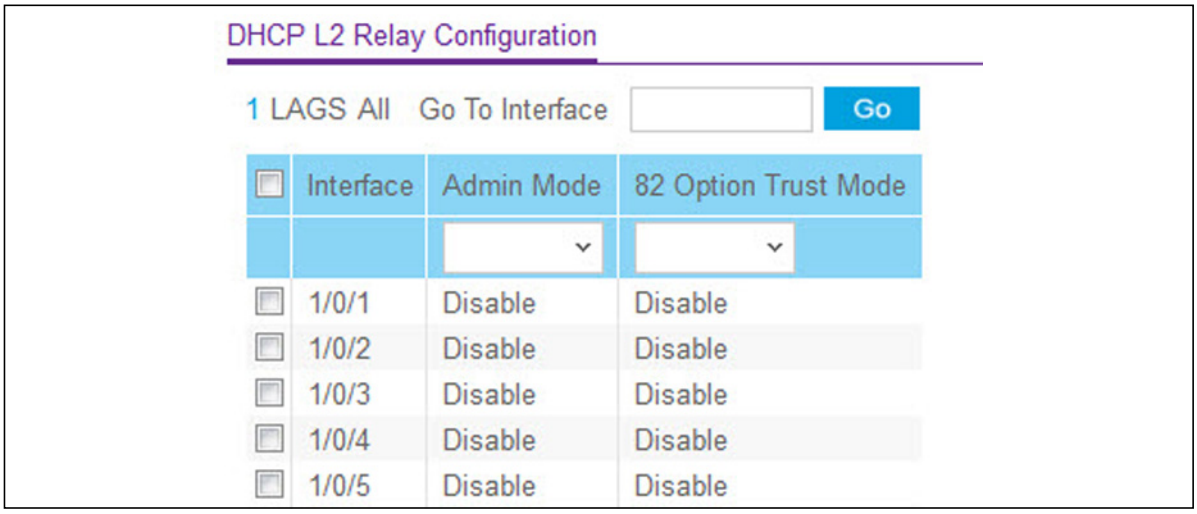
1. Use **Admin Mode** to enable or disable the DHCP L2 Relay on the switch. The default is Disable.

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

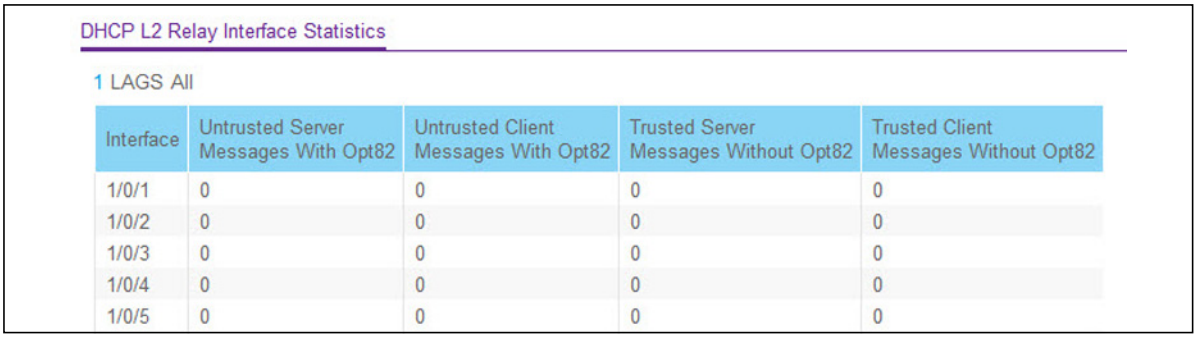
To display the DHCP L2 Relay Interface Configuration page, click **System** > **Services** > **DHCP L2 Relay**> **DHCP L2 Relay Interface Configuration**. A screen similar to the following is displayed.



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 is displayed.



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

Table 32. DHCP L2 Relay Interface Statistics

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

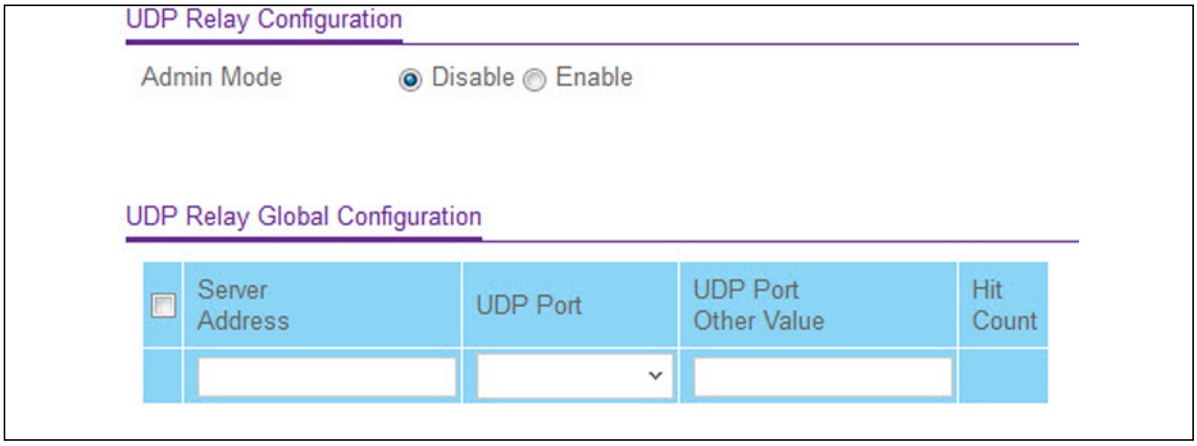
UDP Relay

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

- *UDP Relay Global Configuration* on page 67
- *UDP Relay Interface Configuration* on page 69

UDP Relay Global Configuration

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



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 Routing Image Protocol (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 **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

8. Click **Delete** to remove all entries or a specified one from UDP Relay Table.
9. Click **Update** to update the page with the latest information on the switch.

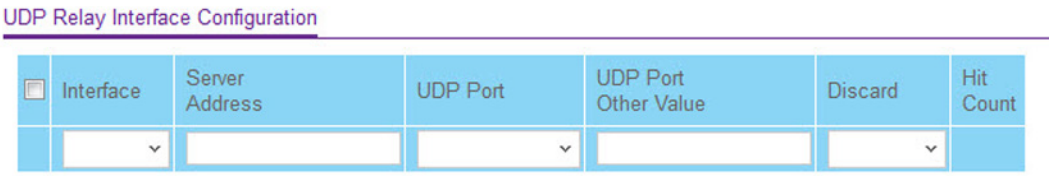
The following table describes the UDP Relay Global Configuration fields.

Table 33. UDP Relay Global Configuration

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 is displayed.



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 **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
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 **Delete** to remove all entries or a specified one from UDP Relay Interface Configuration Table.
10. Click **Update** to update the page with the latest information on the switch.

The following table describes the UDP Relay Interface Configuration fields.

Table 34. UDP Relay Interface Configuration

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

DHCPv6 Server

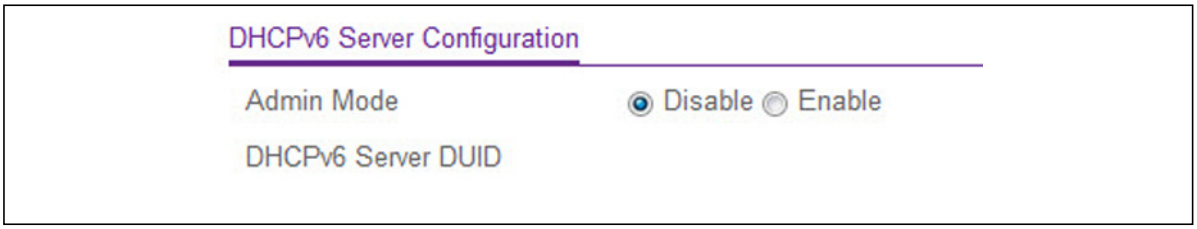
The **System > Services > DHCPv6 Server** navigation contains links to the following web pages that configure and display DHCPv6 data:

- *DHCPv6 Server Configuration*
- *DHCPv6 Pool Configuration* on page 71
- *DHCPv6 Prefix Delegation Configuration* on page 73
- *DHCPv6 Interface Configuration* on page 73
- *DHCPv6 Bindings Information* on page 74
- *DHCPv6 Server Statistics* on page 75

DHCPv6 Server Configuration

Use this page to configure the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server settings on the device. The device can act as a DHCPv6 server or DHCPv6 relay agent to help assign network configuration information to IPv6 clients.

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



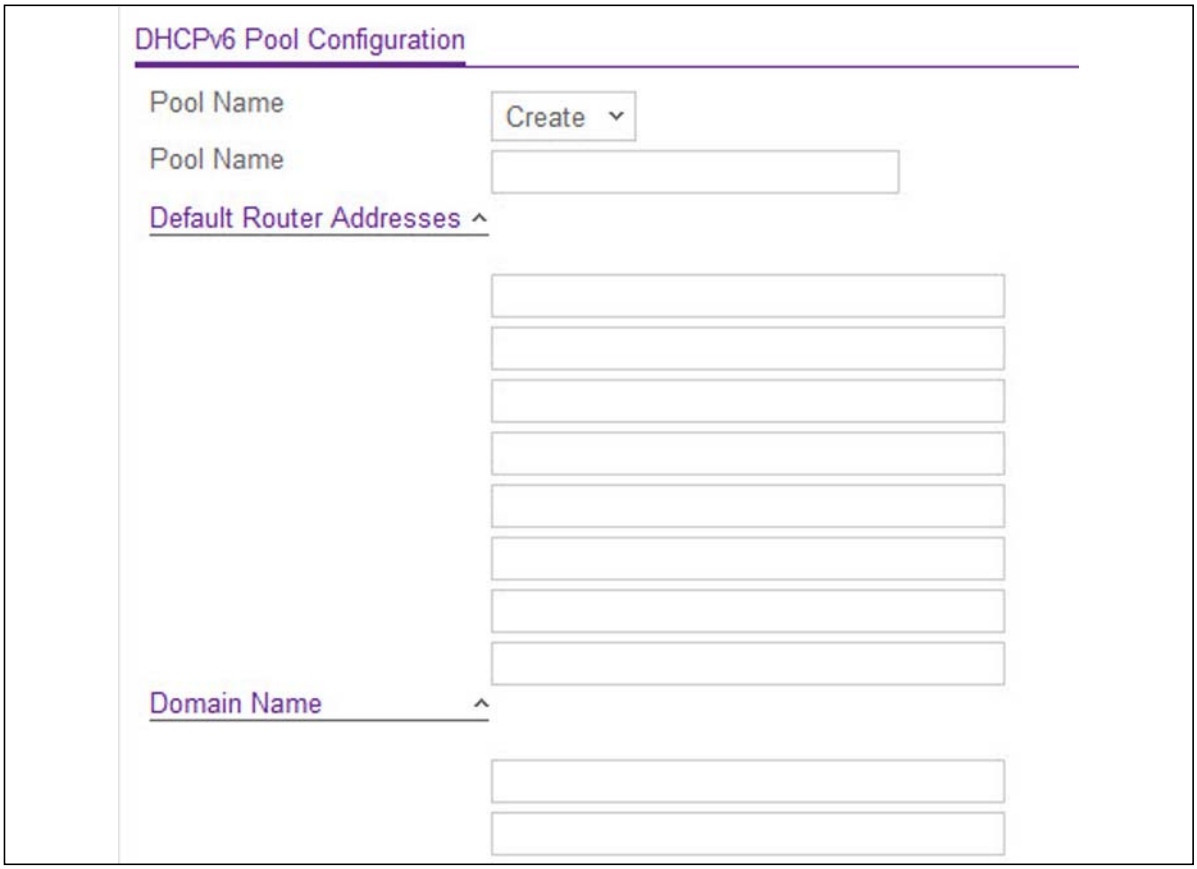
- **To enable or disable DHCP service:**

1. Use **Admin Mode** to specify whether the DHCPv6 Service administrative mode is to be Enabled or Disabled. The default value is Disable.
2. Use the **DHCPv6 Server DUID** field to specify the DHCP Unique Identifier (DUID) of the DHCPv6 server.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

DHCPv6 Pool Configuration

Use this page to view the currently configured DHCPv6 server pools as well as to add and remove pools. A DHCPv6 server pool is a set of network configuration information available to DHCPv6 clients that request the information.

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



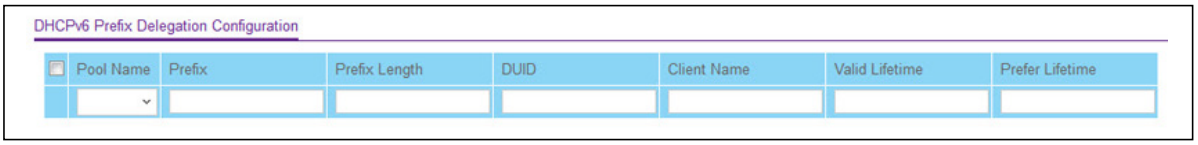
- **To configure DHCPv6 Pool settings:**

1. For a user with read/write permission, the Pool Name field shows the names of all the existing pools, along with the additional **Create** option. When the user selects **Create**, another **Pool Name** text box appears, where the user may enter a unique name that identifies the DHCPv6 server pool to be created. The name can be up to 31 alphanumeric characters in length.

   For a user with read-only permission, this **Pool Name** field would show the names of existing pools only.
2. Use the **Default Router Addresses** field to specify the list of default router addresses for the pool. The user can specify up to eight default router addresses in order of preference.
3. User the **Domain Name** field to specify the domain name for a DHCPv6 client in the pool. The domain name can be up to 255 alphanumeric characters in length.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Delete** to delete the selected pool on the switch. Configuration changes take effect immediately.

DHCPv6 Prefix Delegation Configuration

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



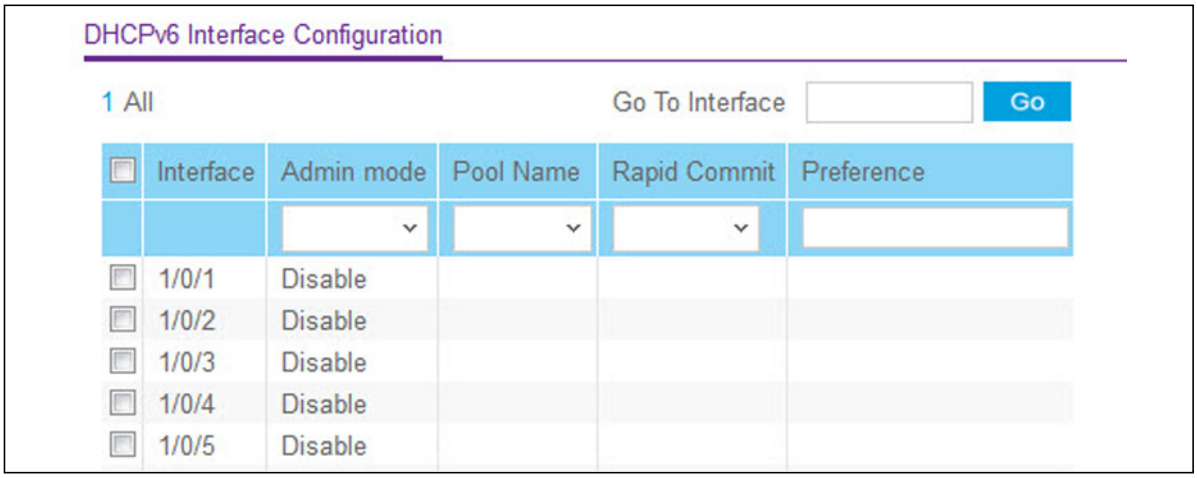
➢ **To configure DHCPv6 Prefix Delegation settings:**

1. Select from the list of configured **Pool Name**s.
2. In the **Prefix** and **Prefix Length** fields, specify the delegated IPv6 prefix.
3. In the **DUID** field, specify the DUID identifier used to identify the client's unique DUID value.
4. Specify the **Client Name**, which is useful for logging or tracing only. The name can be up to 31 alphanumeric characters.
5. Specify the **Valid Lifetime** in seconds for the delegated prefix. Valid values are 0 to 4294967295.
6. Specify the **Prefer Lifetime** in seconds for the delegated prefix. Valid values are 0 to 4294967295.
7. Click **Add** to add a new delegated prefix for the selected pool.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. Click **Delete** to delete the delegated prefix for the selected pool.

DHCPv6 Interface Configuration

Use this page to configure the per-interface settings for DHCPv6. The DHCPv6 interface modes are mutually exclusive. The fields that can be configured on this page depend on the selected mode for the interface.

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



➢ **To configure DHCPv6 Interface settings:**

1. Select the Interface with the information to view or configure. You can either:
   a. In the **Go To Interface** field, enter the interface in unit/slot/port format and click Go. The entry corresponding to the specified interface will be selected.
   b. Select the check box from the list of **Interface**s configured for DHCPv6 server functionality.
2. In the **Admin Mode** list, select to **Enable** or **Disable** DHCPv6 mode to configure server functionality. DHCPv6 server and DHCPv6 relay functions are mutually exclusive.
3. In the **Pool Name** field, specify the DHCPv6 pool containing stateless and/or prefix delegation parameters.
4. **Rapid Commit** is an optional parameter. In the **Rapid Commit** list, select to **Enable** or **Disable** allowing an abbreviated exchange between the client and server.
5. In the Preference field, specify the preference value used by clients to determine the preference between DHCPv6 servers. Valid values are 0 to 4294967295. The default value is 0.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

DHCPv6 Bindings Information

Use this page to view entries in the DHCP Bindings table. After a client acquires IPv6 configuration information from the DHCPv6 server, the server adds an entry to its database. The entry is called a binding.

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

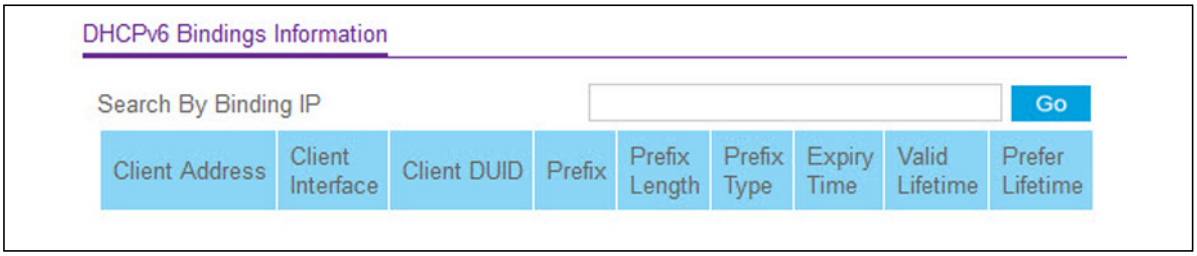


Table 35, DHCPv6 Bindings Information describes the non-configurable fields that are displayed.

Click **Update** to update the page with the latest information on the switch.

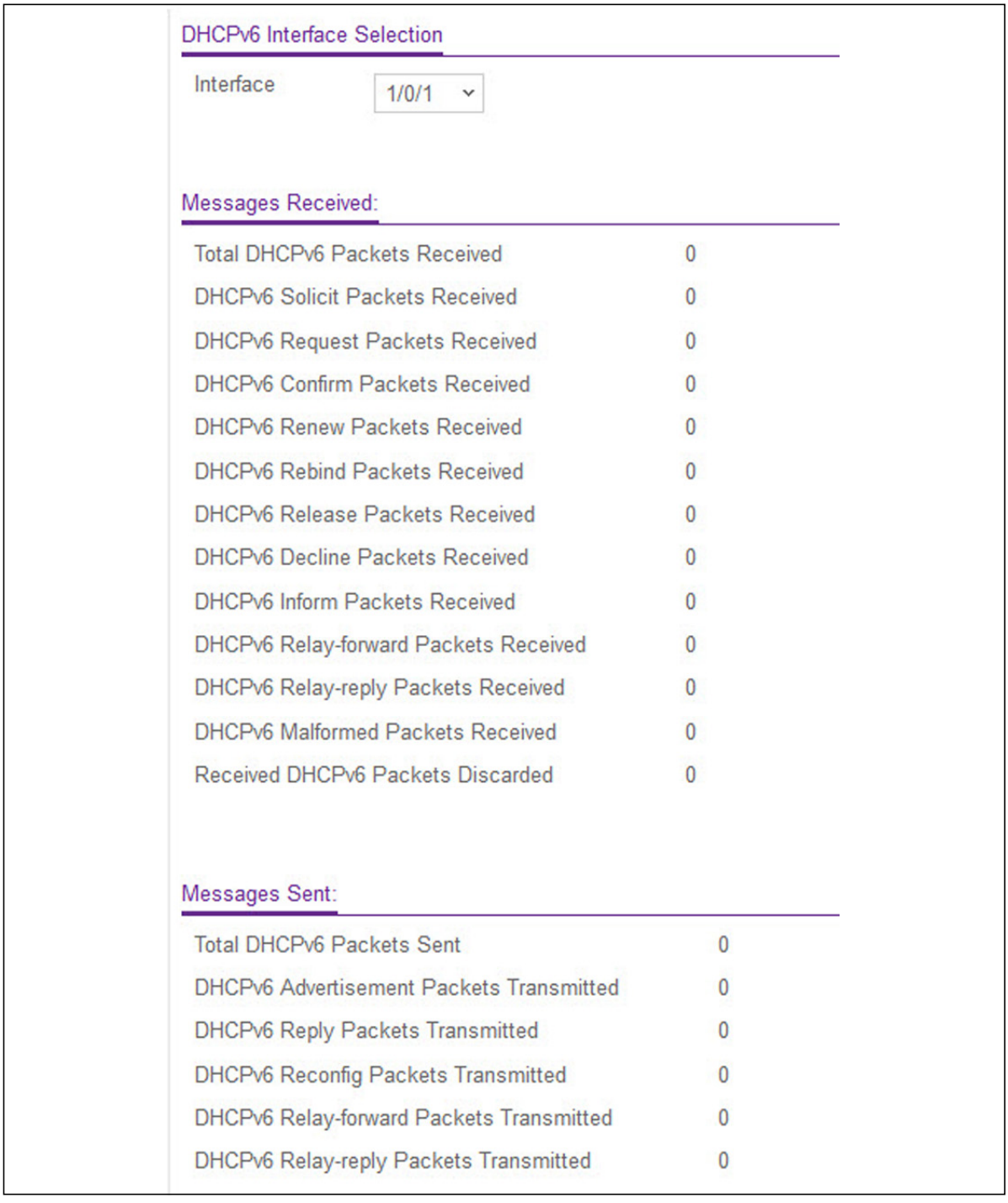
Table 35. DHCPv6 Bindings Information

Field	Description
Client Address	The IPv6 address of the client associated with the binding.
Client Interface	The interface number where the client binding occurred.
Client DUID	The DHCPv6 Unique Identifier (DUID) of the client. The DUID is a combination of the client's hardware address and client identifier.
Prefix	The IPv6 address for the delegated prefix associated with this binding.
Prefix Length	The IPv6 mask length for the delegated prefix associated with this binding.
Prefix Type	The type of IPv6 prefix associated with this binding.
Expiry Time	The number of seconds until the prefix associated with a binding expires.
Valid Lifetime	The maximum amount of time in seconds that the client is allowed to use the prefix.
Prefer Lifetime	The preferred amount of time in seconds that the client is allowed to use the prefix.

DHCPv6 Server Statistics

This page displays the DHCPv6 server statistics for the device, including information about the DHCPv6 messages, sent, received, and discarded globally and on each interface. The values on the page indicate the various counts that have accumulated since they were last cleared.

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



- **Use the buttons to perform the following tasks:**

1. To view detailed DHCPv6 statistics for an interface, from the **Interface** list select the entry for which data is to be displayed. If you select **All**, data will be shown for all interfaces.

2. To reset the DHCPv6 counters for one or more interface, select each interface with the statistics to reset and click **Clear**.
3. Click **Update** to update the page with the latest information on the switch.

Table 36, DHCPv6 Server Statistics describes the non-configurable fields that are displayed.

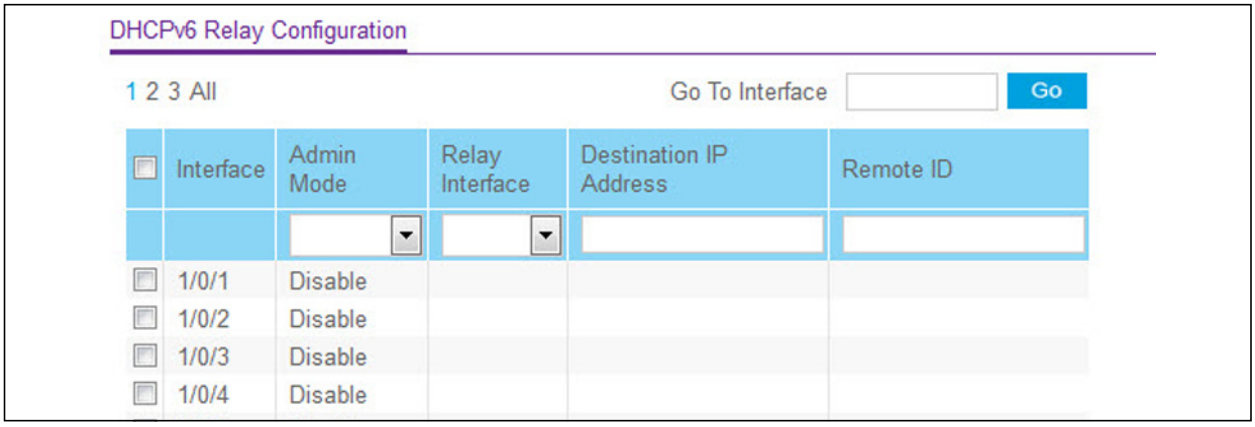
Table 36. DHCPv6 Server Statistics

Field	Description
Messages Received	Specifies the aggregate of all interface level statistics for received messages.
Total DHCPv6 Packets Received	The number of DHCPv6 messages received on the interface. The DHCPv6 messages sent from a DHCPv6 client to a DHCPv6 server include Solicit, Request, Confirm, Renew, Rebind, Release, Decline, and Information-Request messages. Additionally, a DHCPv6 relay agent can forward Relay-Forward messages to a DHCPv6 server.
DHCPv6 Solicit Packets Received	The number of DHCPv6 Solicit messages received on the interface. This type of message is sent by a client to locate DHCPv6 servers.
DHCPv6 Request Packets Received	Specifies the number of Requests.
DHCPv6 Confirm Packets Received	The number of DHCPv6 Confirm messages received on the interface. This type of message is sent by a client to all DHCPv6 servers to determine whether its configuration is valid for the connected link.
DHCPv6 Renew Packets Received	The number of DHCPv6 Renew messages received on the interface. This type of message is sent by a client to extend and update the configuration information provided by the DHCPv6 server.
DHCPv6 Rebind Packets Received	The number of DHCPv6 Rebind messages received on the interface. This type of message is sent by a client to any DHCPv6 server when it does not receive a response to a Renew message.
DHCPv6 Release Packets Received	The number of DHCPv6 Release messages received on the interface. This type of message is sent by a client to indicate that it no longer needs the assigned address.
DHCPv6 Decline Packets Received	The number of DHCPv6 Decline messages received on the interface. This type of message is sent by a client to the DHCPv6 server to indicate that an assigned address is already in use on the link.
DHCPv6 Inform Packets Received	The number of DHCPv6 Information-Request messages received on the interface. This type of message is sent by a client to request configuration information other than IP address assignment.
DHCPv6 Relay-forward Packets Received	The number of DHCPv6 Relay-Forward messages received on the interface. This type of message is sent by a relay agent to forward messages to servers.
DHCPv6 Relay-reply Packets Received	The number of DHCPv6 Relay-Reply messages received on the interface. This type of message is sent by a server to a DHCPv6 relay agent and contains the message for the relay agent to deliver to the client.

Field	Description
DHCPv6 Malformed Packets Received	The number of DHCPv6 messages that were received on the interface but were dropped because they were malformed.
Received DHCPv6 Packets Discarded	Specifies the number of Packets Discarded.
Messages Sent	Specifies the aggregate of all interface level statistics for messages sent.
Total DHCPv6 Packets Sent	The number of DHCPv6 messages sent by the interface. The DHCPv6 messages sent from a DHCPv6 server to a DHCPv6 client include Advertise, Reply, Reconfigure, and Relay-Reply messages.
DHCPv6 Advertisement Packets Transmitted	The number of DHCPv6 Advertise messages sent by the interface. This type of message is sent by a server to a DHCPv6 client in response to a Solicit message and indicates that it is available for service.
DHCPv6 Reply Packets Transmitted	The number of DHCPv6 Reply messages sent from the interface to a DHCPv6 client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.
DHCPv6 Reconfig Packets Transmitted	The number of DHCPv6 Reconfigure messages sent by the interface. This type of message is sent by a server to a DHCPv6 client to inform the client that the server has new or updated information. The client then typically initiates a Renew/Reply or Information-request/Reply transaction with the server to receive the updated information.
DHCPv6 Relay-forward Packets Transmitted	The number of DHCPv6 Relay-Forward messages sent by the interface. This type of message is sent by a relay agent to forward messages to servers.
DHCPv6 Relay-reply Packets Transmitted	The number of DHCPv6 Relay-Reply messages sent by the interface. This type of message is sent by a server to a DHCPv6 relay agent and contains the message for the relay agent to deliver to the client.

DHCPv6 Relay

The **System > Services > DHCPv6 Relay** navigation contains links to the following web page that configures and displays DHCPv6 Relay functionality.



➢ **Use the buttons to perform the following tasks:**

1. To configure DHCPv6 Relay for an interface, select the Interface with the information to view or configure. You can either:
   a. In the **Go To Interface** field, enter the interface in unit/slot/port format and click Go. The entry corresponding to the specified interface will be selected.
   b. Select the check box from the list of **Interface**s configured for DHCPv6 Relay functionality.
2. In the **Admin Mode** field, specify the DHCPv6 mode, either Enable or Disable, to configure DHCPv6 Relay functionality. The default is Disable. DHCPv6 server and DHCPv6 relay functions are mutually exclusive.
3. From the Relay Interface menu, select an interface to reach a relay server.
4. In the Destination IP Address, specify an IPv6 address to reach a relay server.
5. In the Remote ID field, specify the relay agent information option. The Remote ID needs to be derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.
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.

Chassis

Use the **Chassis** screen to move the Primary Management Unit (Supervisor) functionality from one blade to another. When applied, the entire chassis (including all interfaces in the chassis) is unconfigured and reconfigured with the configuration on the new Primary Management Unit. After the reload is complete, all chassis management capability must be performed on the new Primary Management Unit. To preserve the current configuration across a chassis move, save the current configuration to the nvram before performing the chassis move. A chassis move causes all routes and Layer 2 addresses to be lost. The system prompts the administrator to confirm the management move before the changes are applied.

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

- *Basic Chassis Configuration* on page 79
- *Advanced Chassis Configuration* on page 82
- *NSF* on page 92

Basic Chassis Configuration

➢ **To select the Management Unit:**

1. Click **System** > **Chassis > Basic > Chassis Configuration.**
2. Select the **Management Unit**. The Management Unit Selection field displays the Current Primary Management Unit. You can change it by selecting another blade ID listed here.

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

Note: The Move Management operation may cause a change in the system IP address when the IP address is assigned by a DHCP server.

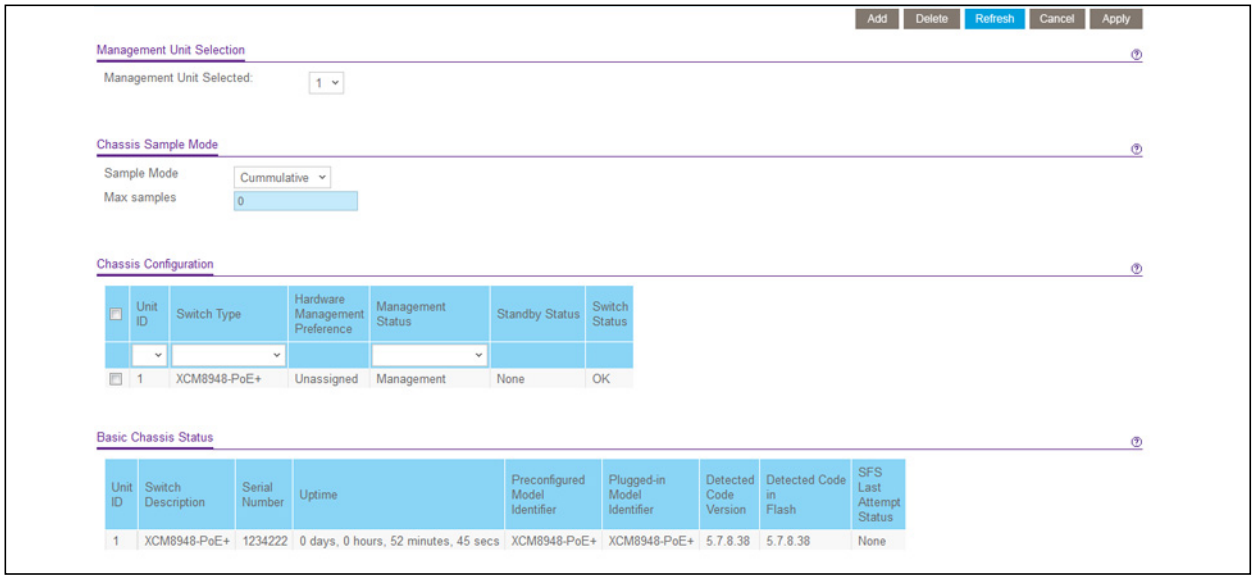


Figure 12. Chassis Configuration

➢ **To configure the global status management mode and sample size:**

1. Select the **Chassis Sample Mode**. The global status management mode which can be:
   - **Cumulative.** This tracks the sum of received time stamp offsets cumulatively.
   - **History**. This tracks the history of received timestamps.
2. Enter a value for **Max Samples** – the maximum number of samples to keep. The valid range is 100 to 500. **Max Samples** applies to **History** mode.
3. Click the **Cancel** button to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. Click the **Apply** button to send the updated configuration to the switch. The mode and sample size parameters are applied globally to all units in the chassis. Configuration changes take effect immediately.

➢ **To configure the chassis:**

1. Select the **Unit ID** from the displayed list of blades.
2. Specify the **Switch Type** - the type of blade hardware when creating a new blade in the chassis.

3. Select the **Management Status.** Indicates whether the selected switch is the management unit, or a normal chassis member, or on standby.
4. Click the **Apply** button. The system prompts the administrator to confirm the management move. Upon administrator confirmation, the entire chassis, including all interfaces in the chassis, is unconfigured and reconfigured with the configuration on the new Primary Management Unit. Configuration changes take place immediately.
5. Click the **Cancel** button to cancel the configuration on the screen. The data on the screen is reset to the latest value of the switch.
6. Click **Update** to update the page with the latest information on the switch.
7. After the reload is complete, all chassis management capability must be performed on the new Primary Management Unit.

The following table describes the non-configurable fields on the **Chassis Configuration** page.

Table 37. Chassis Configuration

Field	Description
Hardware Management Preference	The hardware management preference of the blade. The hardware management preference can be disabled or unassigned.
Standby Status	Identifies the switch that is configured as the Standby Unit. The possible values are: • **Cfg Standby**. Indicates that the blade is configured as the Standby blade. The blade configured as the Standby blade becomes the supervisor if the current supervisor fails. • **Opr Standby**. Indicates that this blade is operating as the Standby.
Switch Status	Displays the status of the selected unit. The possible values are: • **OK** • **Unsupported** • **Code Mismatch** • **Config Mismatch** • **Not Present** • **SDM Mismatch** • **Updating Code**

The following table describes the non-configurable fields in the **Basic Chassis Status**.

Table 38. Basic Chassis Status

Field	Description
Unit ID	The Unit ID of the specific blade.
Switch Description	The description for the blade that can be configured by the user.

Field	Description
Serial Number	The unique box serial number for this blade.
Uptime	Displays the relative time since the last reboot of the blade.
Preconfigured Model Identifier	Displays the model type assigned by the device manufacturer to identify the device.
Plugged-in Model Identifier	Displays the model type assigned by the device manufacturer to identify the plugged-in device.
Detected Code Version	Indicates the detected version of code on this blade.
Detected Code in Flash	Displays the Release number and version number of the code stored in flash.
SFS Last Attempt Status	Displays the Stack Firmware Synchronization last attempt status.

Click **Update** to update the page with the latest information on the switch.

Advanced Chassis Configuration

Advanced > **Chassis Configuration** uses the same screen as **Basic** > **Chassis Configuration** described above.

Chassis Status

➢ **Use the Chassis Status page to display chassis protocol information:**

1. Click **System** > **Chassis > Advanced > Chassis Status.**
2. Select either the **Unit ID** or **All**.
   - Select the **Unit ID** field to display information for the selected unit.
   - Select **All** to display information for all units.

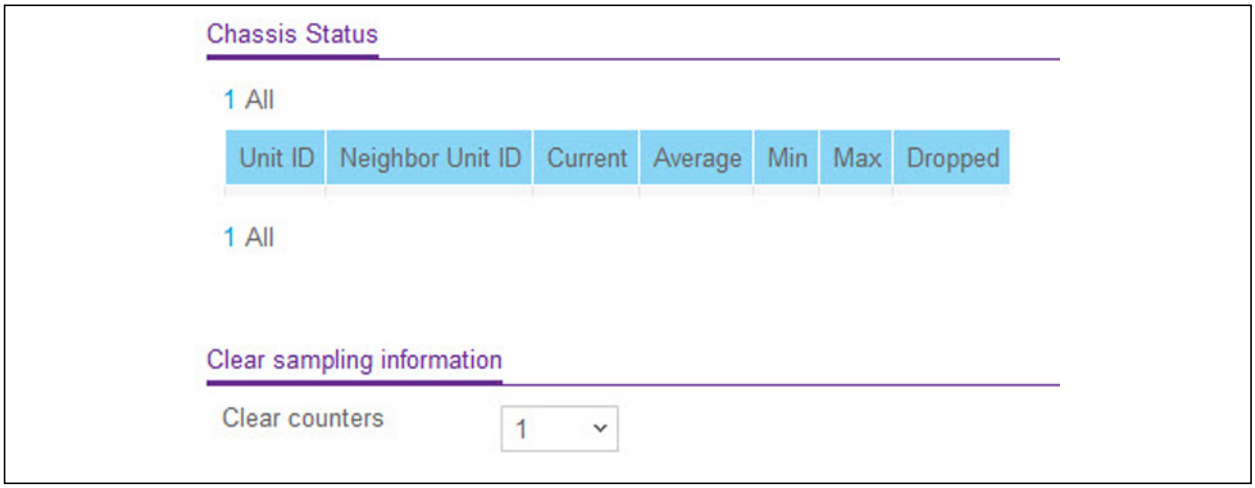


Figure 13. Display Chassis Status

The following table describes the non-configurable **Advanced Chassis Status** data that is displayed.

Table 39. Advanced Chassis Status

Field	Description
Unit ID	The Unit ID of the specific blade.
Neighbor Unit ID	The neighboring blade with which data is exchanged.
Current	Current time of heartbeat message reception.
Average	Average time of heartbeat messages received.
Min	Minimum time of heartbeat messages received.
Max	Maximum time of heartbeat messages received.
Dropped	Heartbeat message dropped or lost counter.

➢ **To clear the sampling information:**

The chassis sampling parameters are configured on the **Chassis Status** page.

1. Click **System** > **Chassis > Advanced > Chassis Status** to display the sampling table. See *Figure 13*.

In the **Clear sampling information** > **Clear counters** field, select the unit to clear the counters. Possible choices are **None**, a **unit ID** number, or **All**.

Chassis Backplane-port Configuration

➢ **To display Backplane-port Configuration:**

1. Click **System** > **Chassis > Advanced > Backplane-port Configuration.**
2. Select either the **Unit ID** or **All**.
   - Select the **Unit ID** field to display information for the selected unit.
   - Select **All** to display information for all units.

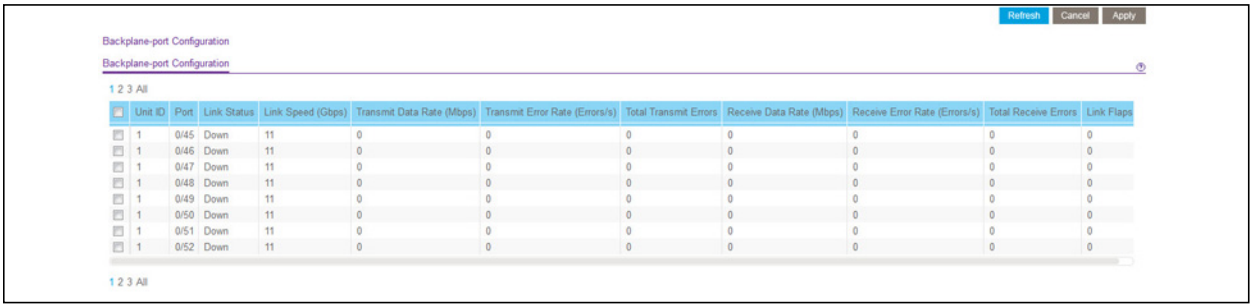


Figure 14. Backplane-Port Configuration

The following table describes the non-configurable **Backplane-port Configuration** data that is displayed.

Table 40. Backplane-Port Configuration

Field	Description
Unit ID	The Unit ID of the specific blade.
Port	Displays the backplane-port on the given blade.
Link Status	Displays the link status (Up/Down) of the port.
Link Speed (Gbps)	Displays the maximum speed of the backplane-port.
Transmit Data Rate (Mbps)	Displays the approximate transmit rate on the backplane-port.
Transmit Error Rate (Error/s)	Displays the number of errors in transmit packets per second.
Total Transmit Errors	Displays the total number of errors in transmit packets since bootup. The counter may wrap.
Receive Data Rate (Mbps)	Displays the approximate receive rate on the backplane-port.
Receive Error Rate (Error/s)	Displays the number of errors in receive packets per second.
Total Receive Errors	Displays the total number of errors in receive packets since bootup. The counter may wrap.
Link Flaps	Displays a backplane-port counter that increments whenever a backplane-port link transitions to the down state.

- Click **Update** to update the page with the latest information on the switch.
- Click the **Cancel** button to cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch.
- Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

Chassis Backplane-port Diagnostics

➢ **To display Backplane-port diagnostics:**

Use the Backplane-port Diagnostics page to display low-level statistics such as APT counts and RPC counts, etc. for all the backplane-ports in the given chassis.

1. Click **System** > **Chassis > Advanced > Backplane-port Diagnostics.**
2. Select either the **Unit ID** or **All**.
   - Select the **Unit ID** field to display information for the selected unit.
   - Select **All** to display information for all units.

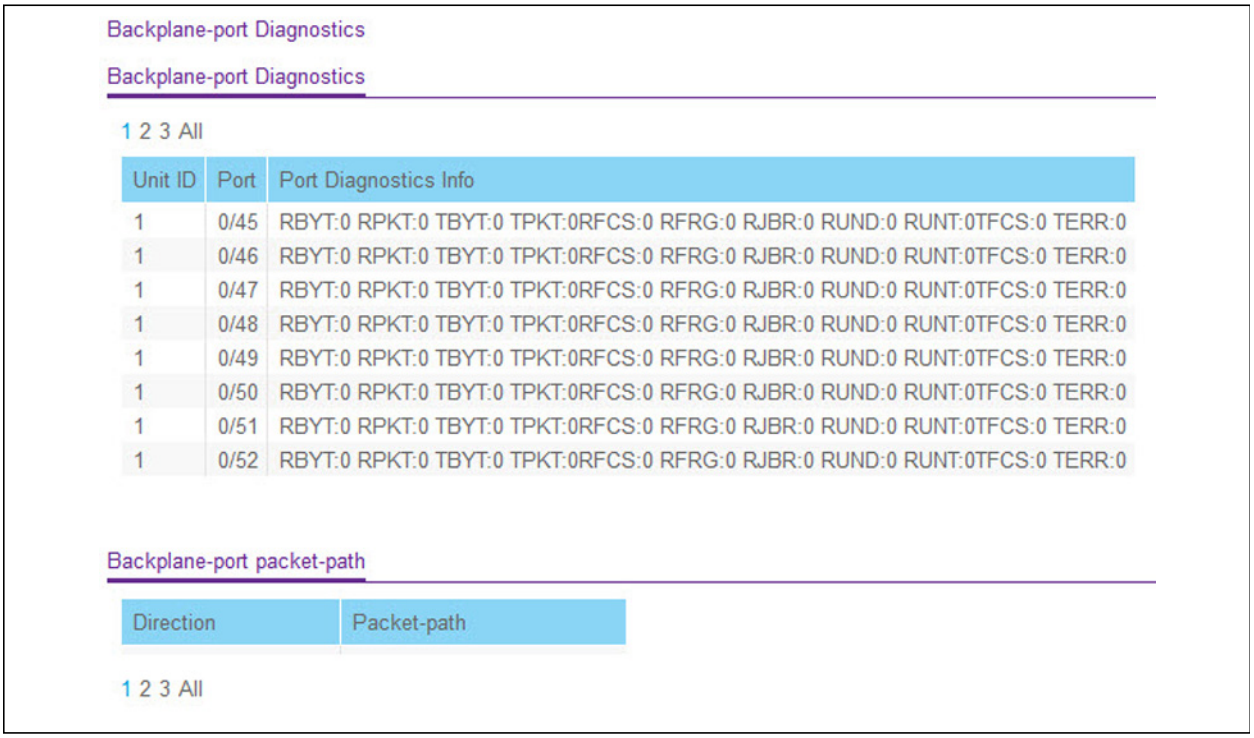


Figure 15. Backplane-Port Diagnostics

The following table describes the non-configurable **Backplane-port Diagnostics** data that is displayed.

Table 41. Backplane-Port Diagnostics

Field	Description
Unit ID	The slot number of the blade.
Port	Displays the backplane-port on the given blade.
Port Diagnostics Info	Displays three text fields (character strings) populated by the driver containing debug and status information. The Port Diagnostics information contains hardware counters; counter values are displayed in hexadecimal digits.

Click **Update** to update the page with the latest information on the switch.

➢ **To display Backplane-Port Packet-Path:**

1. Click **System** > **Chassis > Advanced > Backplane-port Diagnostics** to display the **Blackplane-port packet-path** fields**.**
2. To navigate, select either the **Unit ID** or **All**.
   - Select the **Unit ID** field to display the packet path starting from the selected blade.
   - Select **All** to display the packet path starting from all the blades of the chassis.

The following table describes the non-configurable **Backplane-port packet-path** data that is displayed.

Table 42. Backplane-port Packet-path

Field	Description
Direction	Displays the path direction.
Packet-path	Displays the packet path.

Click **Update** to update the page with the latest information on the switch.

Chassis Power Configuration

➢ **To configure chassis power:**

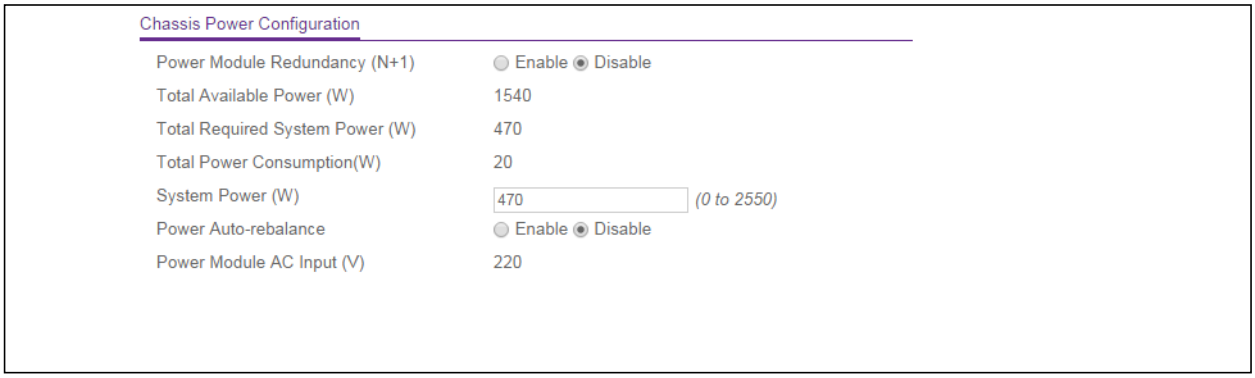


Figure 16. Chassis Power Configuration

1. Click **System > Chassis > Advanced > Chassis Power Configuration**.
2. In the Power Module Redundancy field, specify whether power redundancy mode is **Enabled** or **Disabled**.
3. Click the **Apply** button to apply the power redundancy mode.
4. Click **Update** to update the page with the latest information on the switch.

➢ **To configure system power:**

1. Click **System > Chassis > Advanced > Chassis Power Configuration**.
2. In the **System Power** field, specify the power reserved for system, excluding PoE power.

   This provides a way to reserve power for blades. The remaining power can be used by a PoE sub system. System Power should be less than or equal to 2550W. Use 0 to reset System Power to defaults.
3. Click the **Apply** button to apply the system power.

➢ **To configure power auto-rebalance:**

1. Click **System > Chassis > Advanced > Chassis Power Configuration**.
2. In the **Power Auto-rebalance** field, specify whether power auto-rebalance mode is **Enabled** or **Disabled**.
3. Click the **Apply** button to apply the power auto-rebalance mode.

   When enabled, the system automatically shuts down low priority ports to power up higher priority ports, even if they were spread across different blades on the chassis.

   The following table describes the non-configurable Chassis Power Configuration data that is displayed.

Table 43. Chassis Power Configuration

Field	Description
Total Available Power	Total available power for chassis in watts.
Total Required System Power	Total required system power in watts. Value depends on the type of blades on the chassis. Refer to "Power Matrix" or "Blade Power Consumption" table for power requirements of each blade type.
Total Power Consumption	Total power consumption in watts measured at PSU
Power Module AC Input	Power module input voltage in volts. Possible values are 110 and 220.

➢ **To display Blade Power Consumption:**

1. Click **System > Chassis > Advanced > Chassis Power Configuration**.

   The following table describes the non-configurable Blade Power Consumption data that is displayed.

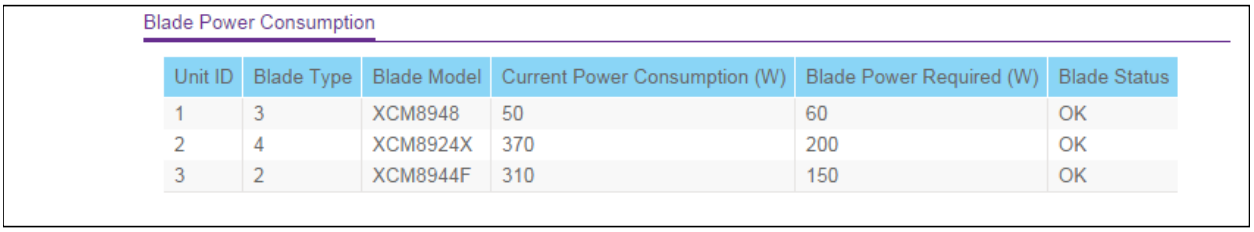


Figure 17. Blade Power Consumption

Table 44. Chassis Power Modules

Field	Description
Unit ID	Displays the Unit ID that identifies the blade slot.
Blade Type	Displays blade type number.
Blade Model	Displays blade model.

Field	Description
Current Power Consumption	Displays amount of power required by blade (excluding PoE power) in watts.
Blade Power Required	Displays amount of power required by blade (excluding PoE power) in watts.
Blade Status	Displays blade status. The possible values are: • OK • Booting up • Bootup Failed • Thermal Shutdown • SW Power Down • Not Enough Power • Unknown Blade • Absent

➢ **To display Power Redundancy:**

1. Click **System > Chassis > Advanced > Chassis Power Configuration**.

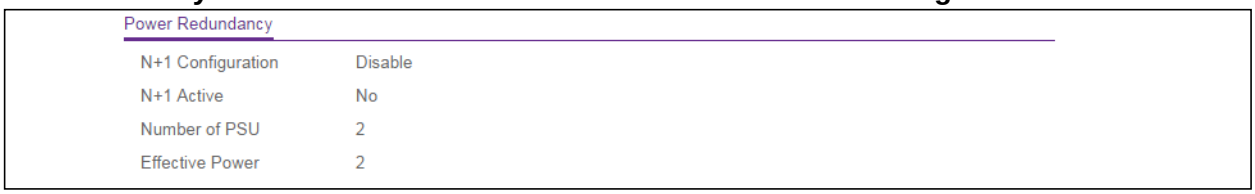


Figure 18. Power Redundancy

The following table describes the non-configurable Power Redundancy data that is displayed.

Table 45. Power Redundancy

FIeld	Description
N+1 Configuration	Power redundancy configuration. Possible values are **Enable** and **Disable**.
N+1 Active	Displays whether power supply N+1 redundancy is active on the chassis.
Number of PSU	Total number of active PSUs in chassis.
Effective Power	Effective number of PSUs in the chassis after factoring N+1 active state. Value will be one less than Number of PSU when N+1 is active on the chassis.

➢ **To display Power Modules:**

1. Click **System > Chassis > Advanced > Chassis Power Configuration**.

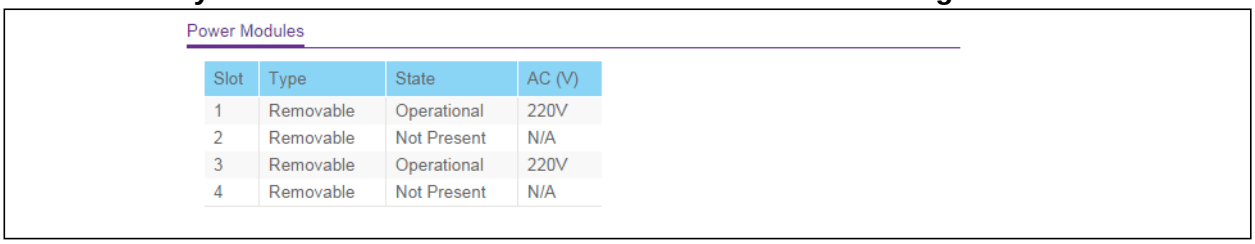


Figure 19. Power Modules

The following table describes the non-configurable Power Module data that is displayed.

Table 46. Power Modules

Field	Description
Slot	Power module number counted from left to right.
Type	Power module type. Valid values are Fixed or Removable.
State	Power module state. Possible states are: • Operational • Failed • Not Present • Not Powered • Not Applicable
AC	Power module input voltage category in volts. Possible values are 110V, 220V and N/A. N/A specifies that power source input voltage cannot be obtained.

➢ **To display EPS power modules:**

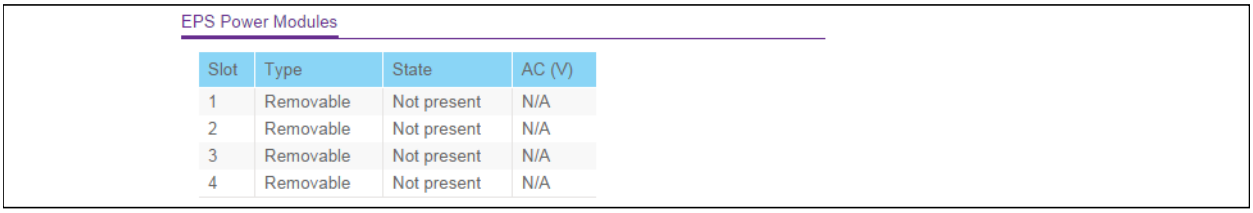


Figure 20. Chassis Power EPS

1. Click **System** > **Chassis > Advanced > Chassis Power Configuration.**

The following table describes the non-configurable EPS power module data that is displayed.

Table 47. EPS Power Modules

Field	Description
Slot	EPS power module number counted from left to right.
Type	EPS power module type. Valid value is Removable.
State	EPS Power module state. Possible states are: • Operational • Not Present
AC	EPS power module input voltage category in volts. Possible values are 110V, 220V and N/A. N/A specifies that power source input voltage cannot be obtained.

➢ **To display EPS ports:**

1. Click **System > Chassis > Advanced > Chassis Power Configuration**.

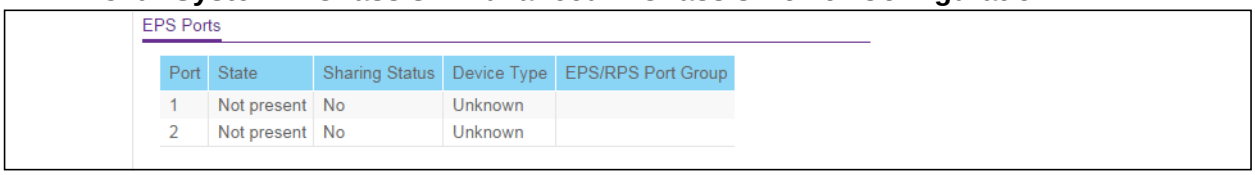


Figure 21. EPS Ports

The following table describes the non configurable EPS Ports data that is displayed.

Table 48. EPS Ports

Field	Description
Ports	EPS port number counted from left to right while facing rear side of the chassis.
State	EPS port state. Possible state is Not present or Operational.
Sharing Status	EPS power sharing status.
Device Type	Device type. Possible values are: • RPS4000v1 • RPS4000v2 • Unknown
EPS/RPS Port Group	Group of EPS slots connected to this port. Possible values are: • 1,2 • 3,4

➢ **To display Power Matrix:**

1. Click **System > Chassis > Advanced > Chassis Power Configuration**.

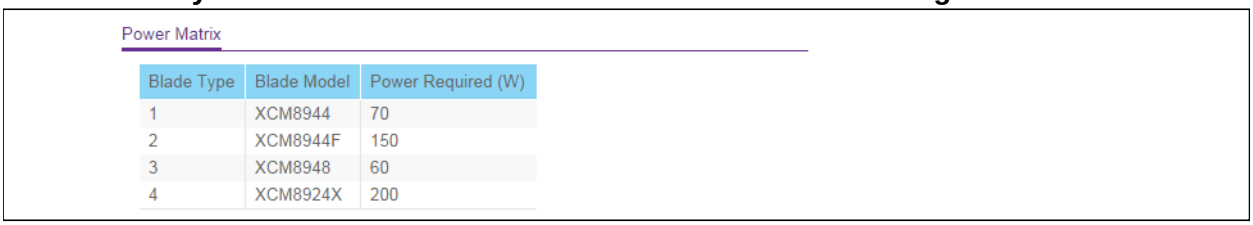


Figure 22. Power Matrix

The following table describes the non-configurable Power Matrix data that is displayed.

Table 49. Power Matrix

Field	Description
Blade Type	The 4-bit identification number assigned to a blade.
Blade Model	Blade model.
Power Required	Maximum consumption by blade in watts (excluding PoE power).

Chassis Power Configuration

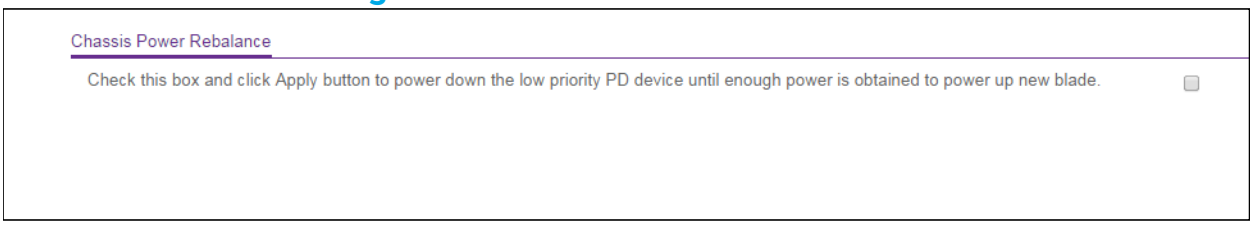


Figure 23. Rebalance Chassis Power

➢ **To rebalance the chassis power:**

1. Click **System > Chassis > Advanced > Chassis Power Rebalance**.
2. Click the checkbox.
3. Click the Apply button to power down the low priority PD device until enough power is obtained to power up new blade or higher priority PoE port on different blade.

Chassis Firmware Synchronization

➢ **To configure Chassis Firmware Synchronization:**

1. Click **System > Chassis > Advanced > Chassis Firmware Synchronization.**
2. In the Chassis Firmware Auto Upgrade field, specify whether the Firmware Synchronization feature is **Enabled** or **Disabled**. The default is **Disabled**.
3. In the Traps field, **Enable** or **Disable** the sending of traps during Chassis Firmware Synchronization Start, Failure, and Finish. The default is **Enabled**.
4. In the Allow Downgrade field, **Enable** or **Disable** downgrading the image on a chassis member if the chassis member's version is newer. The default is **Enabled**.

5. Click **Update** to update the page with the latest information on the switch.
6. Click the **Cancel** button to cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch.
7. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

NSF

➢ **To display NSF Summary data:**

1. Click **System** > **Chassis > NSF > NSF Summary.**
2. The following screen is displayed.

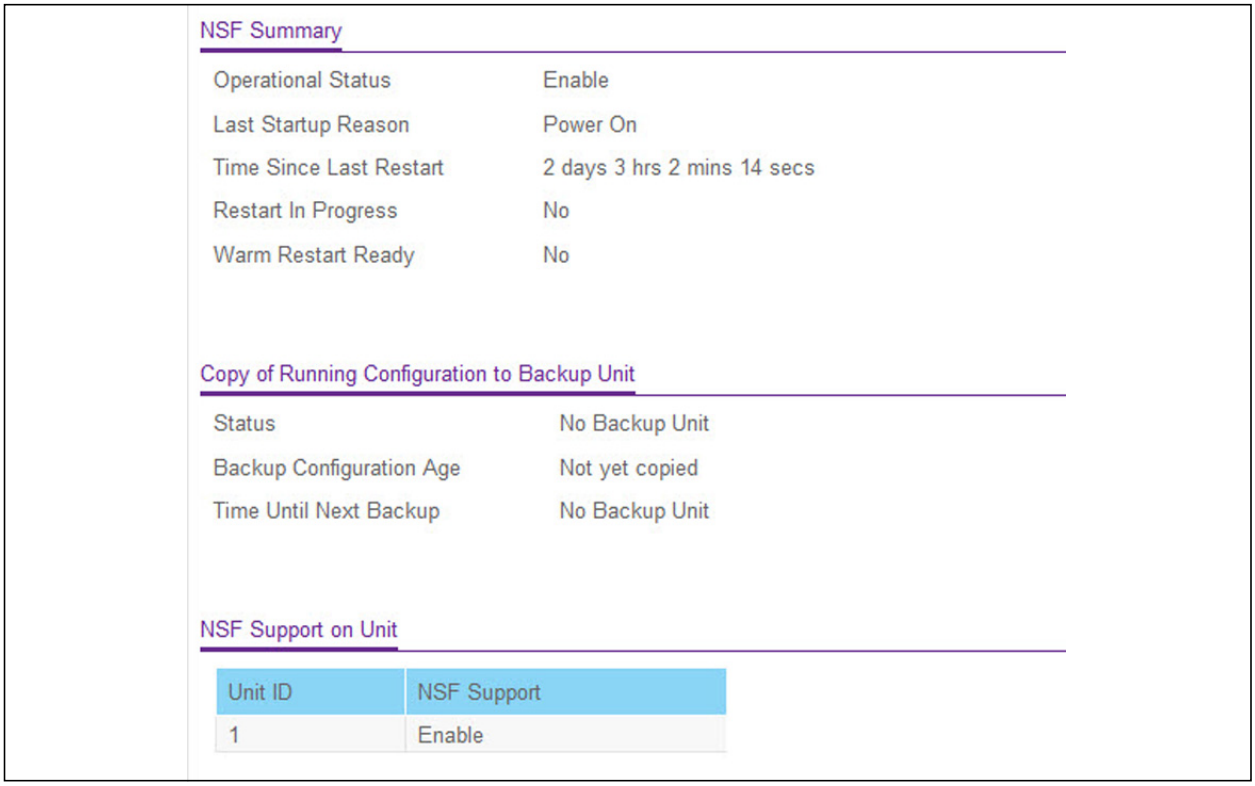


Figure 24. NSF Summary

The following table describes the non-configurable **NSF Summary** data that is displayed.

Table 50. NSF Summary

Field	Description
Operational Status	Indicates whether NSF is enabled on the chassis. NSF is enabled by default.
Last Startup Reason	The type of activation that caused the software to start the last time. The possible values are: • Power On—The switch is rebooted. This could have been caused by a power cycle or by an administrative Reload command. • Cold Admin Move—The system resets all hardware tables without a reboot and the application begins from a pre-initialized state, but no data is retained from before the failover. • Warm Admin Move—The administrator issued a command for the standby manager to take over. • Auto Warm—The primary management card restarted due to a failure, and the system executed a nonstop forwarding failover. • Auto Cold—The system switched from the active manager to the backup manager and was unable to maintain user data traffic. This is usually caused by multiple failures occurring close together.
Time Since Last Restart	Time since the current management card because the active management card. For backup manager, the value is set to 0d:00:00:00.
Restart In Progress	Indicates whether a restart is in progress. A restart is not considered complete until all hardware tables have been fully reconciled.
Warm Restart Ready	Indicates whether the initial full checkpoint has finished.
Copy of Running Configuration to Backup Unit	
Status	Status of copying running configuration to backup blades.
Backup Configuration Age	Indicates the time since the running configuration was last copied to the backup blade.
Time Until Next Backup	Indicates the number of seconds until the running configuration will be copied to the backup blade.
NSF Support on Unit	
Unit ID	Displays the slot number for the blade.
NSF Support	Displays whether the switch supports the Non-Stop Forwarding (NSF) feature.

3. Click **Initiate Failover** to cause the supervisor unit to fail over to the backup blade.
4. Click **Update** to update the page with the latest information on the switch.

NSF Checkpoint Statistics

➢ **To display NSF Checkpoint Statistics:**

1. Click **System** > **Chassis > NSF > Checkpoint Statistics.**
2. Click **Clear** to reset the statistics on the page.
3. Click **Update** to update the page with the latest information on the switch.

The following table describes the non-configurable data that is displayed.

Table 51. NSF Checkpoint Statistics

Field	Description
Messages Checkpoint	Displays the number of messages sent from the Supervisor to the backup blade.
Bytes Checkpointed	Displays how much data has been sent from the Supervisor until to the backup blade.
Time Since Counters Cleared	Displays the amount of time since the counters have been reset.
Checkpoint Message Rate	Indicates the number of seconds between measurements.
Last 10-second Message Rate	Indicates how many messages have been sent in the last measurement interval.
Highest 10-second Message Rate	Indicates the highest number of messages that have been sent in a measurement interval.

PoE

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

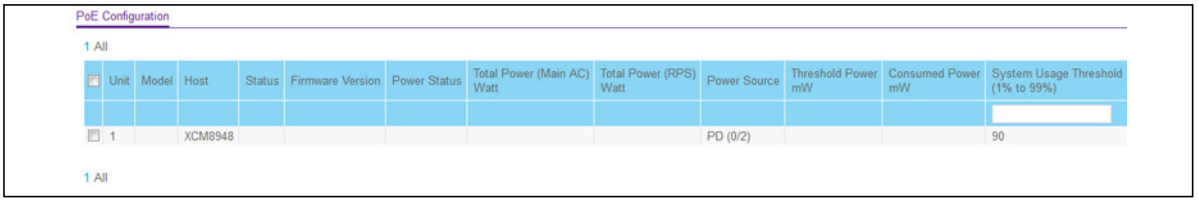
From the PoE link, you can access the following pages:

- *Basic* on page 94
- *Advanced* on page 96

Basic

Use the Basic page to configure the basic PoE settings.

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



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.

Table 52. 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 power up 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 traps, select **Enable** to activate the PoE traps. Select **Disable** to deactivate the PoE traps. The default setting is enabled.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Advanced

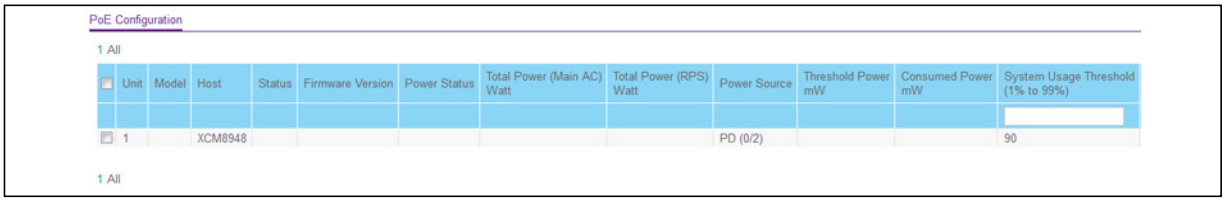
Use the Advanced page to configure the advanced PoE settings.

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

- *PoE Configuration* on page 96
- *PoE Port Configuration* on page 97

PoE Configuration

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



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.

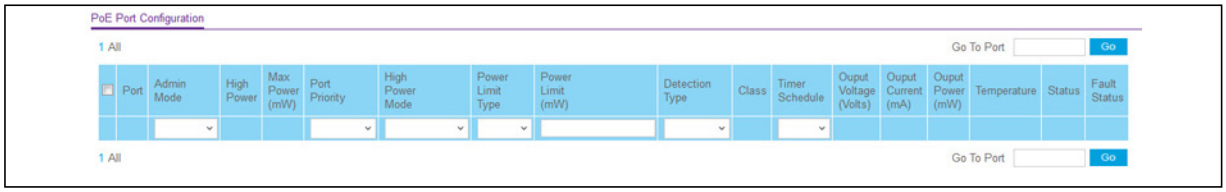
Table 53.

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 power up one port, if consumed power is less than this power. i.e. Consumed power can be between Nominal and Threshold Power values. The threshold power value is effected by changing System Usage Threshold.
Consumed Power	Total amount of a power which is currently being delivered to all ports.

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 traps, select **Enable** to activate the PoE traps. Select **Disable** to deactivate the PoE traps. The default setting is enabled.
5. 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** > **PoE** > **Advanced** > **PoE Port Configuration**. A screen similar to the following is displayed.



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 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 power up.
   - **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 reset 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.

Table 54.

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.

Table 54.

Field	Description
Output Current	Current being delivered to device in mA.
Output Power	Current power being delivered to device in Watts.
Status	The status is the operational status of the port PD detection. • Disabled - indicates no power being delivered. • DeliveringPower - indicates power is being drawn by device. • Fault - indicates a problem with the port. • Test - indicates port is in test mode. • otherFault - indicates port is idle due to error condition. • Searching - indicates port is not in one of the above states.
Fault Status	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.

SNMP

From the 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:

- *SNMP V1/V2* on page 99
- *SNMP V3* on page 104

SNMP V1 / V2

The pages under the SNMP V1/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 100
- *Trap Configuration* on page 101
- *Trap Flags* on page 102

- *Supported MIBs* on page 103

Community Configuration

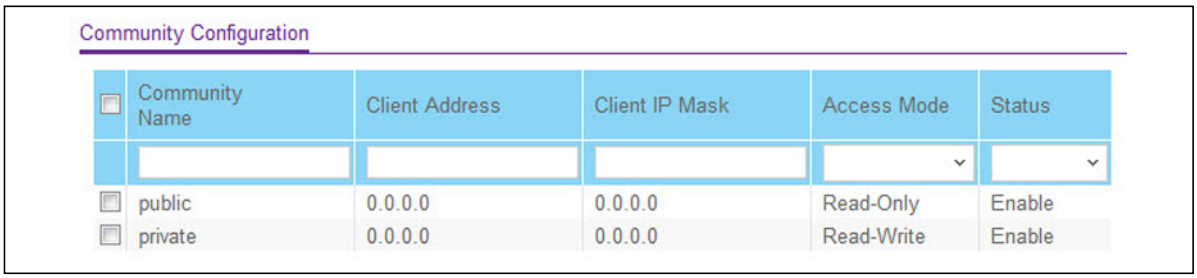
By default, two SNMP Communities exist:

- 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 SNMP V1 and SNMP V2 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 SNMP V1 and SNMP V2 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 is displayed.

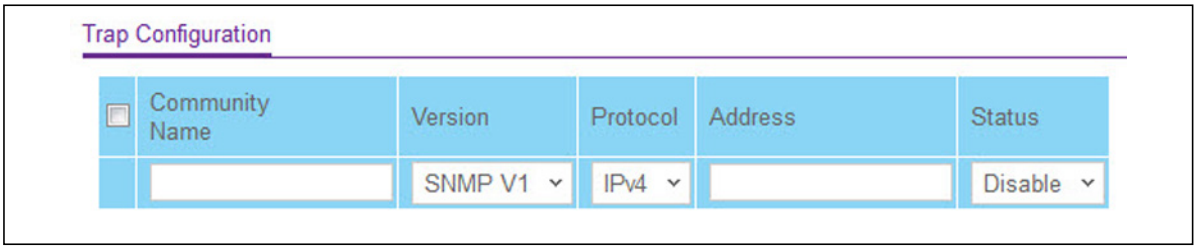


1. Use **Community Name** to reconfigure an existing community, or to create a new one. Use this menu to select one of the existing community names, or select 'Create' to add a new one. A valid entry is a case-sensitive string of up to 16 characters.
2. **Client Address** - Taken together, the Client 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 menu.
5. Use **Status** to specify the status of this community by selecting Enable or Disable from the menu. If you select enable, the Community Name must be unique among all valid Community Names or the set request will be rejected. If you select disable, the Community Name will become invalid.
6. Click **Add** to add the currently selected community to the switch.
7. Click **Delete** to delete the currently selected Community Name.

Trap Configuration

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

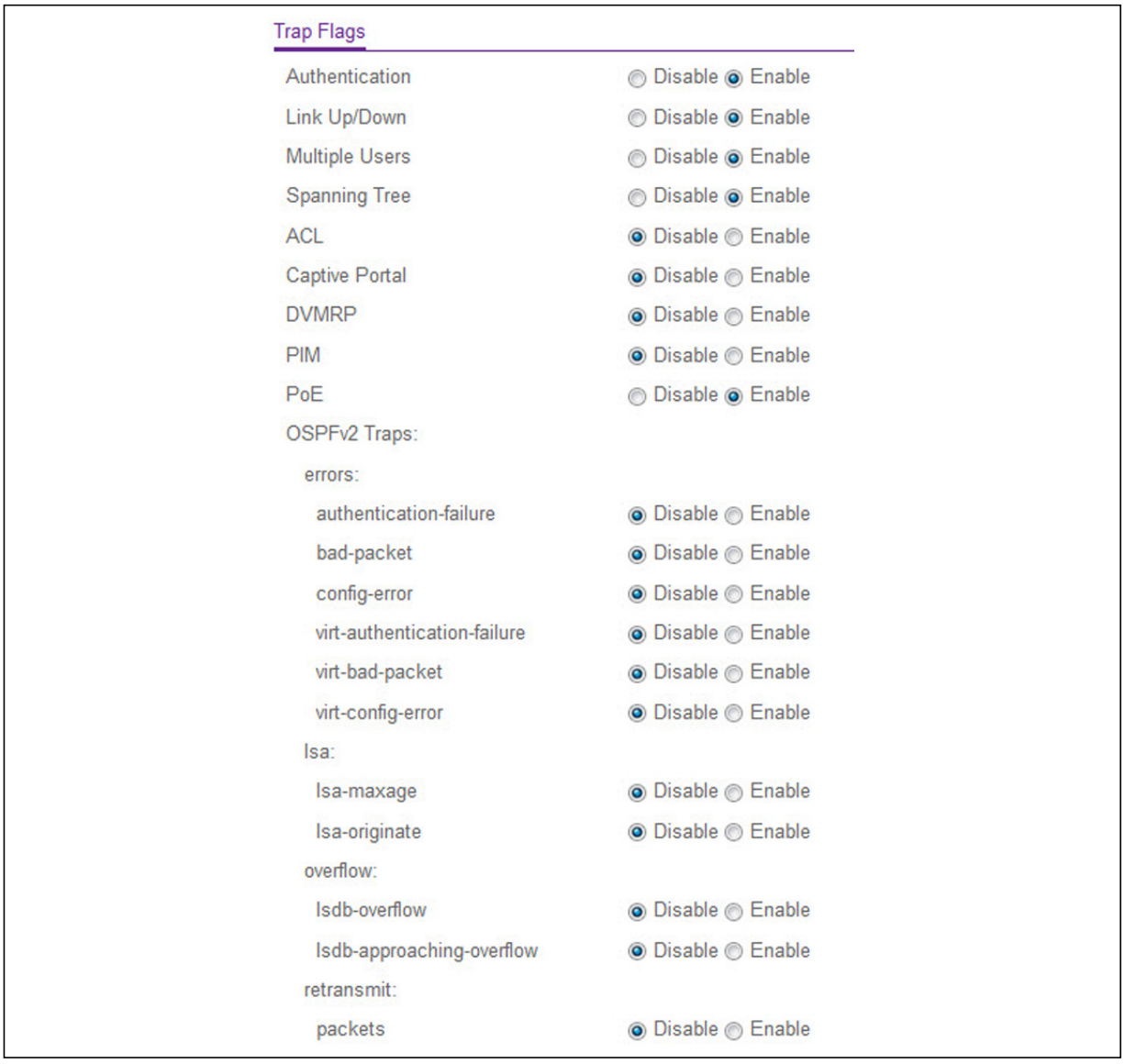


1. To add a host that will receive SNMP traps, enter trap configuration information in the available fields described below, and then click **Add.**
   a. **Community Name** - Enter the community string for the SNMP trap packet to be sent to the trap manager. This may be up to 16 characters and is case sensitive.
   b. **Version** - Select the trap version to be used by the receiver from the 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 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:xxxxx: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 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**.



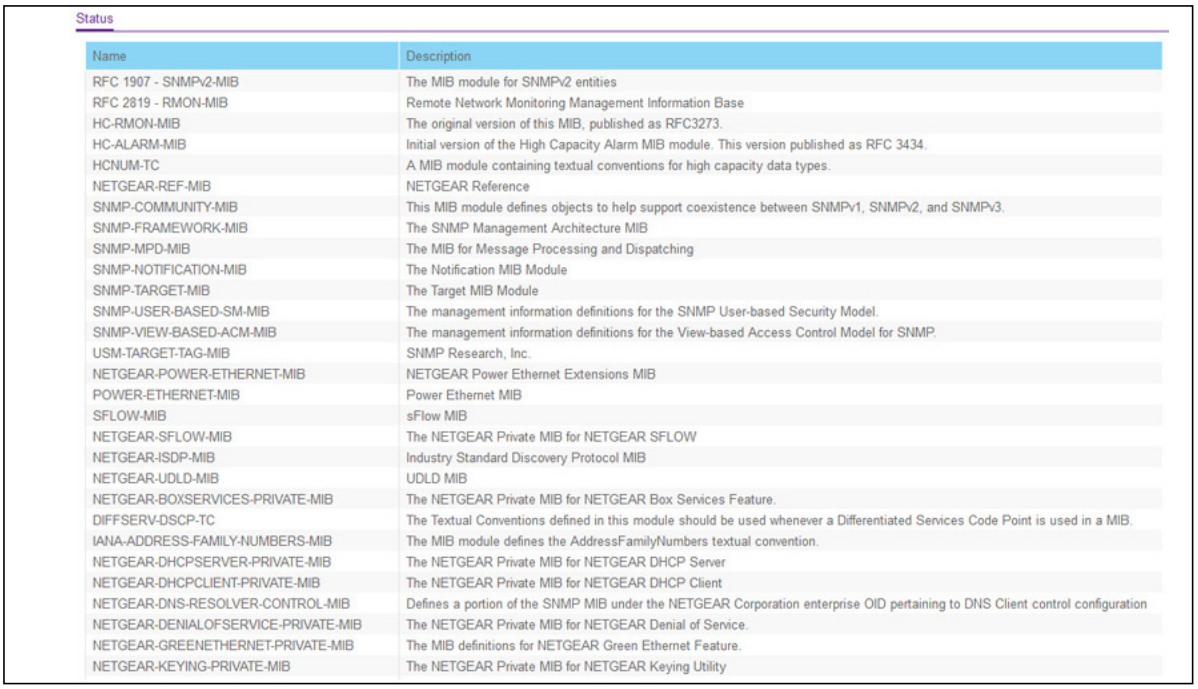
To configure the trap flags:

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**.


Status

Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
HC-RMON-MIB	The original version of this MIB, published as RFC3273.
HC-ALARM-MIB	Initial version of the High Capacity Alarm MIB module. This version published as RFC 3434.
HCNUM-TC	A MIB module containing textual conventions for high capacity data types.
NETGEAR-REF-MIB	NETGEAR Reference
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-FRAMEWORK-MIB	The SNMP Management Architecture MIB
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-NOTIFICATION-MIB	The Notification MIB Module
SNMP-TARGET-MIB	The Target MIB Module
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
USM-TARGET-TAG-MIB	SNMP Research, Inc.
NETGEAR-POWER-ETHERNET-MIB	NETGEAR Power Ethernet Extensions MIB
POWER-ETHERNET-MIB	Power Ethernet MIB
SFLOW-MIB	sFlow MIB
NETGEAR-SFLOW-MIB	The NETGEAR Private MIB for NETGEAR SFLOW
NETGEAR-ISDP-MIB	Industry Standard Discovery Protocol MIB
NETGEAR-UDLD-MIB	UDLD MIB
NETGEAR-BOXSERVICES-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR Box Services Feature.
DIFFSERV-DSCP-TC	The Textual Conventions defined in this module should be used whenever a Differentiated Services Code Point is used in a MIB.
IANA-ADDRESS-FAMILY-NUMBERS-MIB	The MIB module defines the AddressFamilyNumbers textual convention.
NETGEAR-DHCPSERVER-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR DHCP Server
NETGEAR-DHCPCLIENT-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR DHCP Client
NETGEAR-DNS-RESOLVER-CONTROL-MIB	Defines a portion of the SNMP MIB under the NETGEAR Corporation enterprise OID pertaining to DNS Client control configuration
NETGEAR-DENIALOFSERVICE-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR Denial of Service.
NETGEAR-GREENETHERNET-PRIVATE-MIB	The MIB definitions for NETGEAR Green Ethernet Feature.
NETGEAR-KEYING-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR Keying Utility

The following table describes the SNMP Supported MIBs Status fields.

Table 55. SNMP Supported MIBs

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

SNMP V3

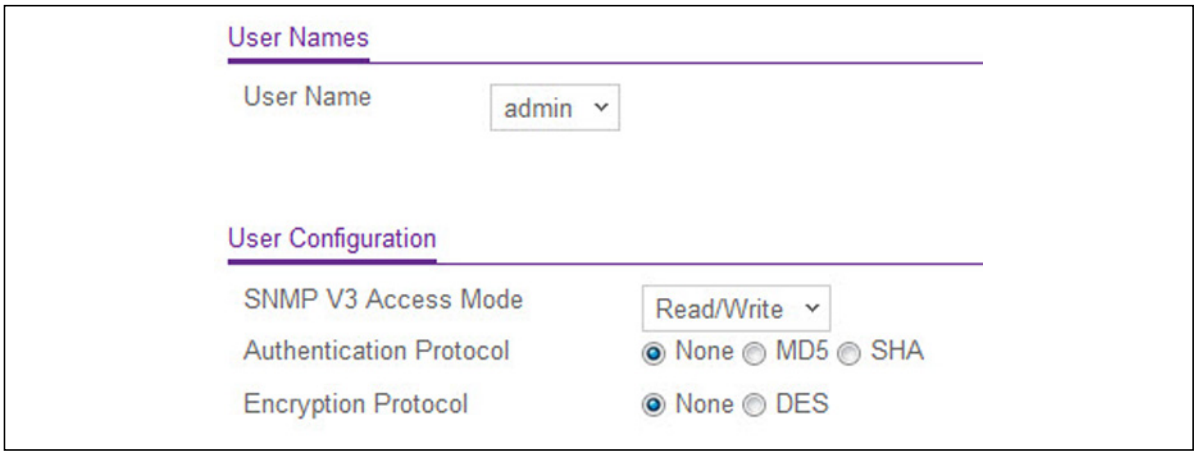
This page provides the configuration information for SNMP v3.

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

- *User Configuration* on page 104

User Configuration

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



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 check box 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 105
- *LLDP-MED* on page 113

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

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

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

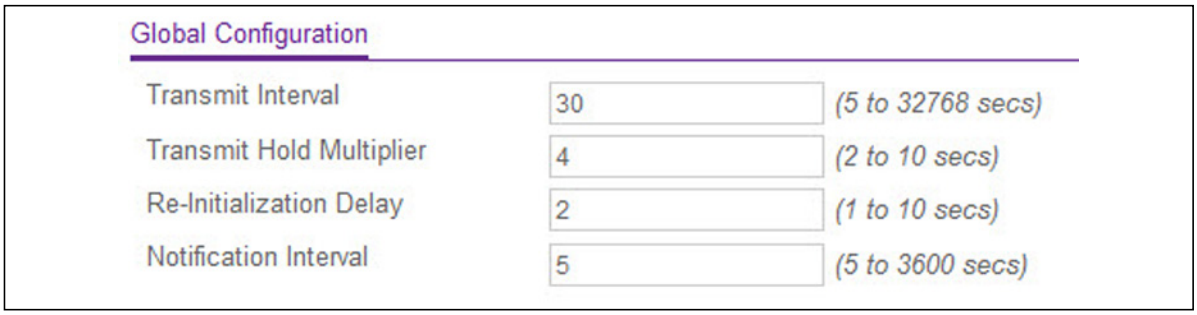
LLDP

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

LLDP Global Configuration

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 is displayed.

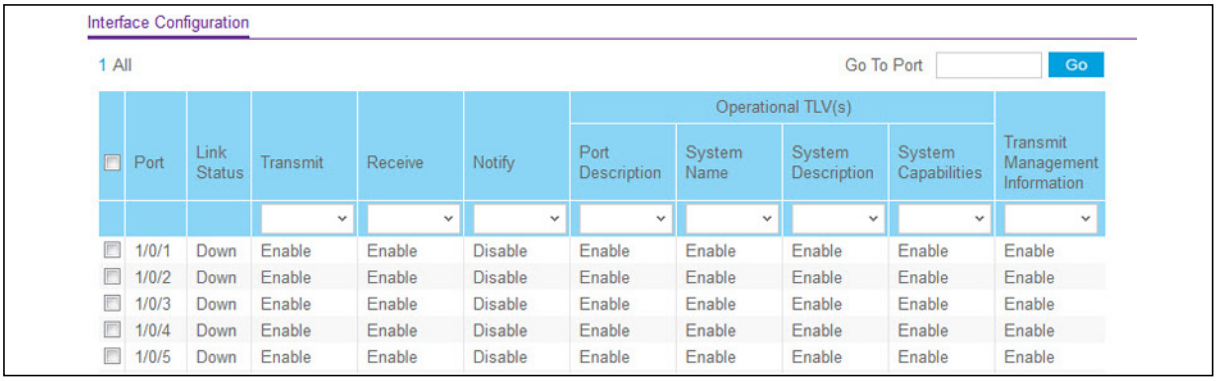


To configure global LLDP settings:

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

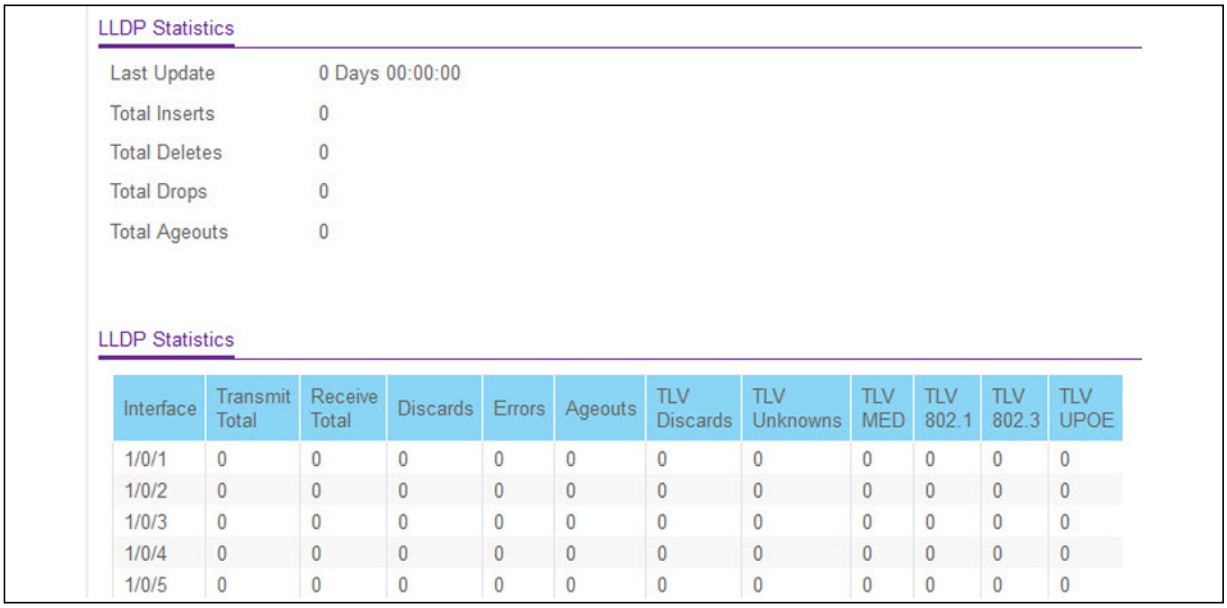
To display this page, click **System** > **LLDP** > **Interface Configuration**. A screen similar to the following is displayed.



1. Use **Go To Port** to enter the Port in unit/slot/port format and click on the **Go** button. The entry corresponding to the specified Port, will be selected.
2. Use **Port** to specify the list of ports on which LLDP - 802.1AB can be configured.
3. **Link Status** indicates whether the Link is up or down.
4. Use **Transmit** to specify the LLDP - 802.1AB transmit mode for the selected interface.
5. Use **Receive** to specify the LLDP - 802.1AB receive mode for the selected interface.
6. Use **Notify** to specify the LLDP - 802.1AB notification mode for the selected interface.
7. Optional TLV(s):
   - Use **Port Description** to include port description TLV in LLDP frames.
   - 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.
8. Use **Transmit Management Information** to specify whether management address is transmitted in LLDP frames for the selected interface.

LLDP Statistics

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



The following table describes the LLDP Statistics fields.

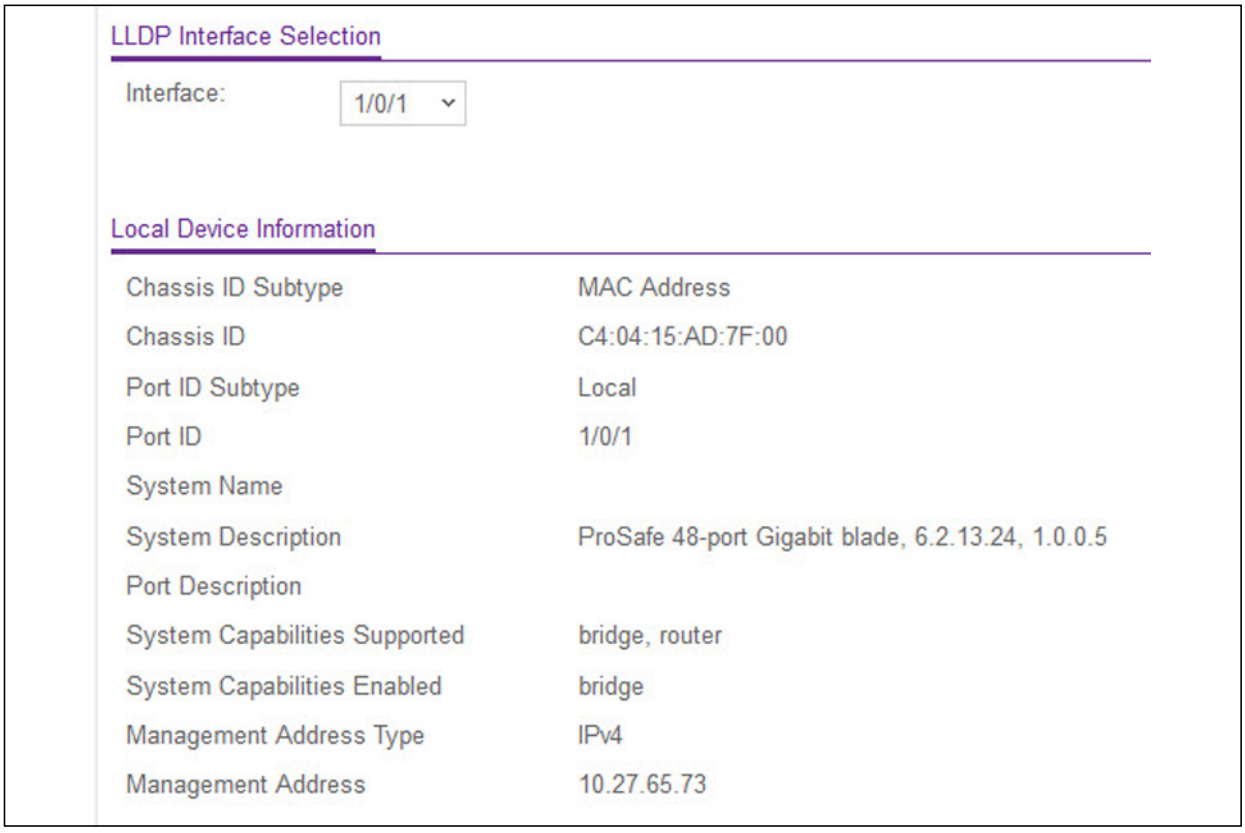
Table 56. LLDP Statistics

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.
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.

Field	Description
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 is displayed.



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

The following table describes the LLDP Local Device Information fields.

Table 57. LLDP Local Device Information

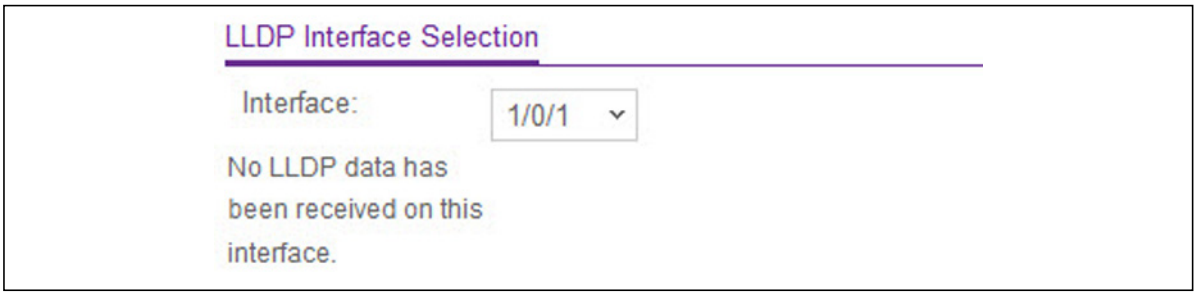
Field	Description
Chassis ID Subtype	Specifies the string that describes the source of the chassis identifier.
Chassis ID	Specifies the string value used to identify the chassis component associated with the local system.
Port ID Subtype	Specifies the string describes the source of the port identifier.
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.

Field	Description
Port Description	Specifies the description of the selected port associated with the local system.
System Capabilities Supported	Specifies the system capabilities of the local system.
System Capabilities Enabled	Specifies the system capabilities of the local system which are supported and enabled.
Management Address Type	Specifies the type of the management address.
Management Address	Specifies the advertised management address of the local system.

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 is displayed.



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

The following table describes the LLDP Remote Device Information fields.

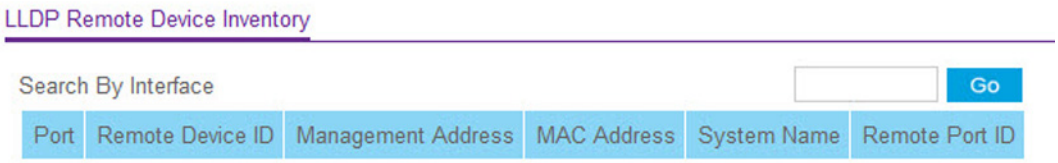
Table 58. LLDP Remote Device Information

Field	Description
Remote ID	Specifies the Remote ID.
Chassis ID	Specifies the chassis component associated with the remote system.
Chassis ID Subtype	Specifies the source of the chassis identifier.
Port ID	Specifies the port component associated with the remote system.
Port ID Subtype	Specifies the source of port identifier.
System Name	Specifies the system name of the remote system.

Field	Description
System Description	Specifies the description of the given port associated with the remote system.
Port Description	Specifies the description of the given port associated with the remote system.
System Capabilities Supported	Specifies the system capabilities of the remote system.
System Capabilities Enabled	Specifies the system capabilities of the remote system which are supported and enabled.
Time to Live	Specifies the Time To Live value in seconds of the received remote entry.
Management Address Type	Specifies the type of the management address.
Management Address	• Management Address - Specifies the advertised management address of the remote system. • Type - Specifies the type of the management address.

LLDP Remote Device Inventory

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



The following table describes the LLDP Remote Device Inventory fields.

Table 59. LLDP Remote Device Inventory

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

Field	Description
System Name	Specifies model name of the remote device.
Remote Port ID	Specifies the port component associated with the remote system.

LLDP-MED

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

- *LLDP-MED Global Configuration* on page 113
- *LLDP-MED Interface Configuration* on page 114
- *LLDP-MED Local Device Information* on page 115
- *LLDP-MED Remote Device Information* on page 117
- *LLDP-MED Remote Device Inventory* on page 120

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 is displayed.

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

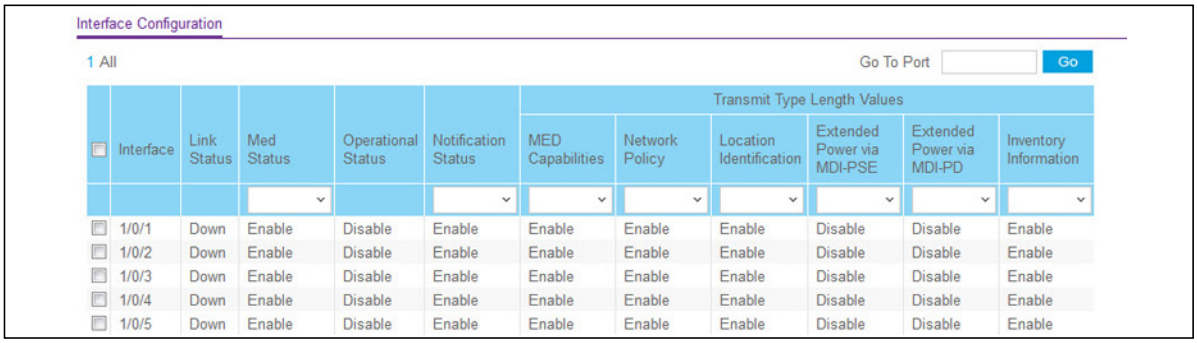
The following table describes the LLDP-MED Global Configuration fields.

Table 60. LLDP-MED Global Configuration

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 is displayed.



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

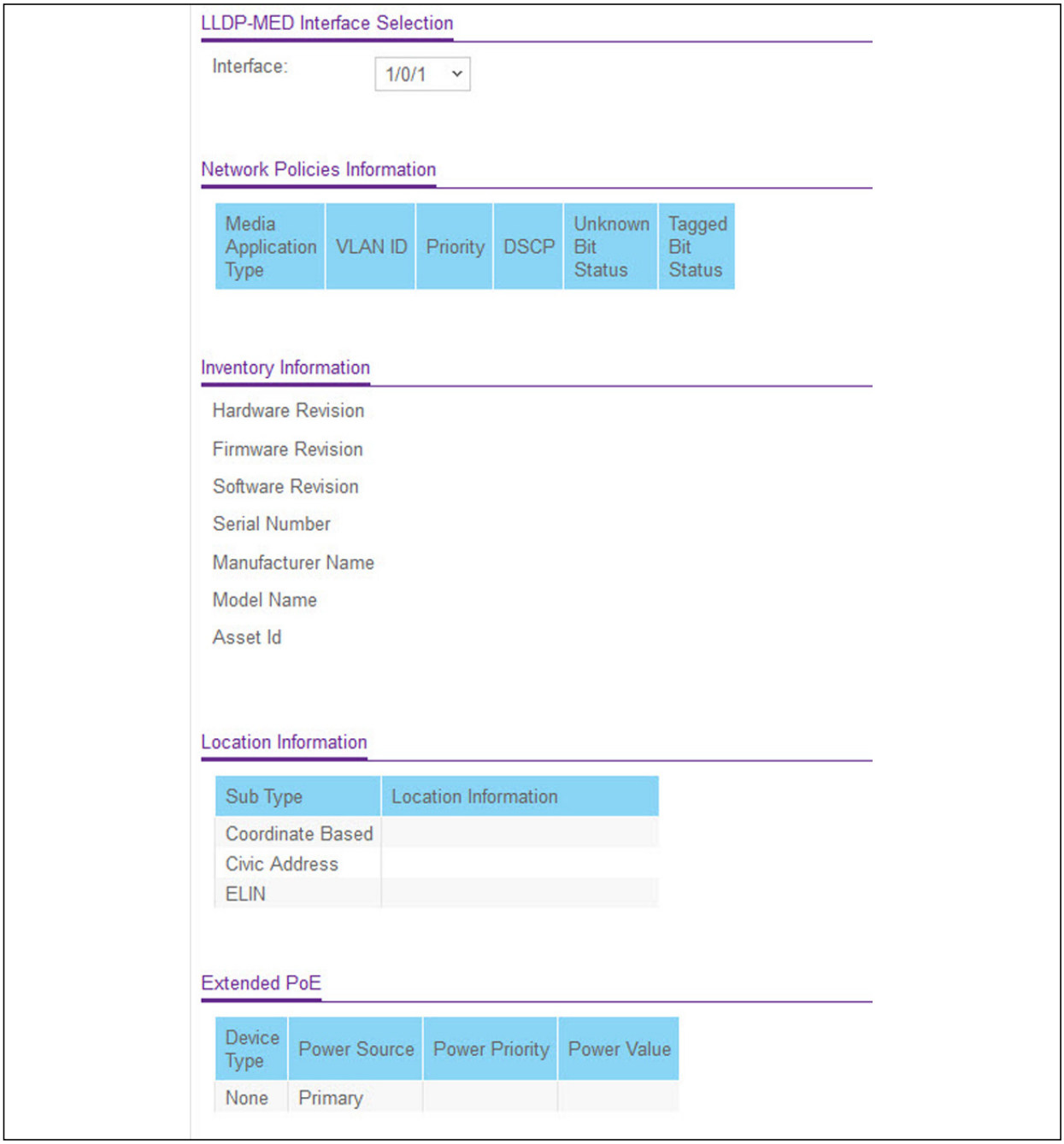
The following table describes the LLDP-MED Interface Configuration fields.

Table 61. LLDP-MED Interface Configuration

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 is displayed.



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

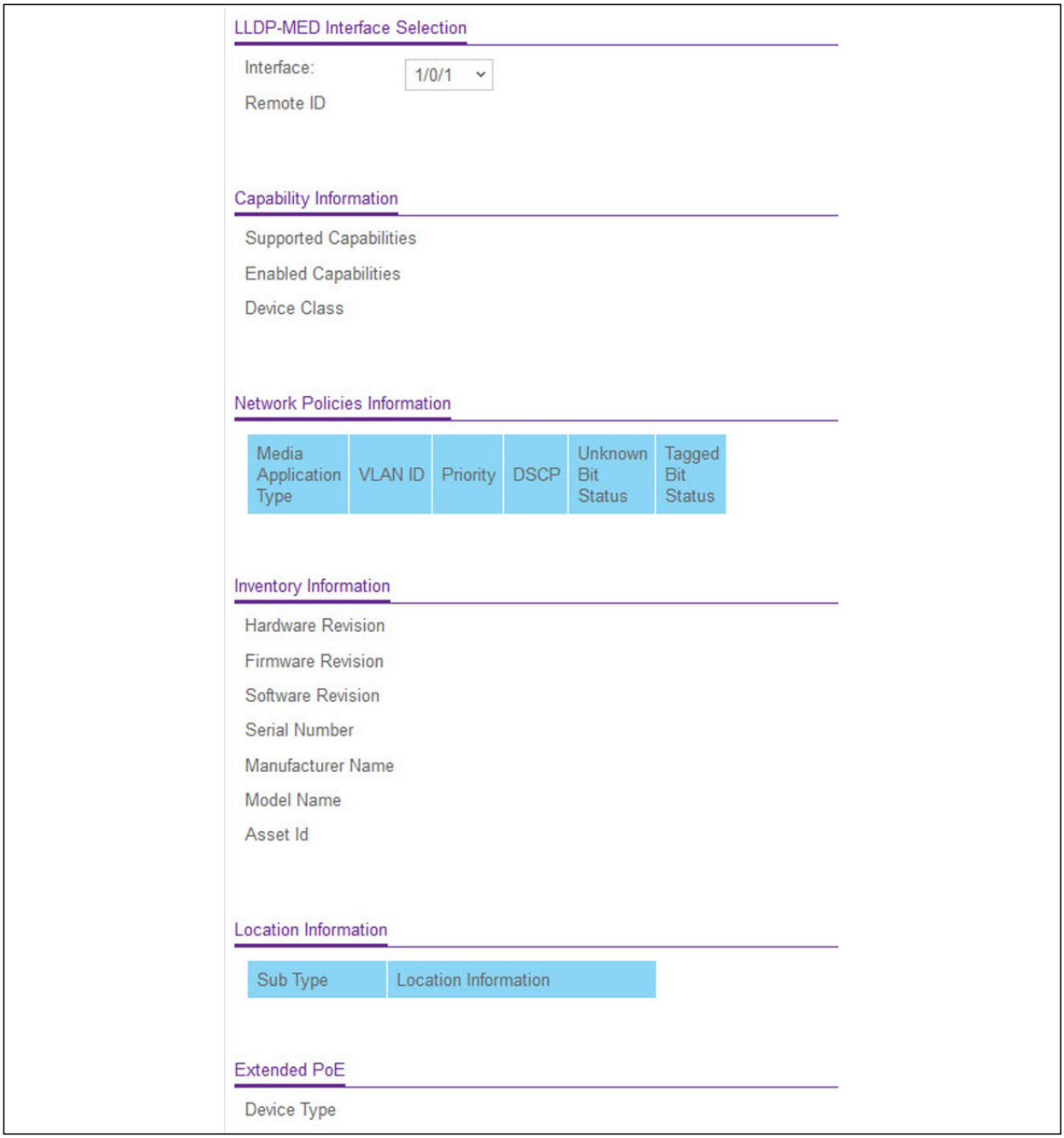
The following table describes the LLDP-MED Local Device Information fields.

Table 62. LLDP-MED Local Device Information

Field		Description
Network Policy Information: Specifies if network policy TLV is present in the LLDP frames.		
	Media Application Type	Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Each application type that is received has the VLAN id, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been transmitted, only then would this information be displayed
Inventory: Specifies if inventory TLV is present in LLDP frames.		
	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.
Location Information: Specifies if location TLV is present in LLDP frames.		
	Sub Type	Specifies type of location information.
	Location Information	Specifies the location information as a string for given type of location id.

LLDP-MED Remote Device Information

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



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

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

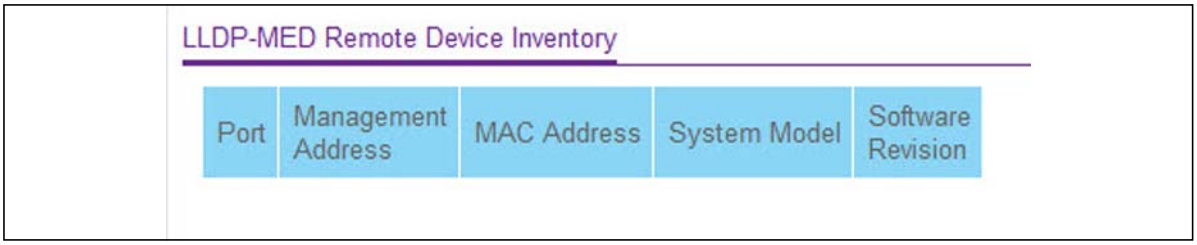
Table 63. LLDP-MED Remote Device Information

Field		Description
Capability Information: Specifies the supported and enabled capabilities that was received in MED TLV on this port.		
	Supported Capabilities	Specifies supported capabilities that was received in MED TLV on this port.
	Enabled Capabilities	Specifies enabled capabilities that was received in MED TLV on this port.
	Device Class	Specifies device class as advertised by the device remotely connected to the port.
Network Policy Information: Specifies if network policy TLV is received in the LLDP frames on this port.		
	Media Application Type	Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Each application type that is received has the VLAN id, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been received 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
Inventory Information: Specifies if inventory TLV is received in LLDP frames on this port.		
	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.
Location Information: Specifies if location TLV is received in LLDP frames on this port.		
	Sub Type	Specifies type of location information.
	Location Information	Specifies the location information as a string for given type of location id.
Extended POE: Specifies if remote device is a PoE device.		
	Device Type	Specifies remote device's PoE device type connected to this port.
Extended POE PSE: Specifies if extended PSE TLV is received in LLDP frame on this port.		
	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.
Extended POE PD: Specifies if extended PD TLV is received in LLDP frame on this port.		
	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 is displayed.



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

Table 64. LLDP-MED Remote Device Inventory

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

ISDP

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

- *Basic* on page 121
- *Advanced* on page 122

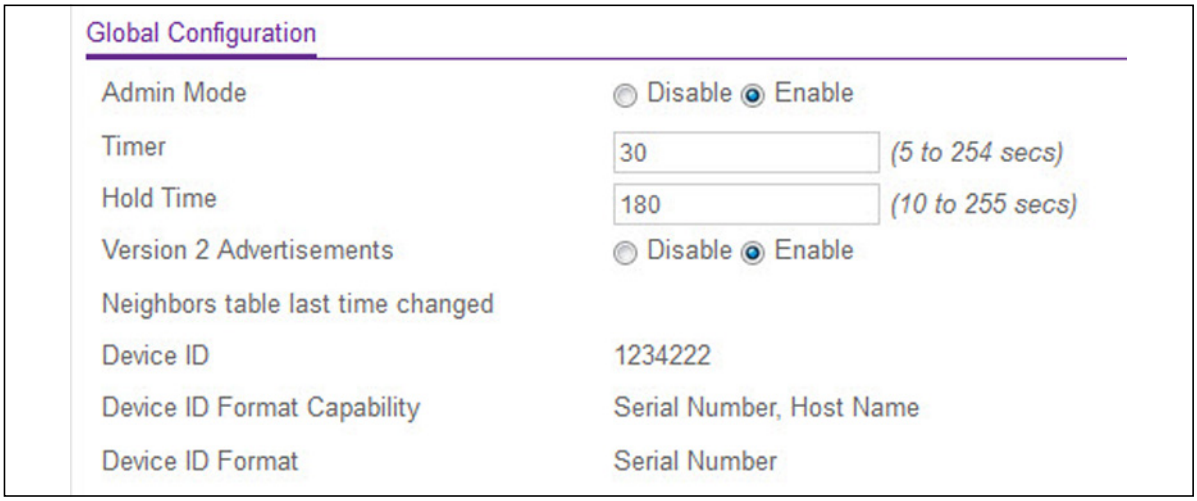
Basic

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

- *Global Configuration* on page 121

Global Configuration

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



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

The following table describes the ISDP Basic Global Configuration fields.

Table 65. ISDP Basic Global Configuration

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.

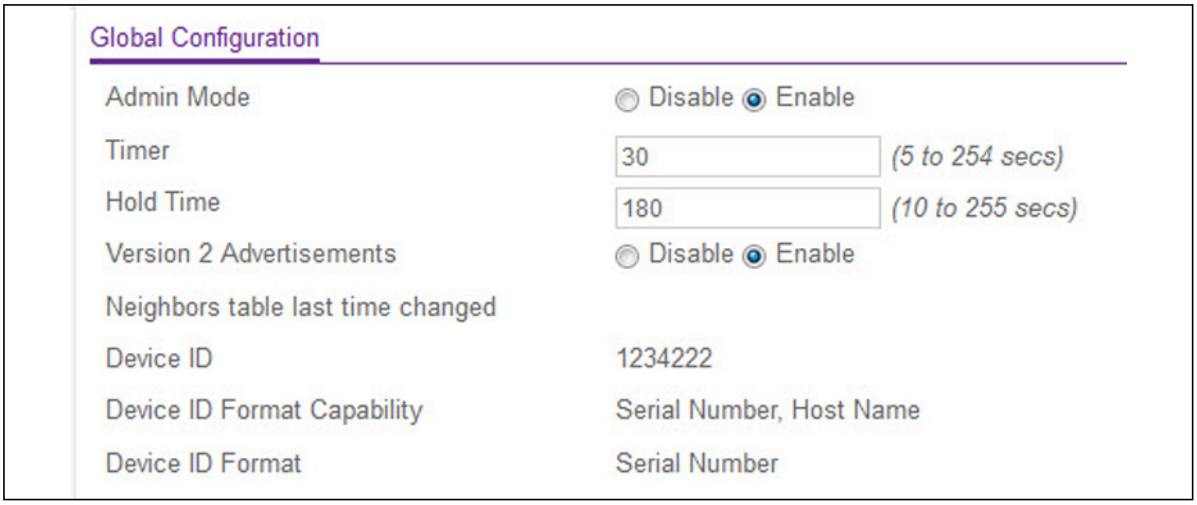
Advanced

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

- *Global Configuration* on page 123
- *Interface Configuration* on page 123
- *ISDP Neighbor* on page 124
- *ISDP Statistics* on page 125

Global Configuration

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



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

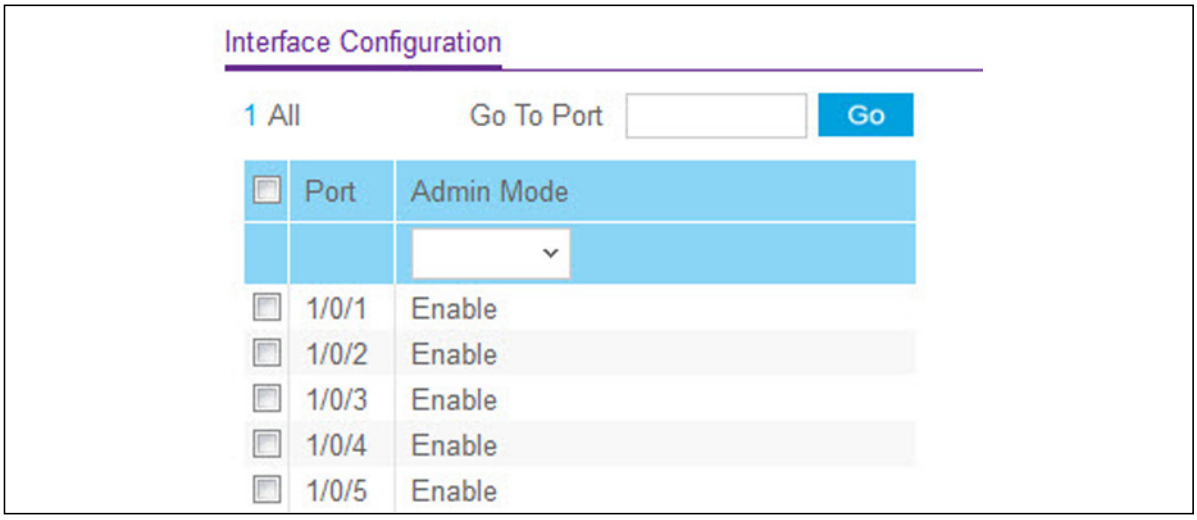
The following table describes the ISDP Advanced Global Configuration fields.

Table 66. ISDP Advanced Global Configuration

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

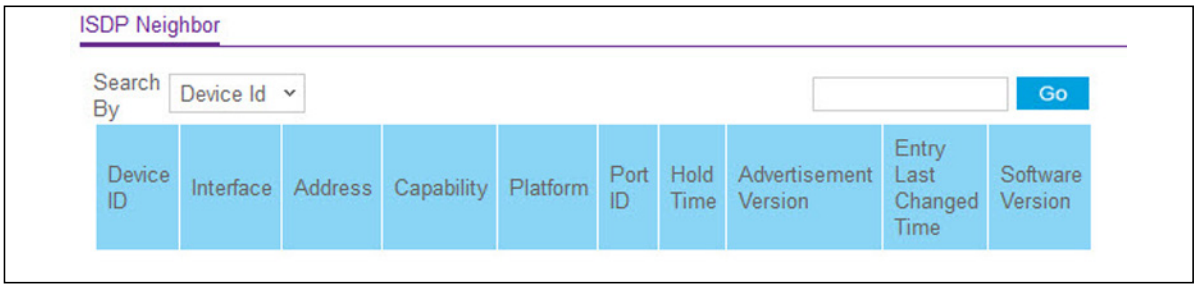
To display this page, click **System** > **ISDP** > **Advanced** > **Interface Configuration**. A screen similar to the following is displayed.



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 is displayed.



The following table describes the ISDP Neighbor fields.

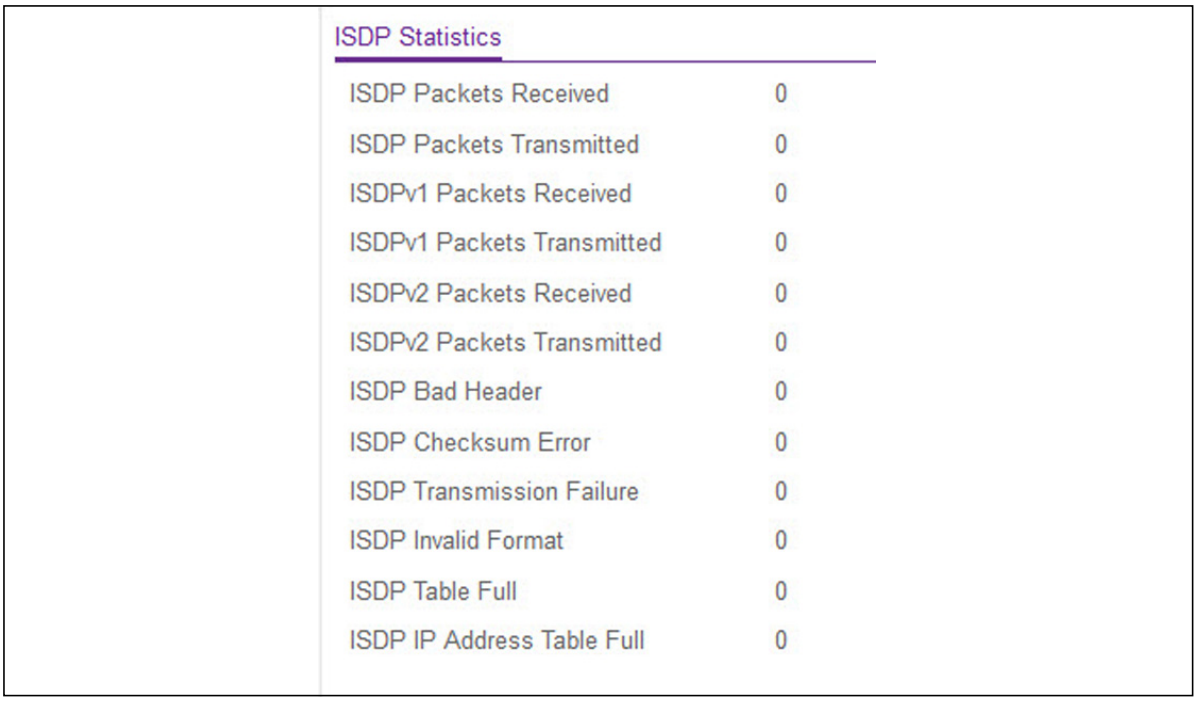
Table 67. ISDP Neighbor

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.

Field	Description
Capability	Displays the capability of the neighbor. These are supported: • Router • Trans Bridge • Source Route • Switch • Host • IGMP • Repeater
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 is displayed.



The following table describes the ISDP Statistics fields.

Table 68. ISDP Statistics

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.

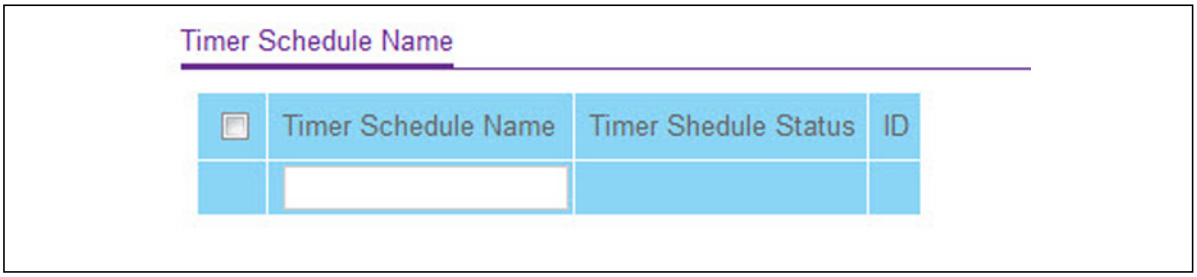
From the Timer Schedule link, you can access the following pages:

- *Timer Global Configuration* on page 126
- *Timer Schedule Configuration* on page 127

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 is displayed.



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.

Table 69. Timer Schedule

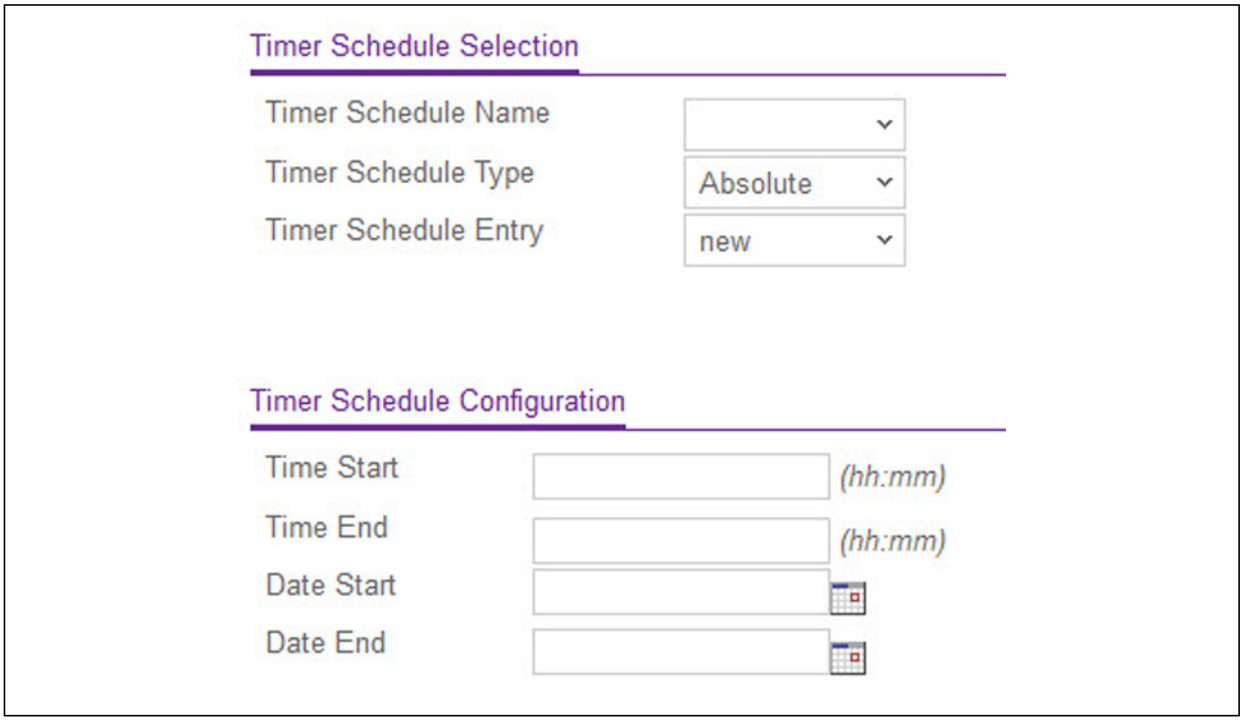
Field	Description
ID	Identification of the timer Schedule. Maximum number of schedules that can be created is 100.

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.
6. 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 is displayed.



1. Use the **Timer Schedule Name** to select the timer schedule name for which data is to be displayed.
2. Use the **Timer Schedule Type** to select the type of the timer schedule entry to be configured. It can be selected as Absolute or Periodic.
3. Use the **Timer Schedule Entry** to select the number of the timer schedule entries to be configured or added. Option 'new' has to be selected to add new entry.
4. 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.
5. Use the **Time End** to set the time of the day in format (HH:MM) when the schedule operation is terminated.
6. Use the **Date Start** to set the schedule start date. If no date is specified, the schedule starts running immediately.
7. Use the **Date Stop** to set the schedule termination date. If No End Date selected, the schedule operates indefinitely.
8. 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 operates.
- **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.

9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest values.
10. 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

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:

- *Advanced* on page 132

Basic

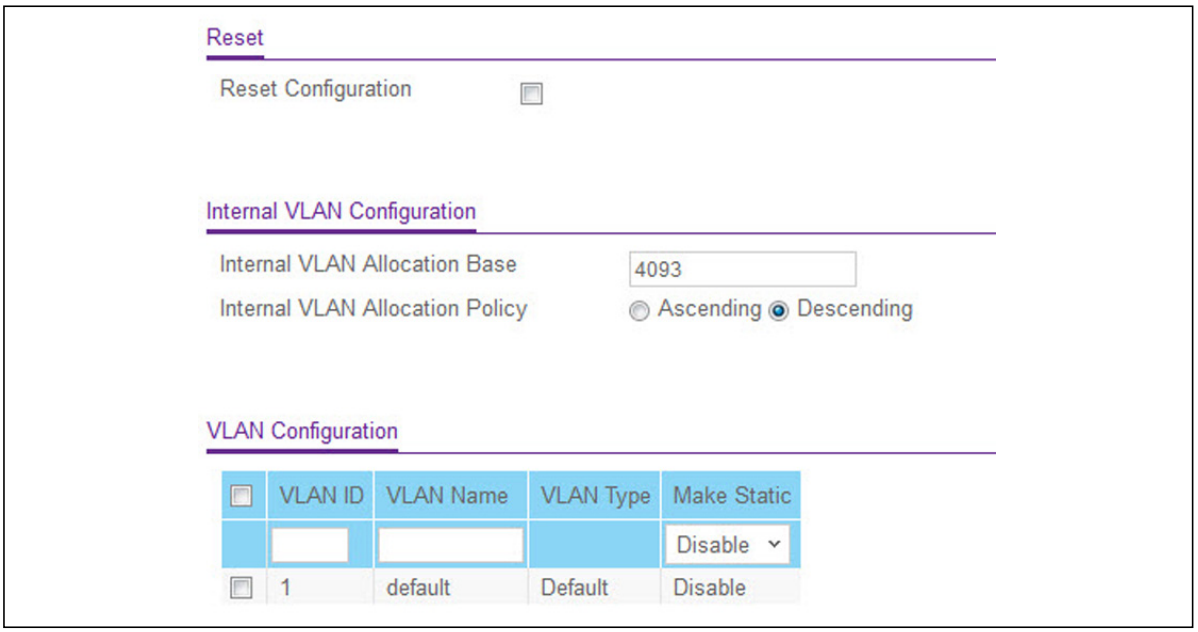
From the Basic link, you can access the following pages:

- *VLAN Configuration* on page 131

VLAN Configuration

Use the VLAN Configuration page to define VLAN groups stored in the VLAN membership table. Each switch in the M6100 Chassis switch family supports up to 1024 VLANs. VLAN 1 is created by default and is the default VLAN of which all ports are members.

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



1. **Reset Configuration** - If you select this check box 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 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.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

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'.

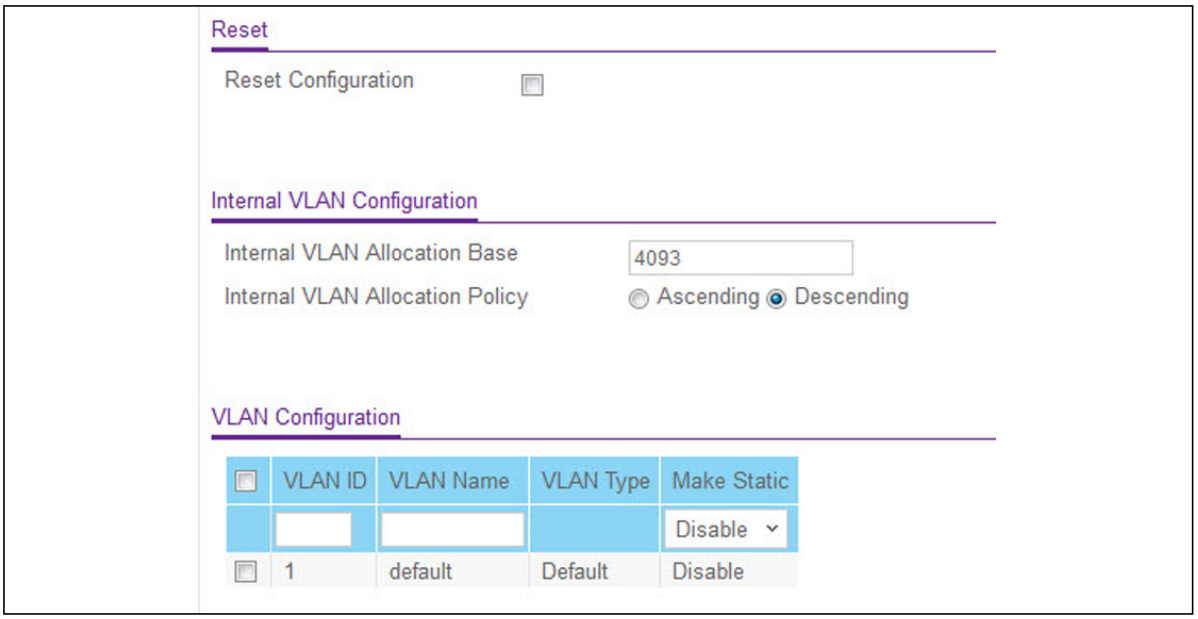
Advanced

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

- *VLAN Configuration* on page 131
- *VLAN Membership* on page 134
- *VLAN Status* on page 135
- *Port PVID Configuration* on page 136
- *MAC Based VLAN* on page 137
- *Protocol Based VLAN Group Configuration* on page 138

VLAN Configuration

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



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

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

Internal VLAN Configuration

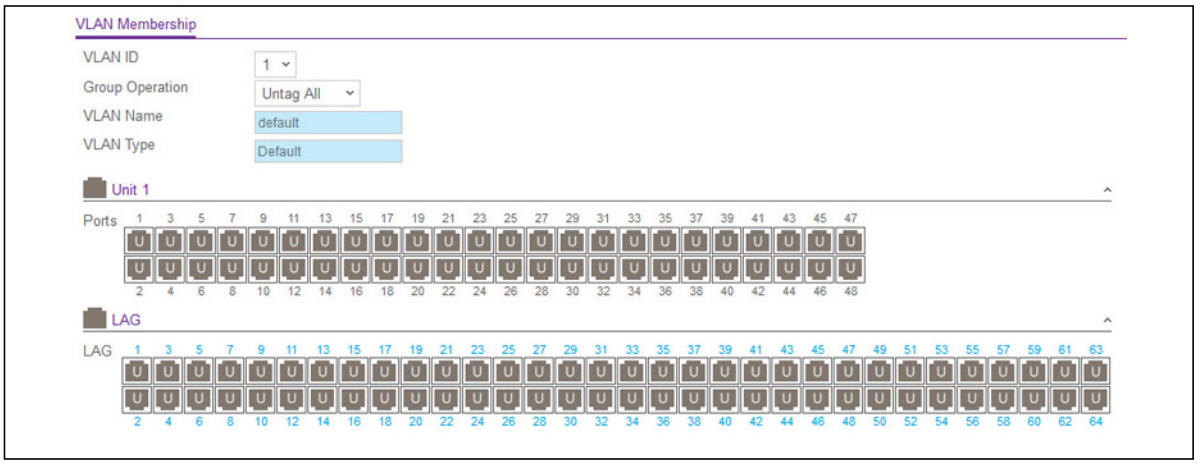
This page displays the allocation base and the allocation mode of internal VLAN. The internal VLAN is reserved by port-based routing interface and invisible to the end user. Once these

internal VLANs are allocated by port-based routing interface, they cannot be assigned to a routing VLAN interface.

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

VLAN Membership

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



To configure VLAN membership:

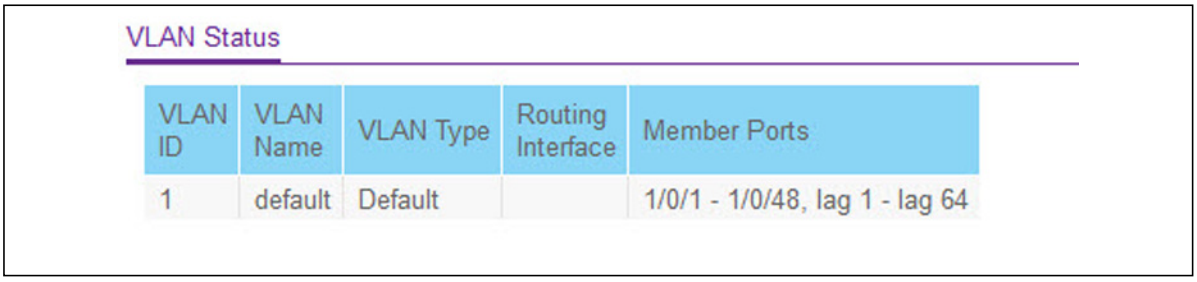
1. Use **VLAN ID** to select the VLAN ID for which you want to display or configure data.
2. Use **Group Operation** to select all the ports and configure them:
   - **Untag All** - Select all the ports on which all frames transmitted for this VLAN will be untagged. All the ports will be included in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

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**.



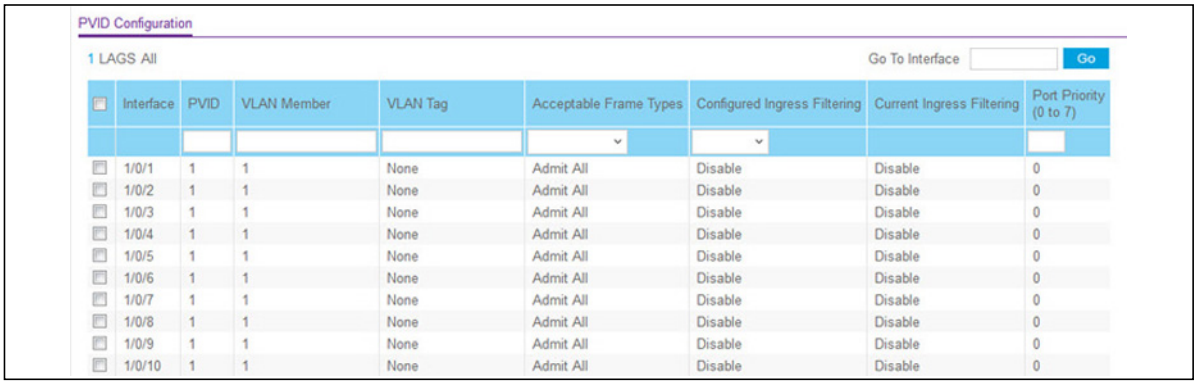
Field	Definition
VLAN ID	The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named `Default`.
VLAN Type	The VLAN type: • Default (VLAN ID = 1) -- always present • Static -- a VLAN you have configured • Dynamic -- a VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore remove
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**.



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 **VLAN Member** to specify the VLAN ID or list of VLANs of a member port. VLAN IDs range from 1 to 4093. The factory default is 1. Use a dash (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.
6. Use **VLAN Tag** to specify the VLAN ID or list of VLANs of a tagged port. VLAN IDs range from 1 to 4093. Use a dash (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted. To reset the VLAN Tag Configuration to the defaults, use the **None** keyword. Port tagging for the VLAN can only be set if the port is a member of this VLAN.
7. 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.

8. **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.
9. 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.

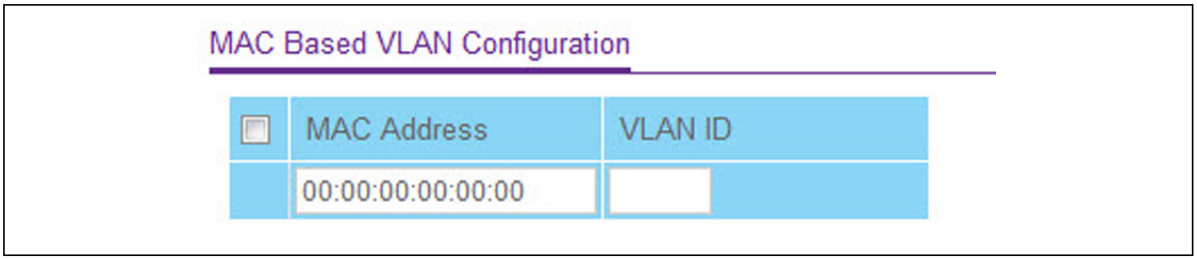
MAC Based VLAN

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 and entry of MAC Address to VLAN mapping.

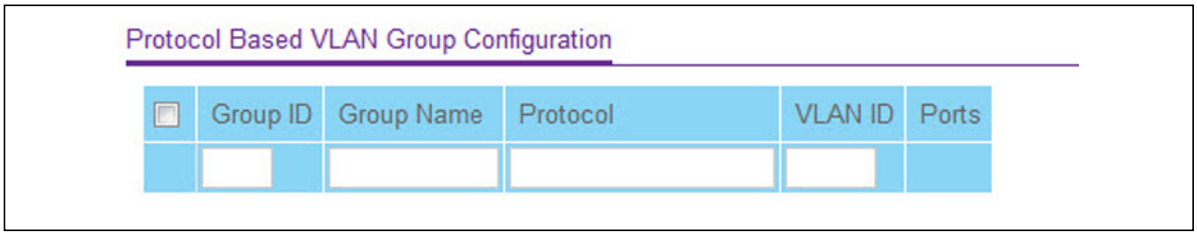
Protocol Based VLAN Group Configuration

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**.

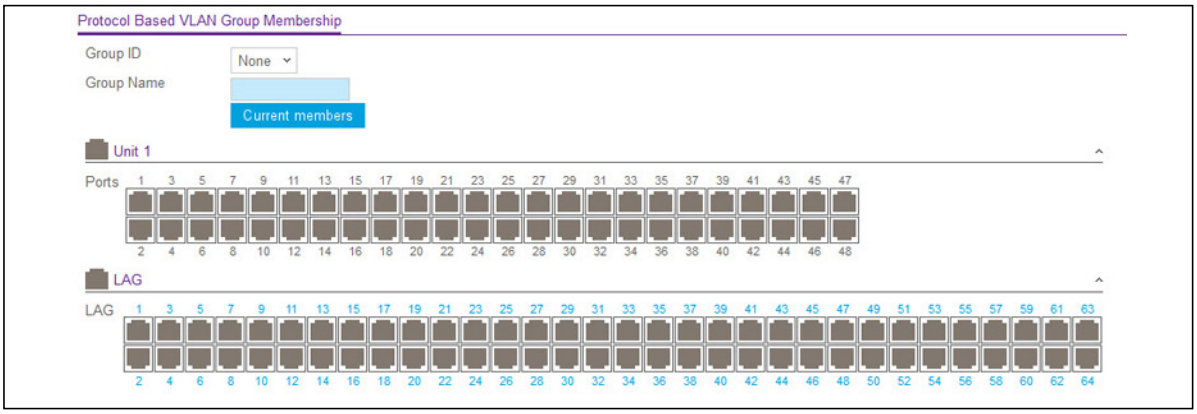


1. Use **Group Name** to assign a name to a new group. You may enter up to 16 characters.
2. Use **Protocol(s)** to select the protocols you want to be associated with the group. There are three configurable protocols: IP, IPX, ARP.
   - **IP** - IP is a network layer protocol that provides a connectionless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



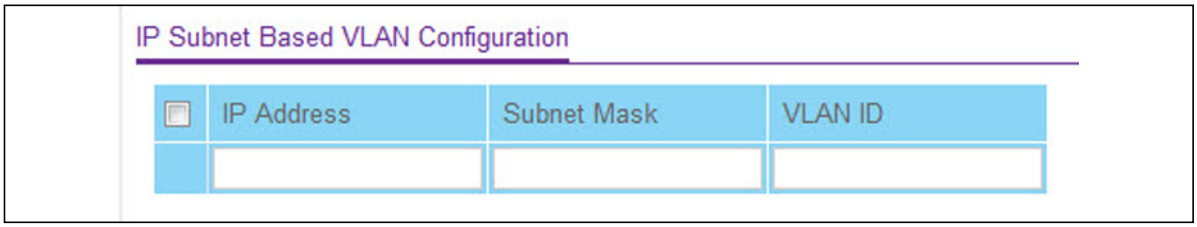
1. Use **Group ID** to select the protocol-based VLAN Group ID for which you want to display or configure data.
2. Use **Port List** to add the ports you selected to this Protocol Based VLAN Group. Note that a given interface can only belong to one group for a given protocol. If you have already added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

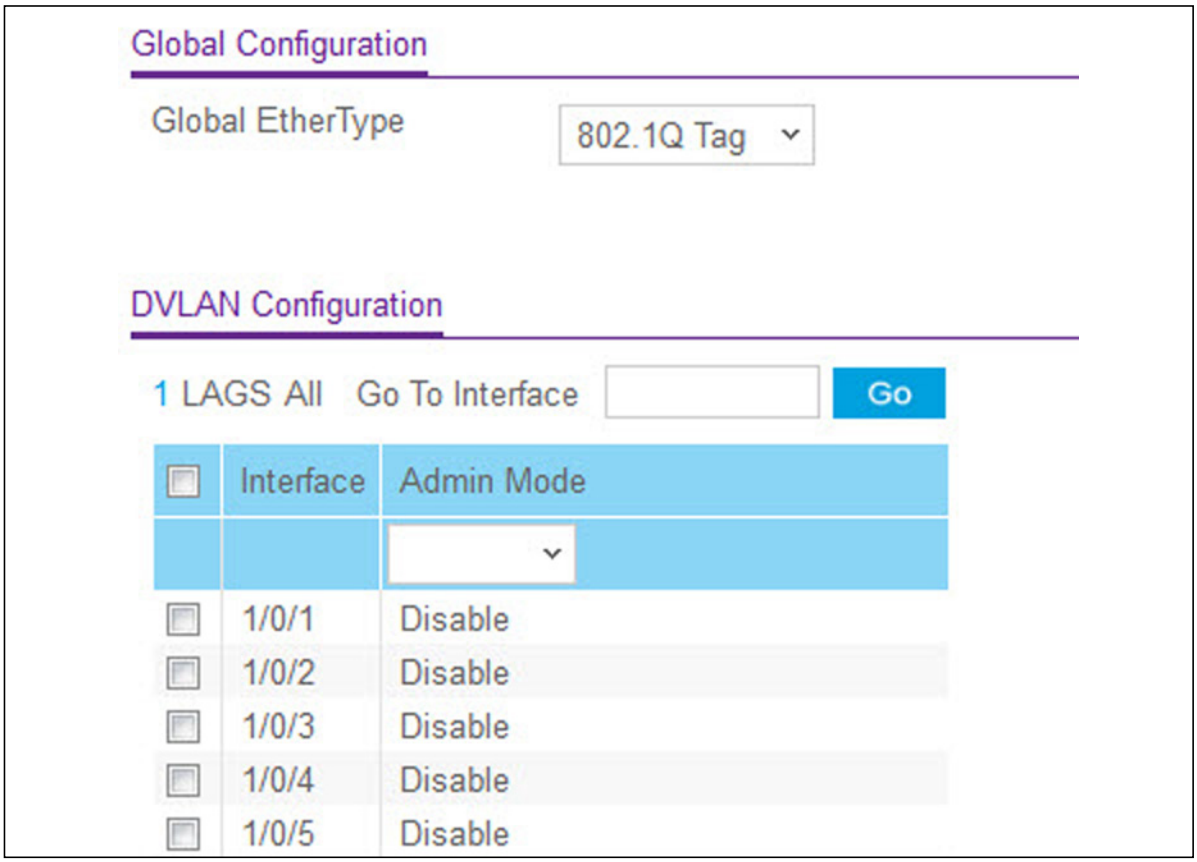
To display the MAC Based VLAN page, click **Switching** > **VLAN** > **Advanced** > **IP Subnet Based VLAN**.



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

Port DVLAN Configuration

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



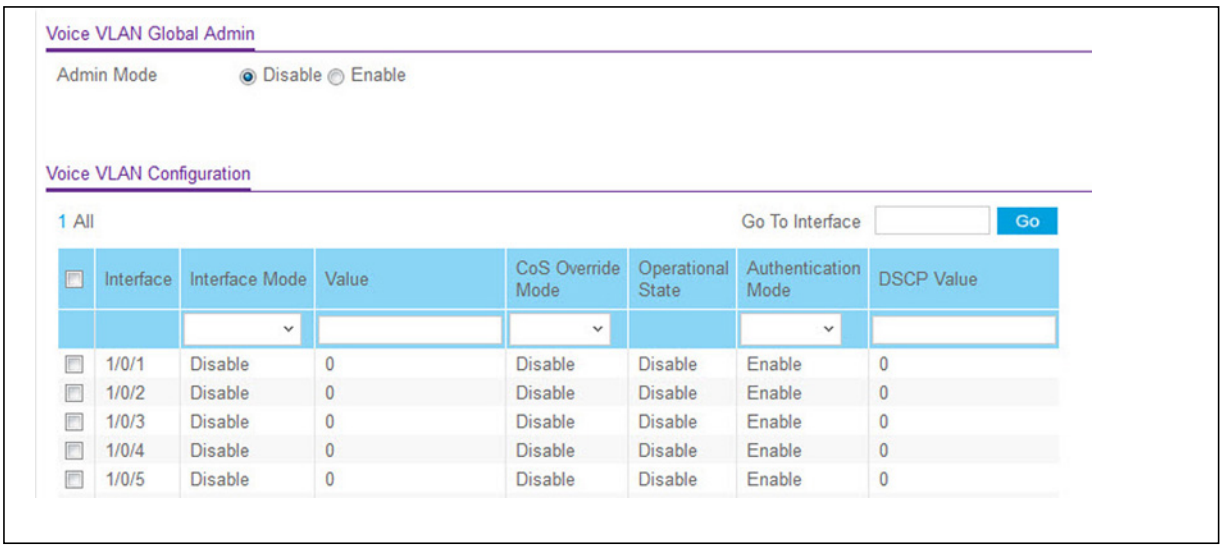
1. Use **Interface** to select the physical interface for which you want to display or configure data. Select 'All' to set the parameters for all ports to same values.

2. Use **Admin Mode** to specify the administrative mode via which Double VLAN Tagging can be enabled or disabled. The default value for this is Disabled.
3. Use the 2-byte hex Global EtherType as the first 16 bits of the DVLAN tag.
   - **802.1Q Tag** - Commonly used tag representing 0x8100
   - **vMAN Tag** - Commonly used tag representing 0x88A8
   - **Custom Tag** - Configure the EtherType in any range from 0 to 65535

Voice VLAN Configuration

Use this page 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**.



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.

6. Use **Authentication Mode** to configure the authentication mode for the selected interface. The default is **Enable**. When authentication mode is enabled, then voice traffic is allowed on an unauthorized Voice VLAN port. When authentication mode is disabled, then devices are authorized through dot1x.

Note: Authentication through dot1x is possible only if dot1x is enabled.

7. Use **DSCP Value** to configure the Voice VLAN DSCP value for the port. The valid range is 0 to 64. The default value is 0.

Table 70 describes the non-configurable Voice VLAN Configuration field.

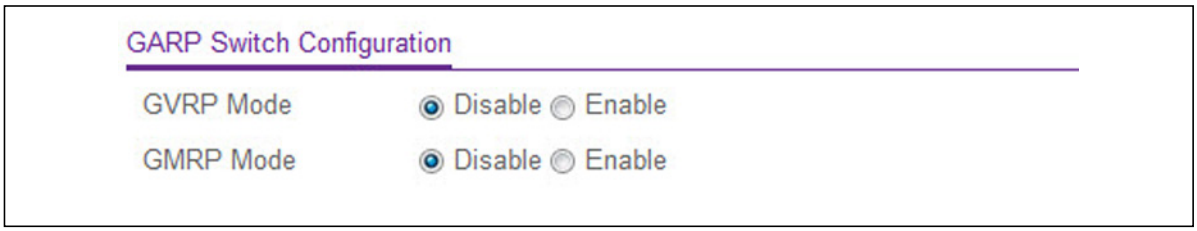
Table 70. Voice VLAN Configuration

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**.

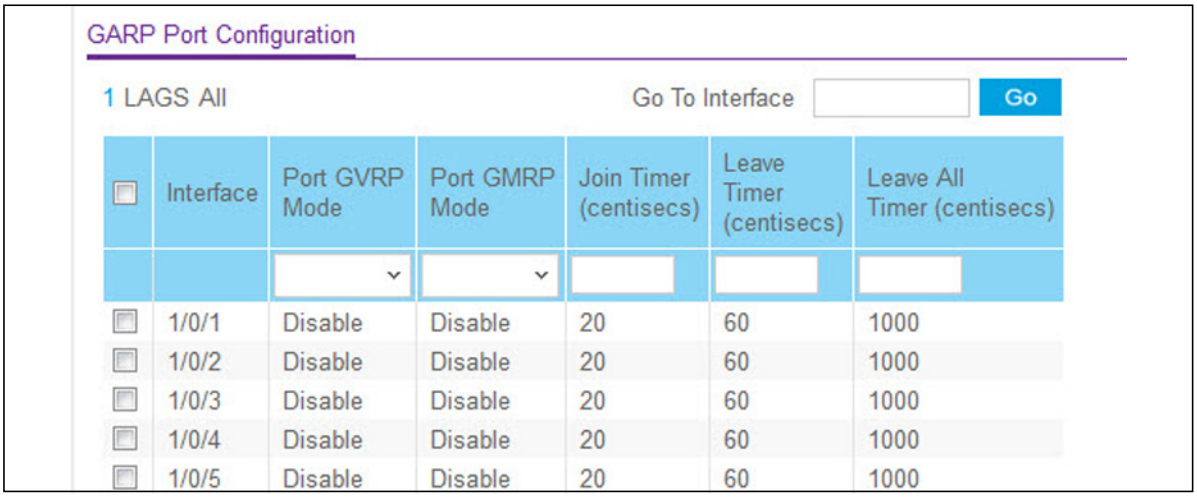


1. Use **GVRP Mode** to choose the GARP VLAN Registration Protocol administrative mode for the switch by selecting enable or disable from the radio button. The factory default is disable.
2. Use **GMRP Mode** to choose the GARP Multicast Registration Protocol administrative mode for the switch by selecting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



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 drop-down 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 drop-down list. If you select disable, the protocol will not be active, and Join Time, Leave Time and Leave All Time have no effect. The factory default is disable.
4. Use **Join Time (centiseconds)** to specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. Enter a number between 10 and 100 (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). An instance of this timer exists for each GARP participant for each port.
5. Use **Leave Time (centiseconds)** to specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 20 and 600 (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.
6. Use **Leave All Time (centiseconds)** to control how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer

is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. The timer is specified in centiseconds. Enter a number between 200 and 6000 (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). An instance of this timer exists for each GARP participant for each port.

Auto-VoIP

The Auto-VoIP feature enables manual and auto assignment of VoIP phone traffic to a special VLAN (e.g., Voice VLAN) allowing the assignment of special QoS parameters to that traffic, giving it high priority services.

From the Auto-VoIP link, you can access the following pages:

- *Protocol-based* on page 144
- *Advanced* on page 154

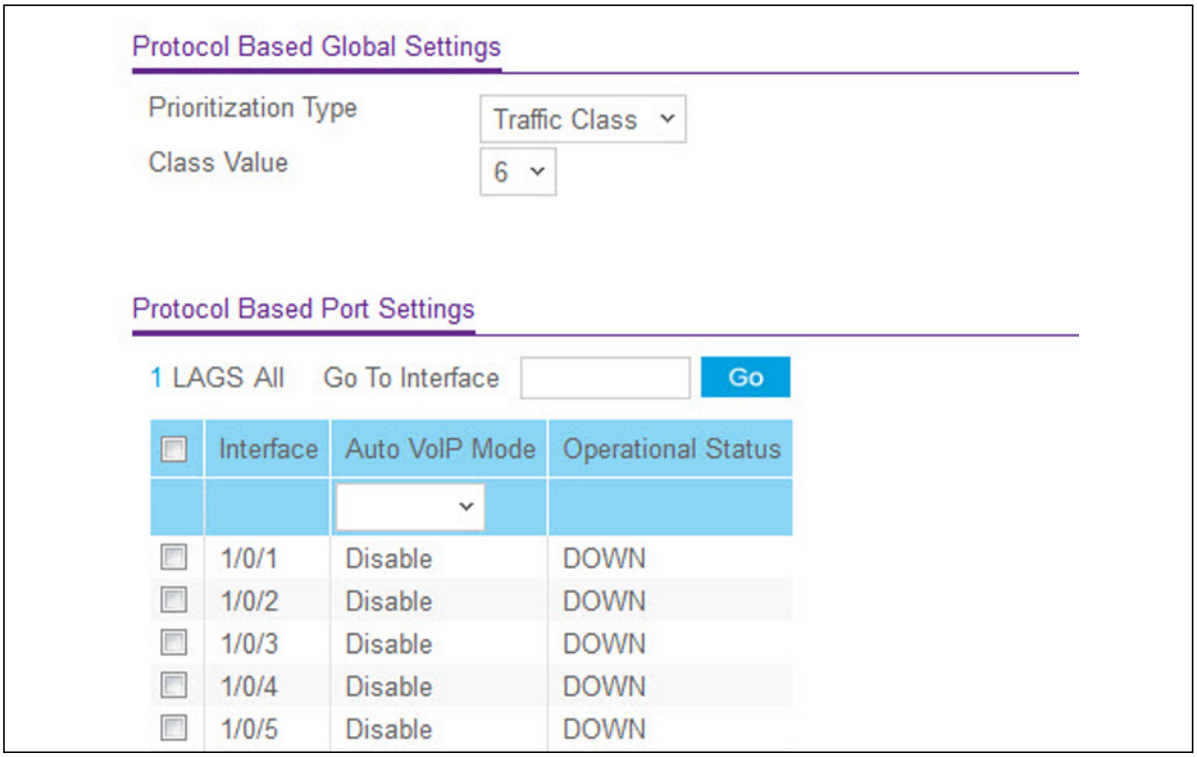
Protocol-based

From the Protocol-based link, you can access the following pages:

- *Port Settings* on page 144

Port Settings

To display the Port Setting page, click **Switching > Auto-VoIP > Protocol-based**> **Port Settings**.



1. Use **Prioritization Type** to specify the type of prioritization. It can be Traffic Class or Remark.
2. Use **Class Value** to specify the CoS tag value to be reassigned for packets received on the voice VLAN when Remark CoS is enabled.
3. Click **Cancel** to cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch.
4. 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.

OUI-based

From the OUI-based link, you can access the following pages:

- *Properties* on page 145
- *Port Settings* on page 146
- *OUI Table* on page 147

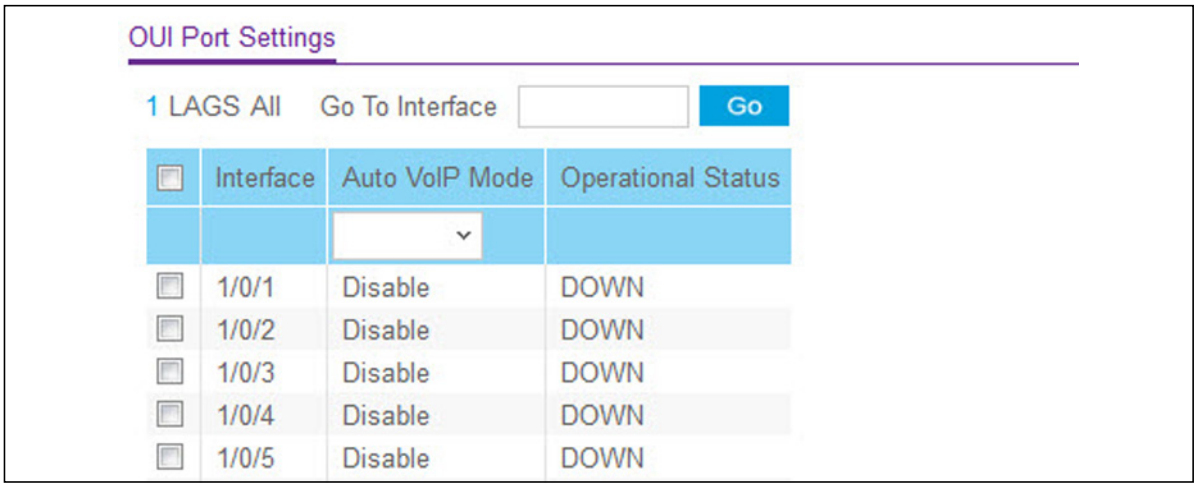
Properties

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

1. Use **VoIP VLAN ID** to configure VoIP VLAN ID on the switch. There is no default VLAN for auto-voip, you must create a VLAN for it first.
2. Use **OUI-based priority** to configure OUI-based priority on the switch. Default value is 7.
3. Click **Cancel** to cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch.
4. 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.

Port Settings

To display the OUI Port Settings page, click **Switching > Auto-VoIP > OUI-based> Port Settings**.

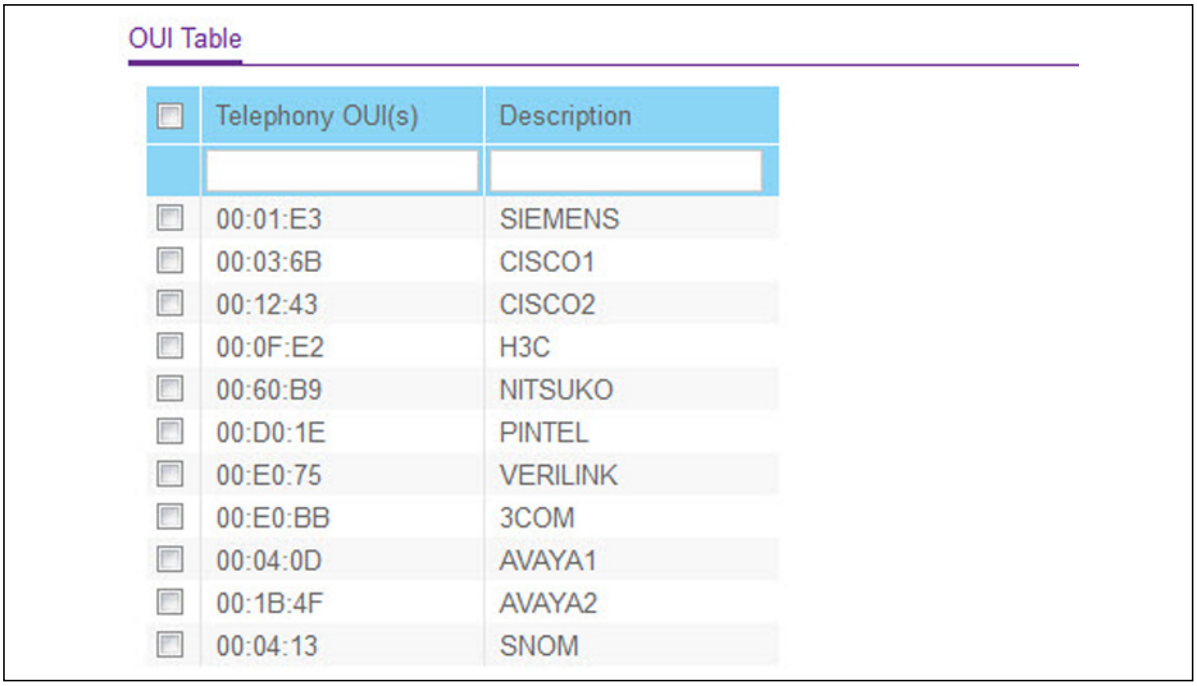


1. Use **Interface** to select the interface for which data is to be displayed or configured.
2. Use **Auto VoIP Mode** to Enable or Disable AutoVoIP mode on the selected interface. Auto VoIP is disabled by default.
3. Use **Go To Interface** to select an interface by entering its number.
4. Click **Cancel** to cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch.
5. Click **Apply** to 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
Operational Status	Displays the current operational status of the interface.

OUI Table

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



1. Use **Telephony OUI(s)** to select the VoIP OUI prefix to be added in the format AA:BB:CC. Up to 128 OUIs can be configured.
2. Use **Description** to enter the description for the OUI. The maximum length of description is 32 characters.
3. The following OUIs are present in the configuration by default:
   - 00:01:E3 - SIEMENS
   - 00:03:6B - CISCO1
   - 00:12:43 - CISCO2
   - 00:0F:E2 - H3C
   - 00:60:B9 - NITSUKO
   - 00:D0:1E - PINTEL
   - 00:E0:75 - VERILINK
   - 00:E0:BB - 3COM
   - 00:04:0D - AVAYA1
   - 00:1B:4F - AVAYA2

4. Click **Add** to add a new telephony OUI entry.
5. Click **Delete** to delete a created entry.
6. Click **Cancel** to cancel the configuration on the screen. Reset the data on the screen to the latest value of the switch.

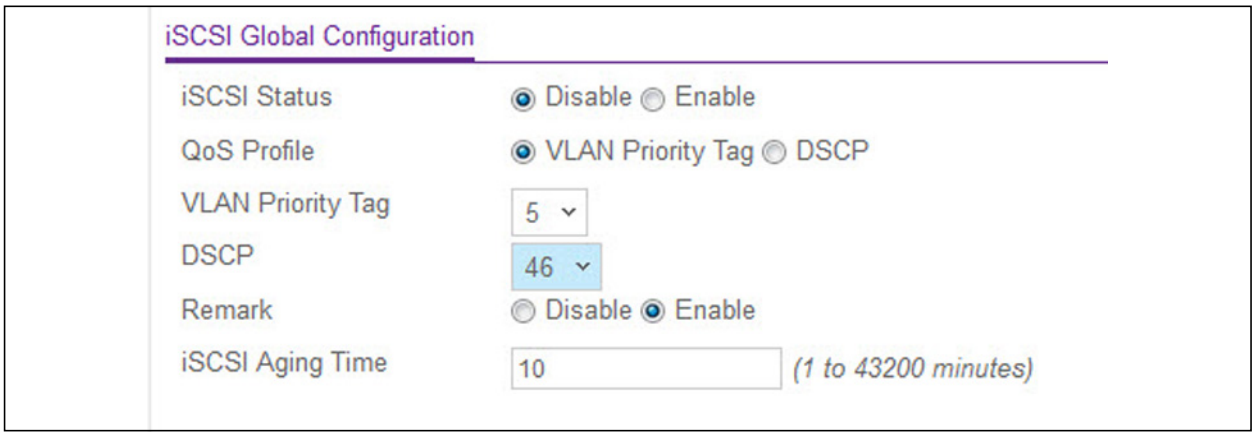
iSCSI

Use this page to view and manage iSCSI Optimization settings on the device. iSCSI Optimization provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment. This is accomplished by monitoring traffic to detect packets used by iSCSI stations to establish iSCSI sessions and connections. Data from these exchanges is used to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port based on these rules.

In addition, if configured, the packets can be updated with IEEE 802.1 or IP-DSCP values. This is done by enabling Remark. Remarking packets with priority data provides special QoS treatment as the packets continue through the network.

iSCSI Global Configuration

- To display the iSCSI Global Configuration page, click **Switching > iSCSI > Basic > Global Configuration**. The following page is displayed.



- Globally configure the iSCSI settings.

1. In the iSCSI Status field, select **Enable** or **Disable** to globally enable or disable the iSCSI Optimization feature. By default, iSCSI Optimization is **Disabled**.
2. In the QoS Profile field, select either **VLAN Priority Tag** or **DSCP** to set the Quality of Service (QoS) profile that will be applied to iSCSI flows. iSCSI flows are assigned by default to the highest VLAN Priority Tag/DSCP mapped to the highest queue not used for chassis management or voice VLAN.

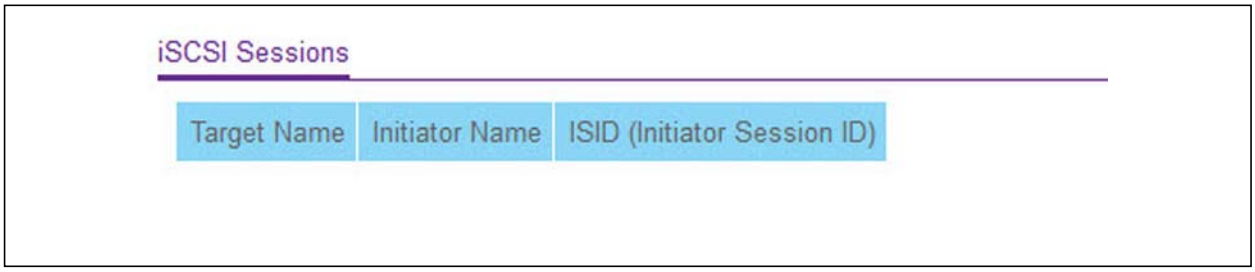
Setting the VLAN Priority Tag/DSCP sets the QoS profile which determines the egress queue to which the frame is mapped. The switch default setting for egress queues scheduling is Weighted Round Robin (WRR). Complete the QoS setting by configuring the relevant ports to work in other scheduling and queue management modes via the Class of Service settings. Depending on the platform, these choices may include strict priority for the queue used for iSCSI traffic. The downside of strict priority is that, in certain circumstances (under heavy high priority traffic), other lower priority traffic may get starved. In WRR, the queue to which the flow is assigned to can be set to get the required percentage.

3. Configure the global traffic class mapping in Class of Service. The global traffic class mapping configuration determines the traffic class used to transmit iSCSI packets. The traffic mapping configuration options are:
   - IEEE 802.1P
   - IP-DSCP

   The configuration of the CoS component determines changes in the mapping of IEEE 802.1p or IP-DSCP values to traffic classes. For more information, see *Class of Service* on page 370.
4. Select the VLAN Priority Tag from the menu to assign the iSCSI session packets. The range is 0 to 7. The default is 5.
5. Select the DSCP value from the menu to assign iSCSI session packets. The range is 0 to 63. The default is 46.
6. Use the Remark field to **Enable** or **Disable** the marking of iSCSI frames with the configured VLAN Priority Tag/DSCP when egressing the switch. Enabling Remark updates the packets with IEEE 802.1p or IP-DSCP values. Remarking packets with priority data provides special QoS treatment as the packets continue through the network. Remark is enabled by default.
7. Configure the iSCSI Aging Time—the number of minutes a session must not be active prior to it's removal. iSCSI Aging Time must be a whole number in the range of 1 to 43200 minutes. The default is 10 minutes.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

iSCSI Sessions

- To display the iSCSI Sessions page, click **Switching > iSCSI > Basic > Sessions**. The following page is displayed.



The *Table 71* describes the non-configurable iSCSI Sessions information.

Table 71. iSCSI Sessions

Field	Description
Target Name	Displays the target's name.
Initiator Name	Displays the initiator's name.
Initiator Session ID (ISID)	The iSCSI identifier.

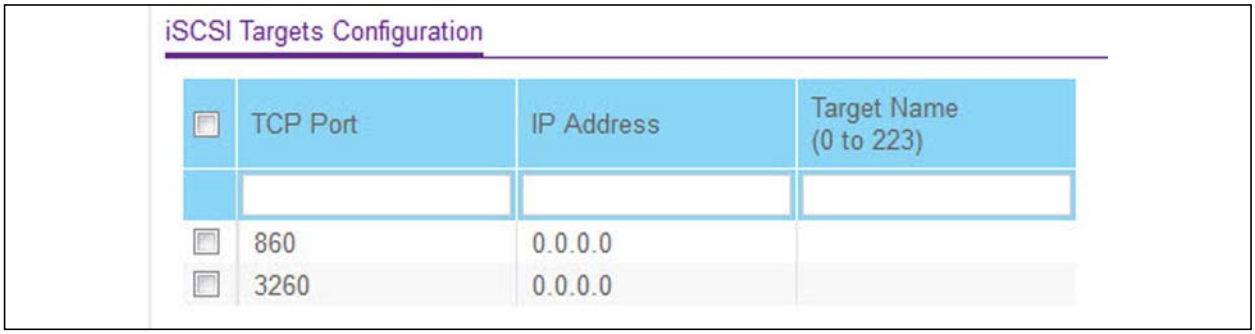
Click **Update** to update the page with the latest information on the switch.

iSCSI Targets Configuration

Use the iSCSI Targets screen to configure iSCSI targets.

- To configure iSCSI targets:

1. Click **Switching > iSCSI > Advanced > iSCSI Targets**. The following page is displayed.



2. Enter a **TCP Port** number on which an iSCSI target listens to requests. Up to 16 TCP ports can be defined in the system. iSCSI well-known ports 860 and 3260 are configured as defaults but you can remove them as any other configured target.

3. Enter the **IP address** of the iSCSI target. The default is 0.0.0.0.
4. Enter the iSCSI name of the iSCSI target. The iSCSI **Target Name** can be up to 233 characters in length.
5. Click **Add** to add the new iSCSI targets configuration.
6. Click **Delete** to delete a selected iSCSI targets configuration.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

iSCSI Sessions Detailed

Use the iSCSI Sessions Detailed screen to display detailed information about iSCSI sessions.

1. Click **Switching > iSCSI > Advanced > Sessions Detailed**.

The *Table 72* describes the non-configurable iSCSI Sessions Detailed information.

Table 72. iSCSI Sessions Detailed

Field	Description
Session Index	The list of session indices.
The rest of the fields on this page correspond to the currently selected Session Index.	
Target Name	The target's name.
Initiator Name	The initiator's name.
Up Time	The time elapsed since the creation of the current session.
Time for Aging Out (in Seconds)	The time left for the current session to expire in seconds.
Initiator Session ID (ISID)	The unique identifier an initiator assigns to its session endpoint which, when combined with the iSCSI initiator name, provides a unique name for the iSCSI initiator port.
Initiator IP Address	The initiator's IP address.
Initiator TCP Port	The initiator's TCP port number of one of the connections between the target and initiator.
Target IP Address	The IP address of the target.
Target TCP Port	The target's TCP port number of one of the connections between the target and initiator.

Click **Update** to update the page with the latest information on the switch.

Spanning Tree Protocol

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

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information on configuring Common STP, see “CST Port Configuration” on page 3-159.

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

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

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

- *Basic* on page 152
- *Advanced* on page 154

Basic

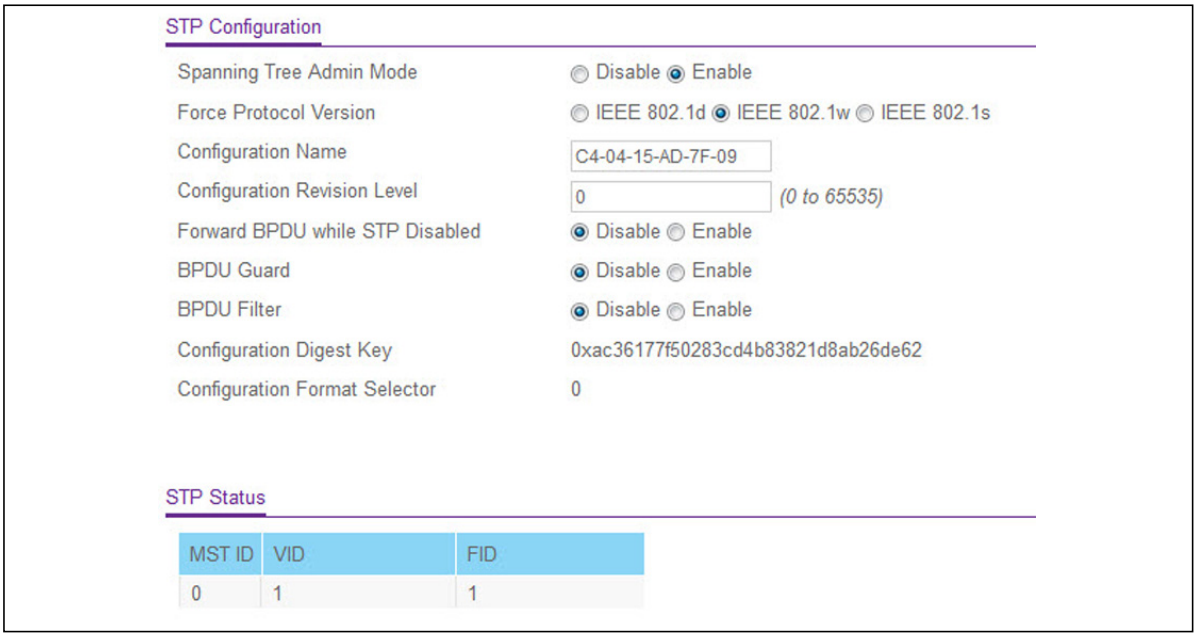
From the Basic link, you can access the following pages:

- *STP Configuration* on page 152

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**.



1. Use **Spanning Tree Admin Mode** to specify whether spanning tree operation is enabled on the switch. Value is enabled or disabled.
2. Use **Force Protocol Version** to specify the Force Protocol Version parameter for the switch. The options are IEEE 802.1d, IEEE 802.1w and IEEE 802.1s.
3. Use **Configuration Name** to specify an identifier used to identify the configuration currently being used. It may be up to 32 alphanumeric characters.
4. Use **Configuration Revision Level** to specify an identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0.
5. Use **Forward BPDU while STP Disabled** to specify whether spanning tree BPDUs should be forwarded or not while spanning-tree is disabled on the switch. Value is enabled or disabled.
6. Use **BPDU Guard** to specify whether the BPDU guard feature is enabled. The STP BPDU guard allows a network administrator to enforce the STP domain borders and keep the active topology consistent and predictable. The switches behind the edge ports that have STP BPDU guard enabled will not be able to influence the overall STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that is configured with this option and transitions the port into disable state. This would lead to an 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.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. 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
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

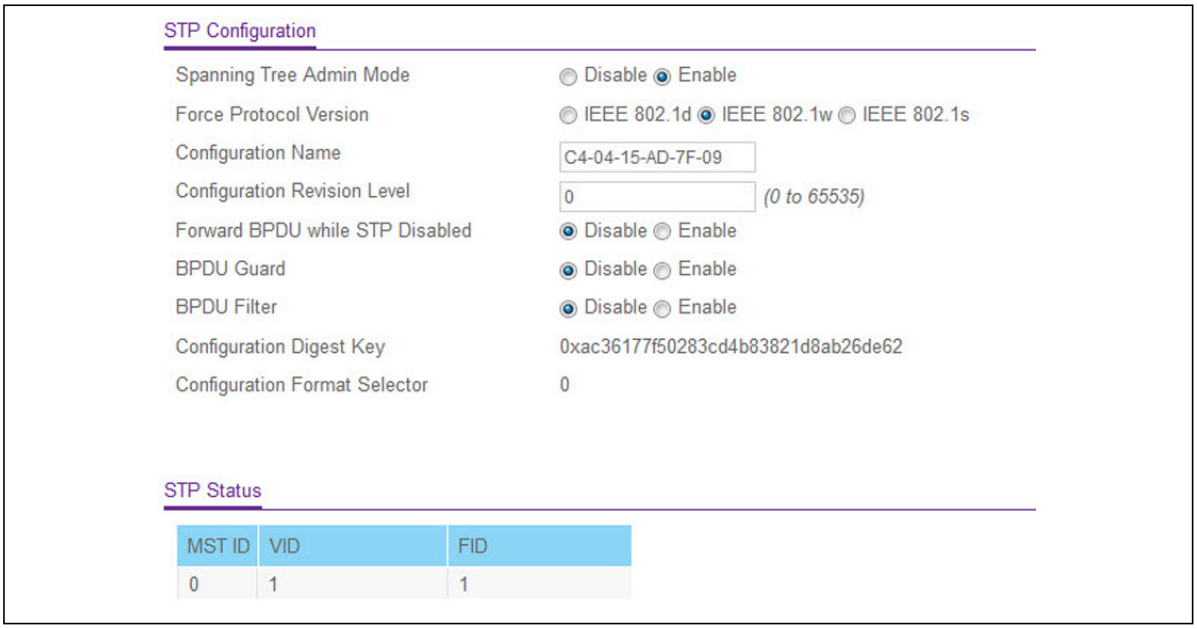
From the Advanced link, you can access the following pages:

- *STP Configuration* on page 154
- *CST Configuration* on page 156
- *CST Port Configuration* on page 159
- *CST Port Status* on page 160
- *MST Configuration* on page 162
- *MST Port Status* on page 164
- *STP Statistics* on page 165

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**.



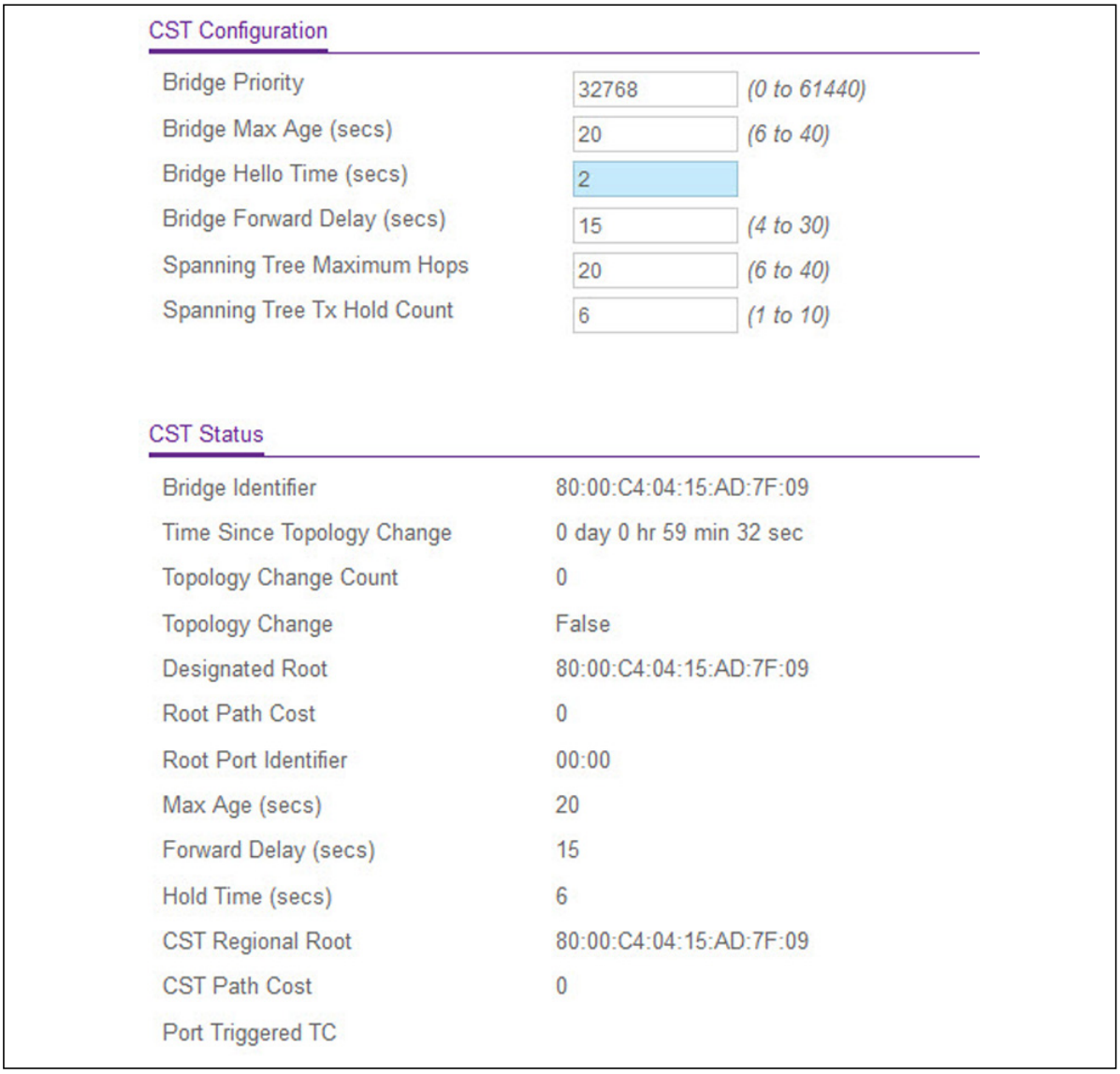
1. Use **Spanning Tree Admin Mode** to specify whether spanning tree operation is enabled on the switch. Value is enabled or disabled. The default is **Enable**.
2. Use **Force Protocol Version** to specify the Force Protocol Version parameter for the switch. The options are IEEE 802.1d, IEEE 802.1w, and IEEE 802.1s. The default is **IEEE 802.1w**.
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. The default is **Disable**.
6. Use **BPDU Guard** to specify whether the BPDU guard feature is enabled or disabled. The default is **Disable**. 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 an administrative disable of the port.
7. Use **BPDU Filter** to specify whether the BPDU Filter feature is enabled or disabled. The default is **Disable**. 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.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. 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
Configuration digest key	Identifier used to identify the configuration currently being used.
STP Status	
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**.



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 * Bridge Forward Delay) – 1 and greater than or equal to 2 * (Bridge Hello Time +1). The default value is **20**.

- **Bridge Hello Time (secs)** - Specifies the 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 (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 (Bridge Max Age / 2) + 1. The time range is from 4 seconds to 30 seconds. The default value is **15** seconds.
- **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 6–40. The default is 20 hops.
- **Spanning Tree Tx Hold Count** - Configures the maximum number of bpdus the bridge is allowed to send within the hello time window. The valid range is 1–10. The default value is 6.

2. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. Click **Update** to update the page with the latest information on the switch.

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.

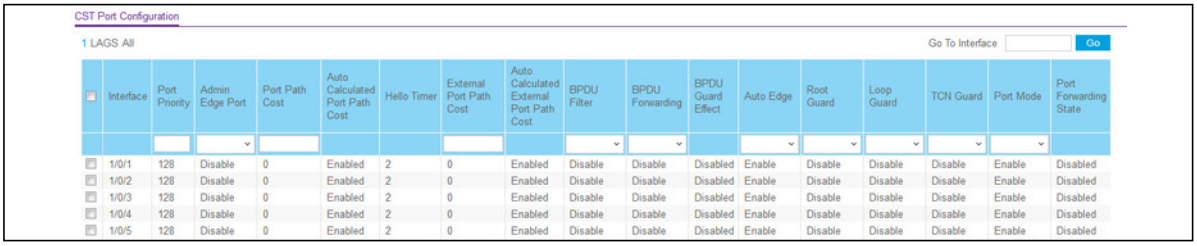
Field	Description
Forward Delay(secs)	Derived value of the Root Port Bridge Forward Delay parameter.
Hold Time(secs)	Minimum time between transmission of Configuration BPDUs.
CST Regional Root	Priority and base MAC address of the CST Regional Root.
CST Path Cost	Path Cost to the CST tree Regional Root.

CST Port Configuration

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

A port can become *Diagnostically Disabled* (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria is such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

To display the Spanning Tree CST Port Configuration page, click **Switching > STP > Advanced** > **CST Port Configuration**.



To configure CST port settings:

1. **Interface** - One of the physical or port channel interfaces associated with VLANs associated with the CST.
2. Use **Port Priority** to specify the priority for a particular port within the CST. The port priority is set in multiples of 16. For example if the priority is attempted to be set to any value between 0 and 15, it will be set to 0. If it is tried to be set to any value between 16 and (2*16-1) it will be set to 16 and so on. The default value is **128**.
3. Use **Admin Edge Port** to specify if the specified port is an Edge Port within the CIST. Use the menu to select Disable or Enable. The default value is **Disable**.
4. Use **Port Path Cost** to set the Path Cost to a new value for the specified port in the common and internal spanning tree. It takes a value in the range of 1 to 200000000. The default is **0**.
5. Use **External Port Path Cost** to set the External Path Cost to a new value for the specified port in the spanning tree. It takes a value in the range of 1 to 200000000. The default is **0**.
6. Use **BPDU Filter** to configure the BPDU Filter, which filters the BPDU traffic on this port when STP is enabled on this port. The possible values are Enable or Disable. The default value is **Disable**.

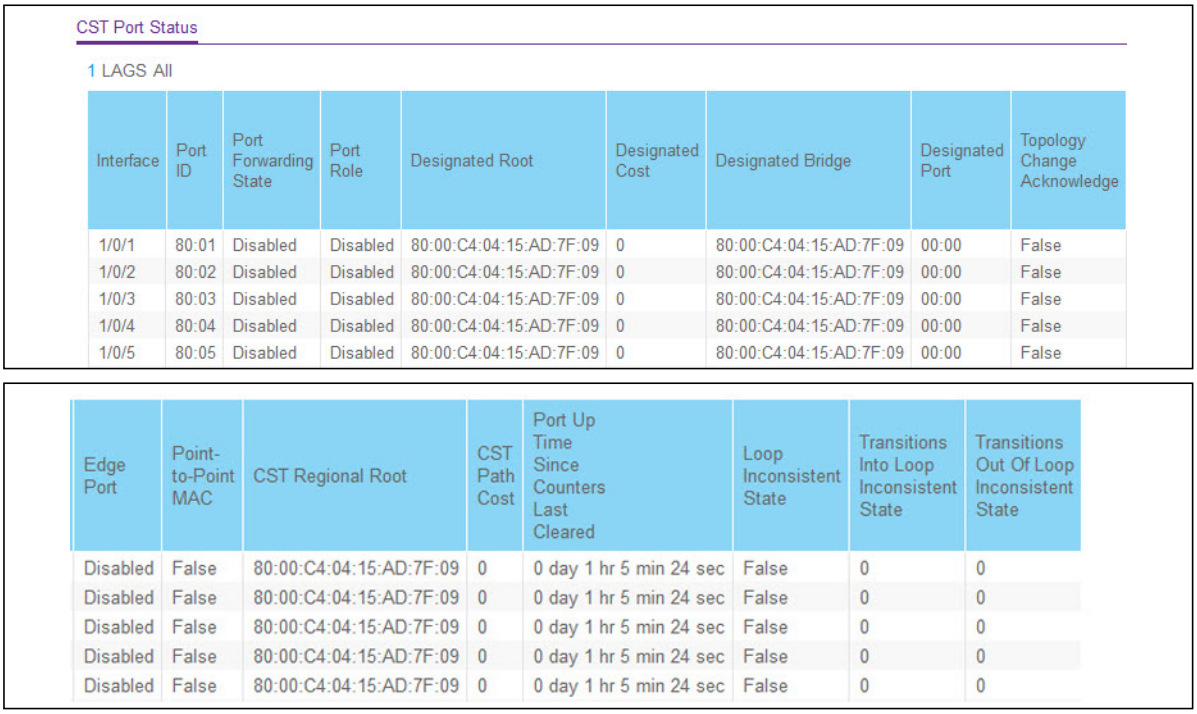
7. Use **BPDU Flood** to configure the BPDU Flood, which floods the BPDU traffic arriving on this port when STP is disabled on this port. The possible values are Enable or Disable. The default value is **Disable**.
8. Use **Auto Edge** to configure the auto edge mode of a port, which allows the port to become an edge port if it does not see BPDUs for some duration. The possible values are Enable or Disable. The default value is **Enable**.
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. The default value is **Disable.**
10. Use **Loop Guard** to enable or disable 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. The default value is **Disable**
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. The default value is **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. The default value is **Disable**
13. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
14. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
15. Click **Update** to update the page with the latest information on the switch.

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 the 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

1 LAGS All

Interface	Port ID	Port Forwarding State	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port	Topology Change Acknowledge
1/0/1	80:01	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/2	80:02	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/3	80:03	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/4	80:04	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/5	80:05	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False

Edge Port	Point-to-Point MAC	CST Regional Root	CST Path Cost	Port Up Time Since Counters Last Cleared	Loop Inconsistent State	Transitions Into Loop Inconsistent State	Transitions Out Of Loop Inconsistent State
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0

The following table describes the CST Status information displayed on the screen. Click **Update** to update the page with the latest information on the switch.

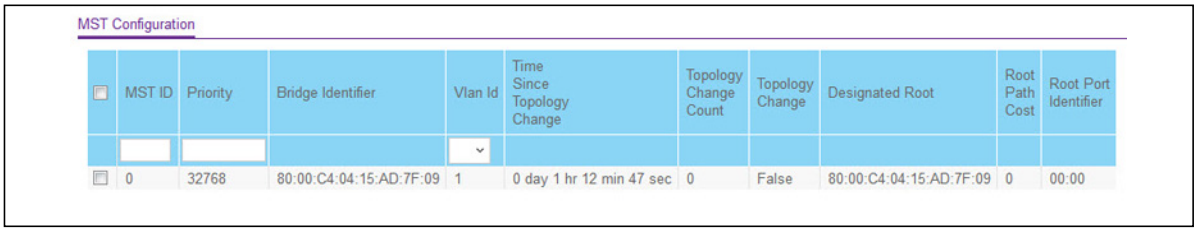
Field	Description
Interface	Identify the physical or port channel interfaces associated with VLANs associated with the CST.
Port ID	The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
Port Forwarding State	The Forwarding 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.

Field	Description
Designated Bridge	Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Topology Change Acknowledge	Identifies whether the next BPDU to be transmitted for this port would have the topology change acknowledgement flag set. It is either “True” or “False”.
Edge port	Indicates whether the port is enabled as an edge port. It takes the value “Enabled” or “Disabled”.
Point-to-point MAC	Derived value of the point-to-point status.
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
CST Path Cost	Path Cost to the CST Regional Root.
Port Up Time Since Counters Last Cleared	Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.
Loop Inconsistent State	This parameter identifies whether the port is in loop inconsistent state or not.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out Of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

MST Configuration

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

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



To configure an MST instance:

1. 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. Click **Add** to create a new MST which you have configured.
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.
5. To delete an MST instance, select the check box next to the instance and click **Delete**.
6. Click **Update** to update the page with the latest information on the switch.

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

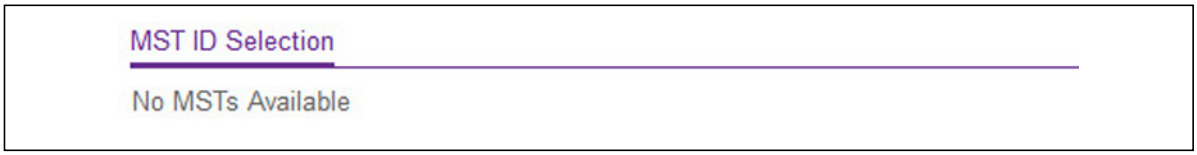
Field	Description
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time n seconds since the topology of the selected MST instance last changed.
Topology Change Count	Number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

MST Port Status

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

A port can become *Diagnostically Disabled* (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria is such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

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

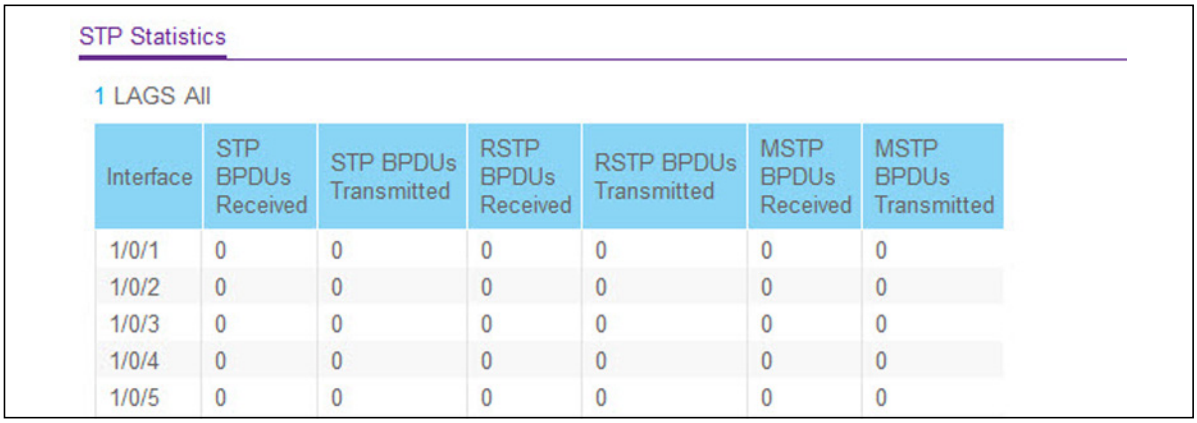
The following table describes the read-only MST port configuration information displayed on the Spanning Tree CST Configuration page.

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.
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 following table describes the information available on the STP Statistics page. Click **Update** to update the page with the latest information on the switch.

Field	Description
Interface	Selects one of the physical or port channel interfaces of the switch.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.

Multicast

Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255.

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

- *MFDB* on page 167
- *IGMP Snooping* on page 168
- *MLD Snooping* on page 176

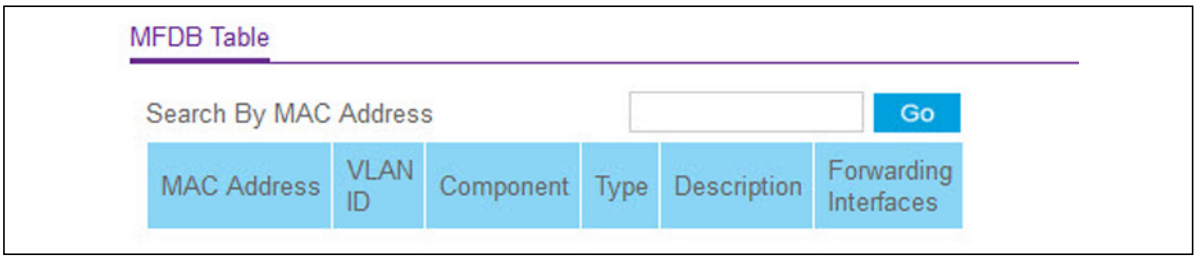
MFDB

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

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**.

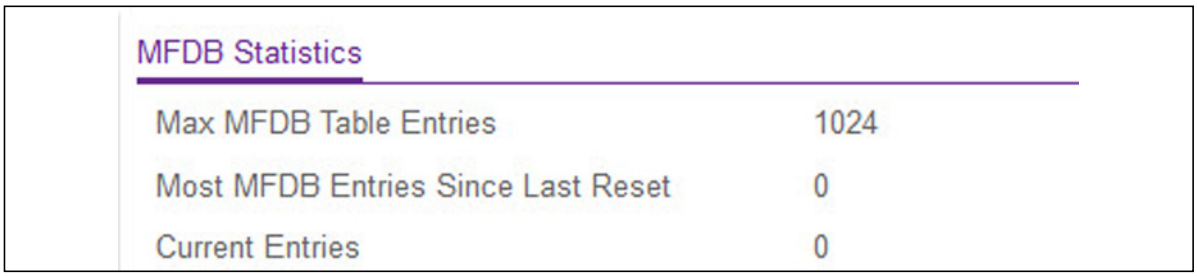


1. Use **Search by MAC Address** to enter a MAC Address whose MFDB table entry you want displayed. Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67. Then click on the “GO” button. If the address exists, that entry will be displayed. An exact match is required.

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.
Forwarding Interfaces	The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

MFDB Statistics

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



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.

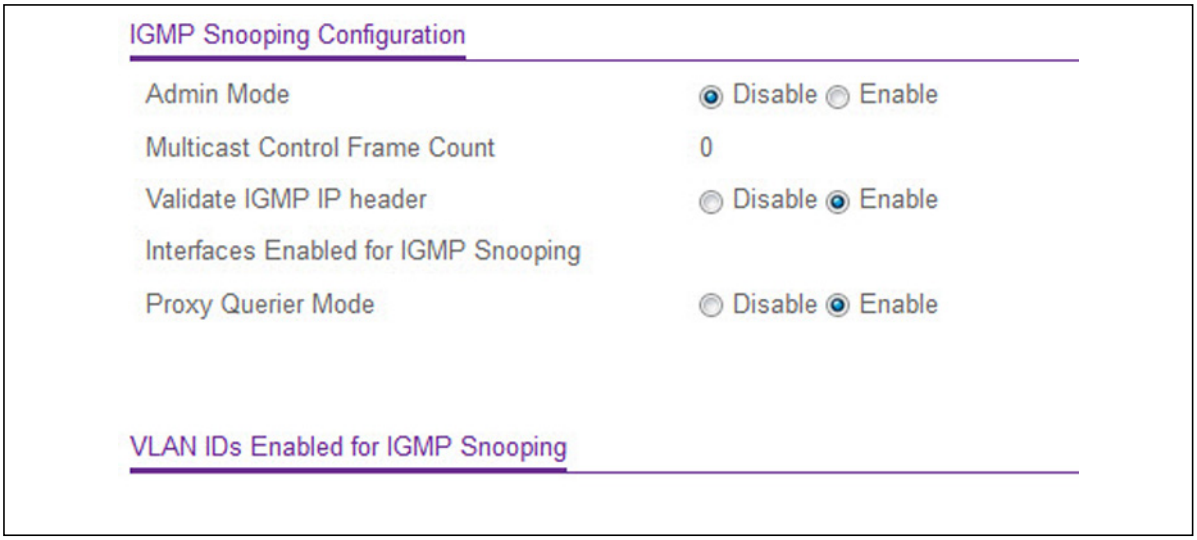
From the IGMP Snooping link, you can access the following pages:

IGMP Snooping Configuration

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

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

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



To configure IGMP Snooping:

1. Use the **Admin Mode** Enable/Disable radio button to select the administrative mode for IGMP Snooping for the switch. The default is **Disable**.
2. Use the **Validate IGMP IP header** option to **Enable** or **Disable** header validation for all IGMP versions. If Validate IGMP IP Header is enabled, then IGMP IP header checks for Router Alert option, ToS and TTL. The default value is **Enable**.

3. Use the **Proxy Querier Model** field to **Enable** or **Disable** IGMP Proxy Querier on the system. If disabled, then the IGMP proxy query with source IP 0.0.0.0 is not sent in response to IGMP leave packet. the default value is **Enable**.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Update** to update the page with the latest information on the switch.

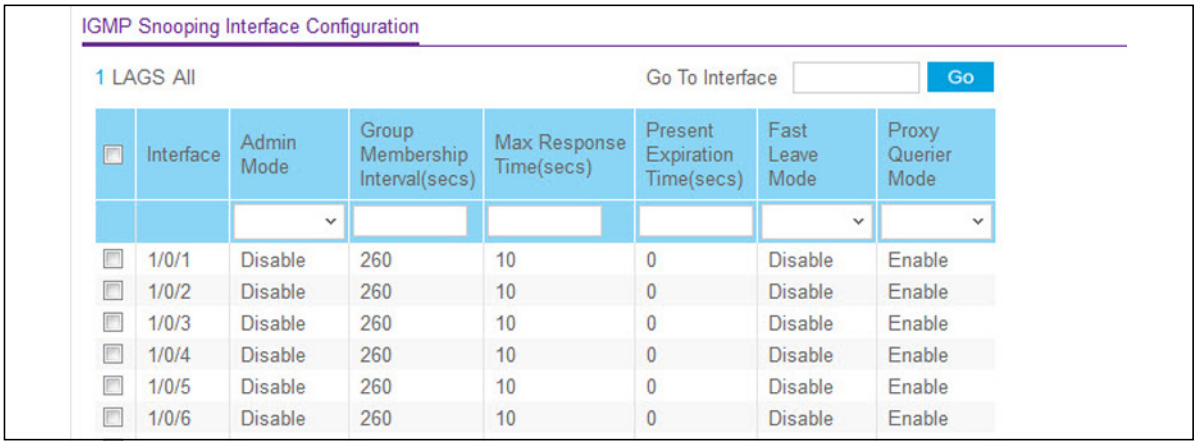
The following table displays information about the global IGMP Snooping status and statistics on the page.

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.
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**.



To configure IGMP Snooping interface settings:

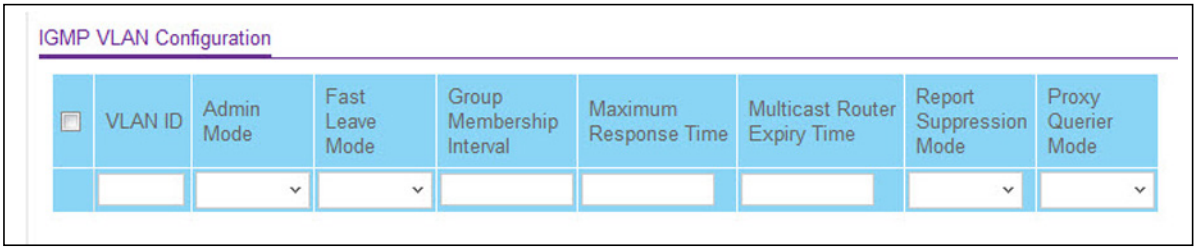
1. Interface: Lists all physical, VLAN, and LAG interfaces. Select the interface you want to configure.
2. Use **Admin Mode** to select the interface mode for the selected interface for IGMP Snooping for the switch from the menu. The default is disable.

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 a particular interface from the menu. The default is disable.
7. Use **Proxy Querier Mode** to select the Proxy Querier mode for a particular interface from the menu. If it is disabled, then IGMP proxy query with source IP 0.0.0.0 is not sent in response to IGMP leave packet. The default value is Enable.
8. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
9. If you make 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**.



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.

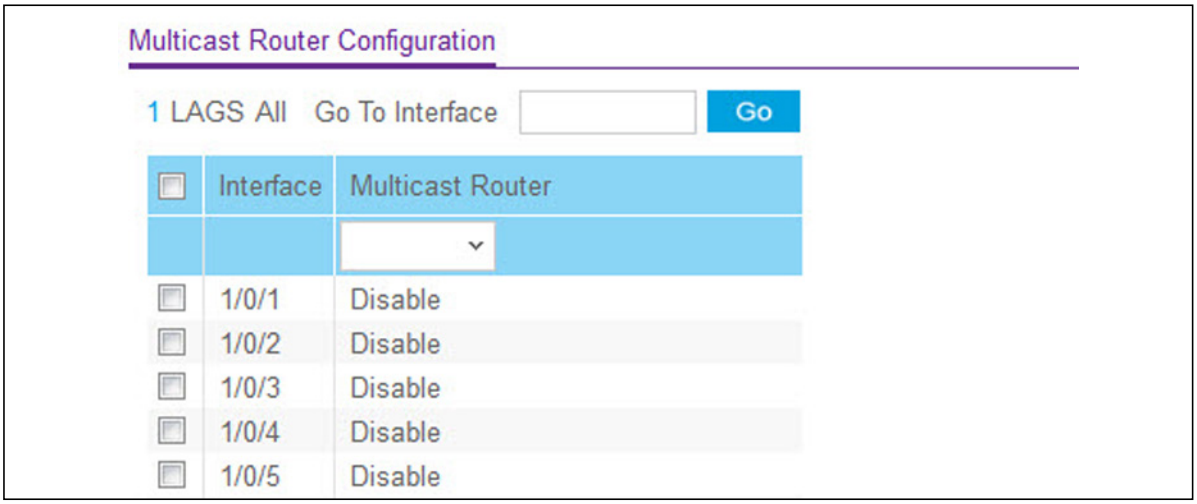
- Use **Maximum Response Time** to set the value for maximum response time of IGMP Snooping for the specified VLAN ID. Valid range is 1 to (Group Membership Interval - 1). Its value should be greater than group membership interval value.
- Use **Multicast Router Expiry Time** to set the value for multicast router expiry time of IGMP Snooping for the specified VLAN ID. Valid range is 0 to 3600 seconds.
- Use **Report Suppression Mode** to enable or disable IGMP Snooping Report Suppression mode for the specified VLAN ID. IGMP Snooping Report Suppression allows the suppression of the IGMP reports sent by the multicast hosts by building a Layer 3 membership table, thereby sending only the very needed reports to the IGMP Routers to receive the multicast traffic. As a result, the multicast report traffic being sent to the IGMP Routers is reduced.
- **Enable** or **Disable** the **Proxy Querier Mode** for the specified VLAN ID. If Proxy Querier Mode is disabled, then IGMP proxy query with source IP 0.0.0.0 is not sent in response to an IGMP leave packet. The default is Enable.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. To disable IGMP Snooping on a VLAN and remove it from the list, select the check box next to the VLAN ID and click **Delete**.
4. To modify IGMP Snooping settings for a VLAN, select the check box next to the VLAN ID, update the desired values, and click **Apply**.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Multicast Router Configuration

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

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

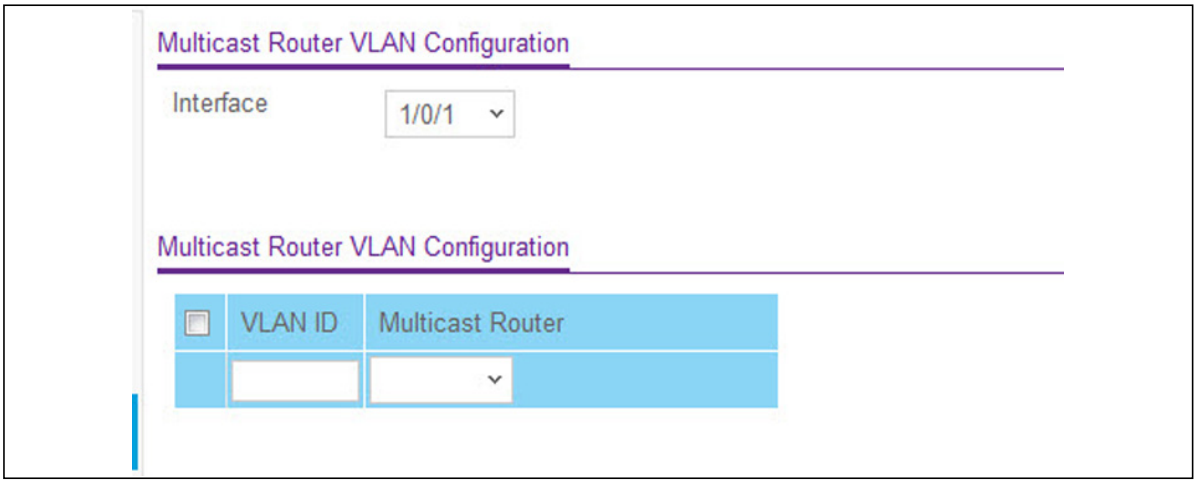


1. Use **Interface** to select the physical interface for which you want Multicast Router to be enabled.
2. Use **Multicast Router** to enable or disable Multicast Router on the selected interfaces.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Multicast Router VLAN Configuration

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

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



1. Use **Interface** to select the interface for which you want Multicast Router to be enabled or to be displayed.
2. Use **VLAN ID** to select the VLAN ID for which the Multicast Router Mode is to be Enabled or Disabled.
3. Use **Multicast Router** to enable or disable multicast router for the VLAN ID.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IGMP Snooping Querier

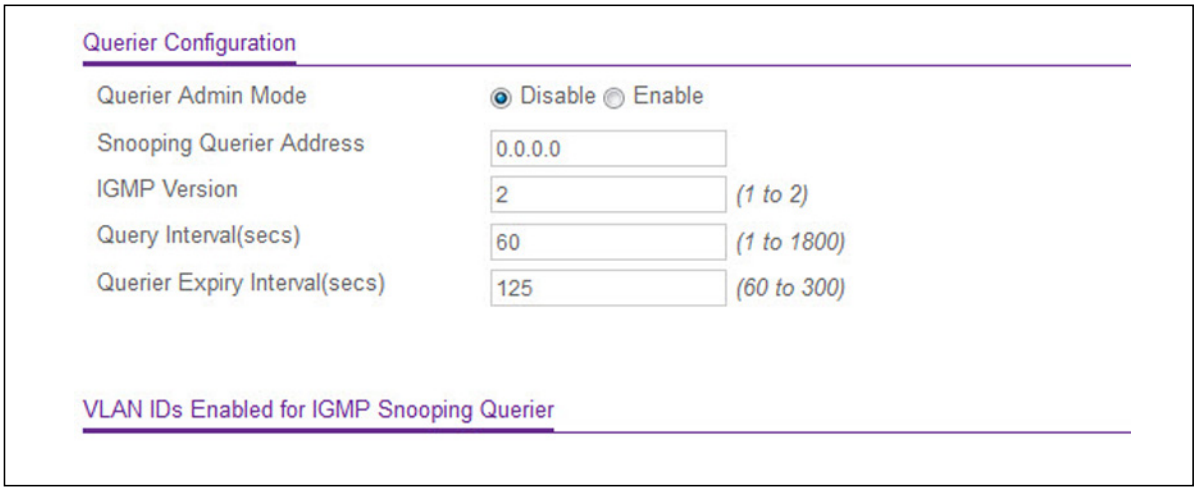
IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP Querier. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership 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**.

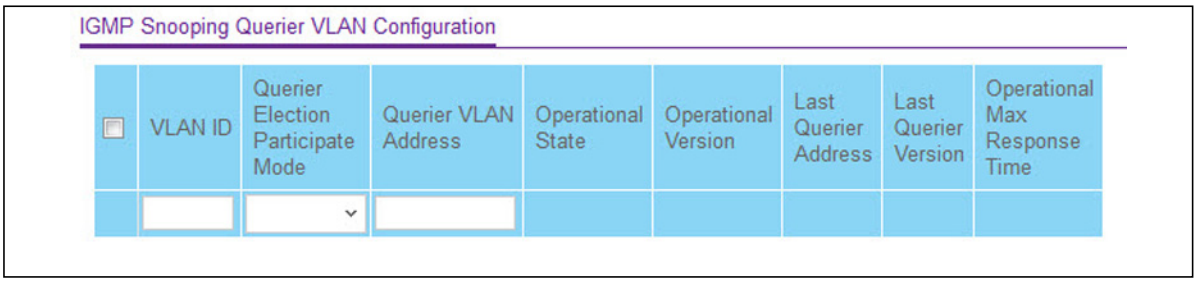
2. Use **Querier IP Address** to specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.
3. Use **IGMP Version** to specify the IGMP protocol version used in periodic IGMP queries. The range is 1 to 2. The default value is **2**.
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 **125**.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Field	Description
VLAN IDs Enabled For IGMP Snooping Querier	Displays VLAN IDs enabled for IGMP Snooping Querier.

IGMP Snooping Querier VLAN Configuration

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

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



To configure Querier VLAN settings:

1. 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.

2. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately
3. To disable Snooping Querier on a VLAN, select the VLAN ID and click **Delete**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Update** to update the page with the latest information on the switch.

Field	Description
Operational State	Displays the operational state of the IGMP Snooping Querier on a VLAN. It can be in any of the following states: • 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. • Non-Querier: Snooping switch is in Non-Querier mode in the VLAN. If the Querier expiry interval timer is expired, the Snooping switch will move into Querier mode. • 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.
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.

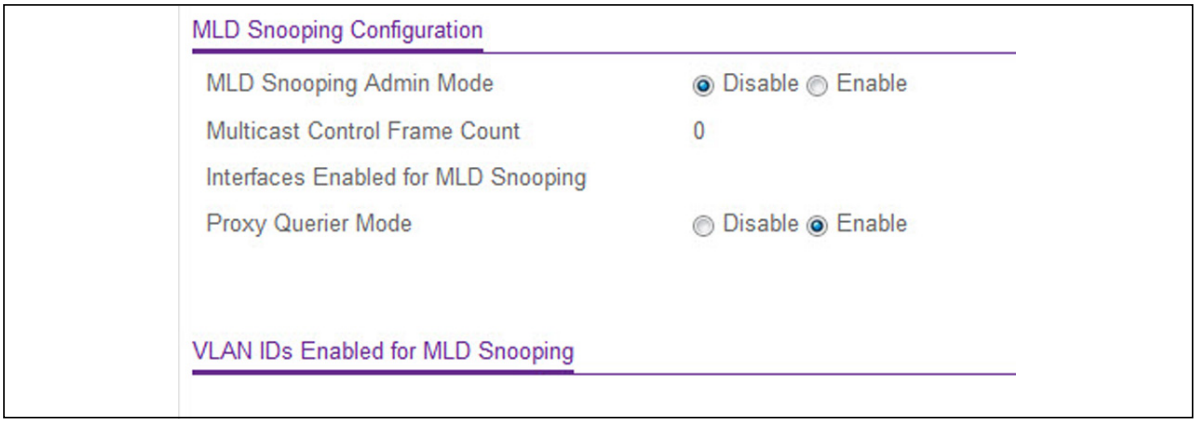
MLD Snooping

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

MLD Snooping Configuration

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**.
2. Select the **Proxy Querier Mode** to **Enable** or **Disable** MLD Proxy Querier on the system. If it is disabled, then MLD Proxy query with source IP 0::0 is not sent in response to an MLD leave packet. If it is enabled, then MLD Proxy queries are sent. The default value is **Enable**.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Update** to update the page with the latest information on the switch.

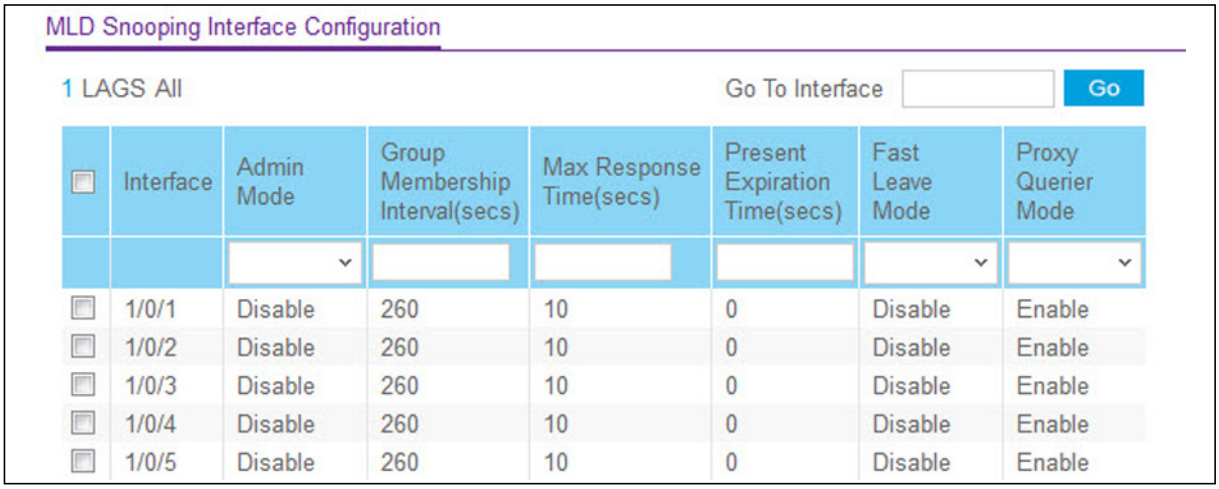
Table 73 describes the non-configurable MLD Snooping Configuration fields.

Table 73. MLD Snooping Configuration

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.
VLAN IDs Enabled For MLD Snooping	Displays VLAN IDs enabled for MLD Snooping.

MLD Snooping Interface Configuration

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

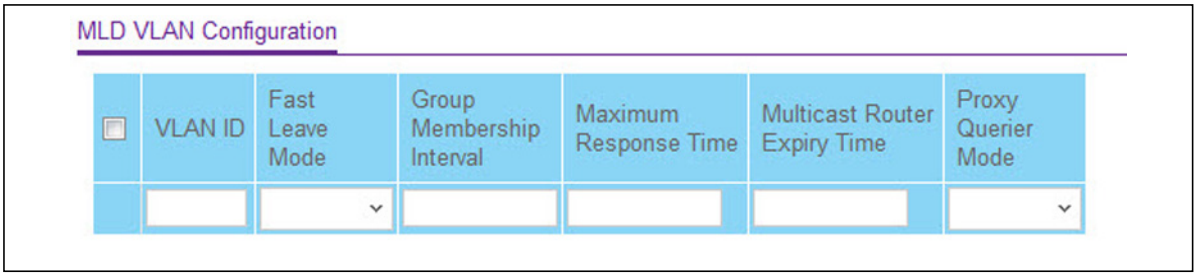


1. **Interface** - Displays all physical, VLAN, and LAG interfaces. Select the interface you want to configure.
2. Use **Admin Mode** to select the interface mode for the selected interface for MLD Snooping for the switch. The default is disable.
3. Use **Group Membership Interval(secs)** to specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group. The valid range is from (2 to 3600) seconds. The configured value must be greater than Max Response Time. The default is 260 seconds.
4. Use **Max Response Time (secs)** to specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds. The default is 10 seconds. The configured value must be less than the Group Membership Interval.
5. Use **Present Expiration Time** to specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite time-out, i.e. no expiration.

6. Use **Fast Leave Admin mode** to select the Fast Leave mode for a particular interface from the menu. The default is disable.
7. Select the **Proxy Querier Mode** to **Enable** or **Disable** MLD Proxy Querier on the system. If it is disabled, then MLD Proxy query with source IP 0::0 is not sent in response to an MLD leave packet. If it is enabled, then MLD Proxy queries are sent. The default value is **Enable**.

MLD VLAN Configuration

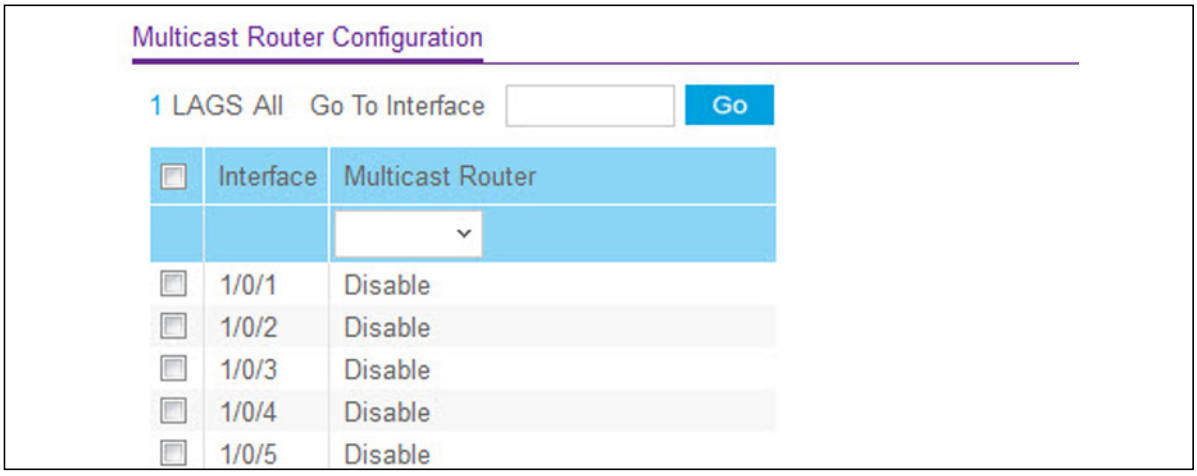
To access the MLD VLAN Configuration page, click **Switching** > **Multicast** > **MLD Snooping** > **MLD VLAN Configuration**.



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

Multicast Router Configuration

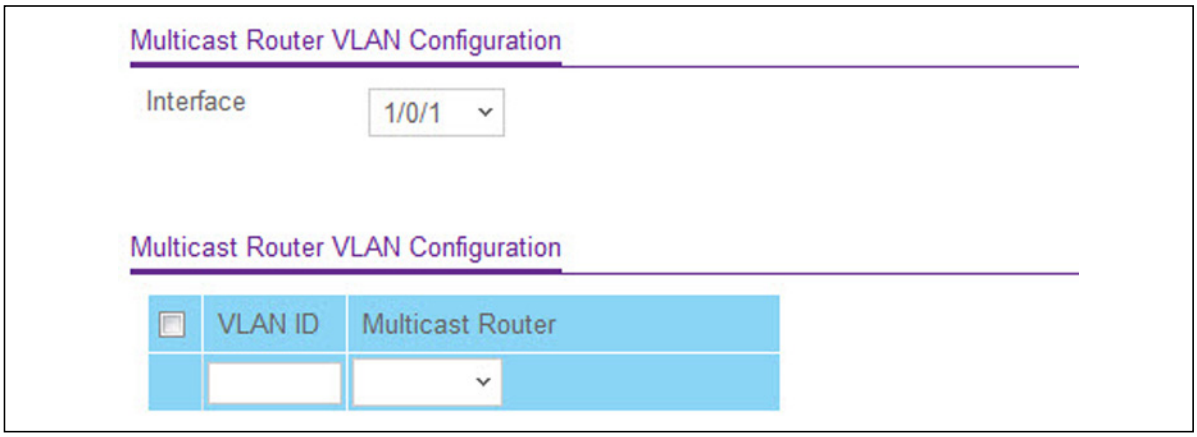
To access the Multicast Router Configuration page, click **Switching** > **Multicast** > **MLD Snooping** > **Multicast Router Configuration**.



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

Multicast Router VLAN Configuration

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

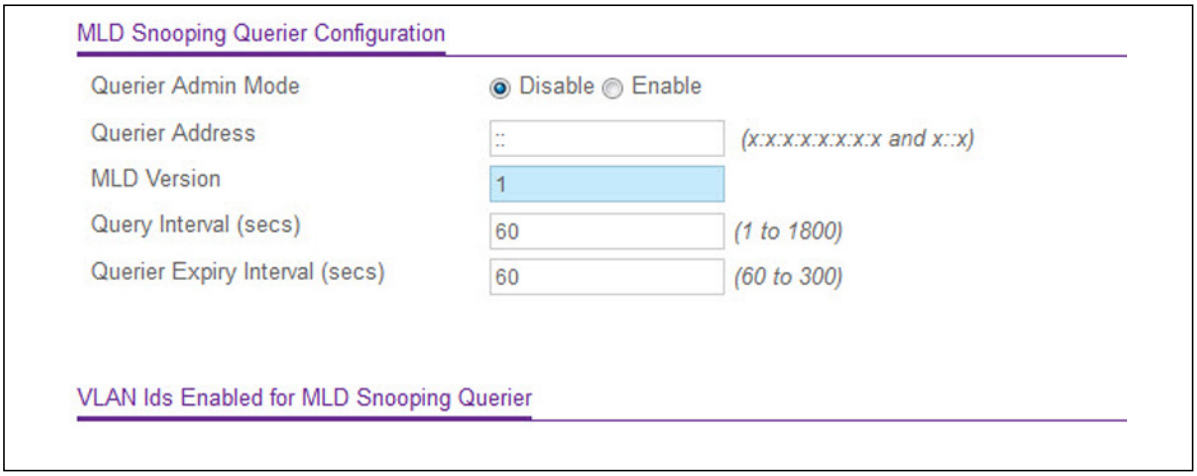


1. Use **Interface** to select the interface for which you want Multicast Router to be enabled.
2. Use **VLAN ID** to select the VLAN ID for which the Multicast Router Mode is to be Enabled or Disabled.
3. Use **Multicast Router** to enable or disable the multicast router for the VLAN ID.

MLD Snooping Querier Configuration

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

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

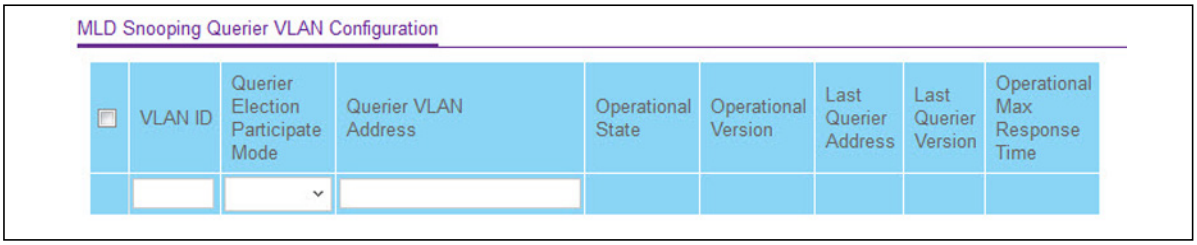


1. Use **Querier Admin Mode** to select the administrative mode for MLD Snooping for the switch. The default is disable.
2. Use **Querier Address** to specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN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

Field	Description
VLAN IDs Enabled For MLD Snooping Querier	Displays VLAN IDs enabled for MLD Snooping Querier.

MLD Snooping Querier VLAN Configuration

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



1. **VLAN ID** - Specifies the VLAN ID on which MLD Snooping Querier is administratively enabled and VLAN exists in the VLAN database.

2. Use **Querier Election Participate Mode** to enable or disable the MLD Snooping Querier participate in election mode. When this mode is disabled, 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	Specifies the operational state of the MLD Snooping Querier on a VLAN. It can be in any of the following states: • 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. • Non-Querier: Snooping switch is in Non-Querier mode in the VLAN. If the Querier expiry interval timer is expired, the Snooping switch will move into Querier mode. • 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.
Operational Version	Displays the operational MLD protocol version of the Querier.
Last Querier Address	Displays the IP address of the last Querier from which a query was snooped on the VLAN.
Last Querier Version	Displays the MLD protocol version of the last Querier from which a query was snooped on the VLAN.
Operational Max Response Time	Displays maximum response time to be used in the queries that are sent by the Snooping Querier.

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 183
- *Advanced* on page 184

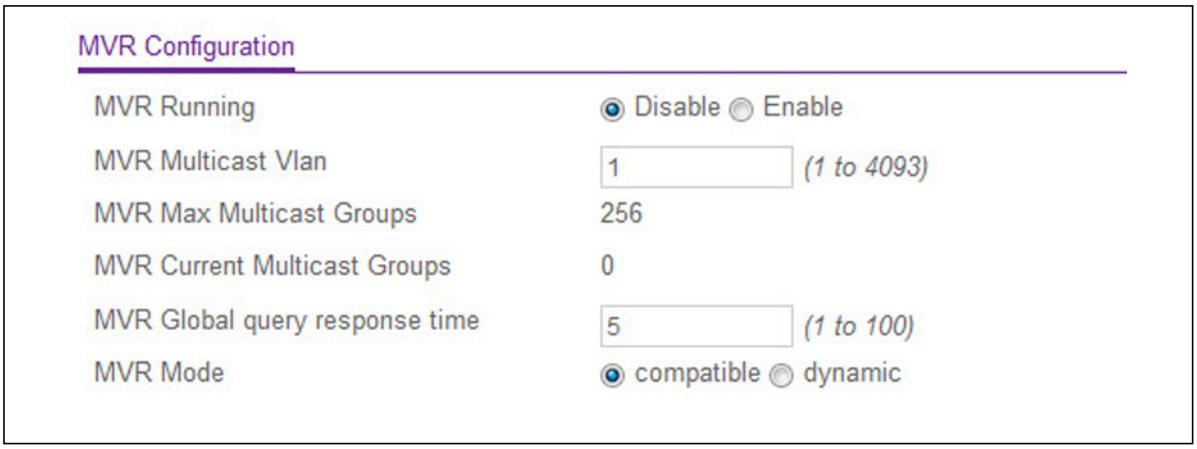
Basic

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

- *MVR Configuration* on page 183

MVR Configuration

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



1. Use **MVR Running** to **Enable** or **Disable** the MVR feature. The factory default is **Disable**.
2. Use **MVR Multicast VLAN** 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 query time 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. Possible values are compatible or dynamic. The factory default is **compatible**.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

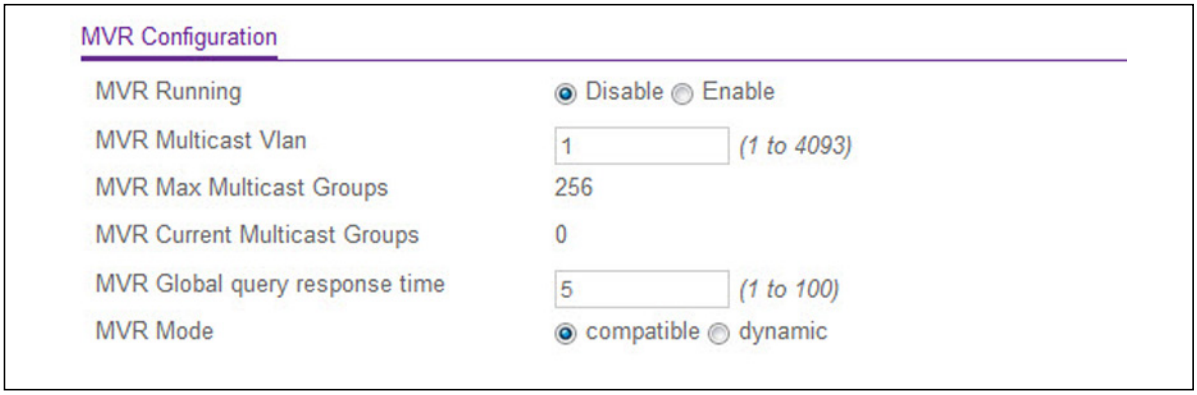
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. Click **Update** to update the page with the latest information on the switch.

Advanced

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

MVR Configuration

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



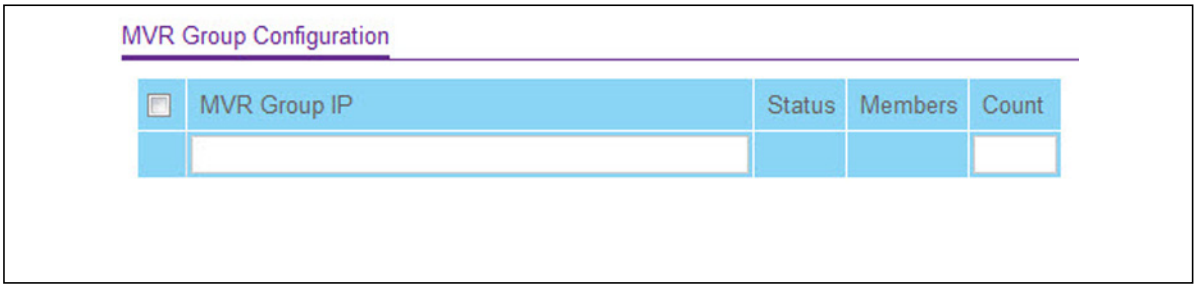
1. Use the **MVR Running** to Enable or Disable the MVR feature. The factory default is Disable.
2. Use the **MVR Multicast VLAN** to specify the VLAN on which MVR multicast data will be received. All source ports belong to this VLAN. The value can be set in a range of 1 to 4094. The default value is 1.
3. Use the **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 query time 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 the **MVR Mode** to specify the MVR mode of operation. The factory default is compatible.
5. Click **Update** to update the page with the latest information on 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. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

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.

MVR Group Configuration

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

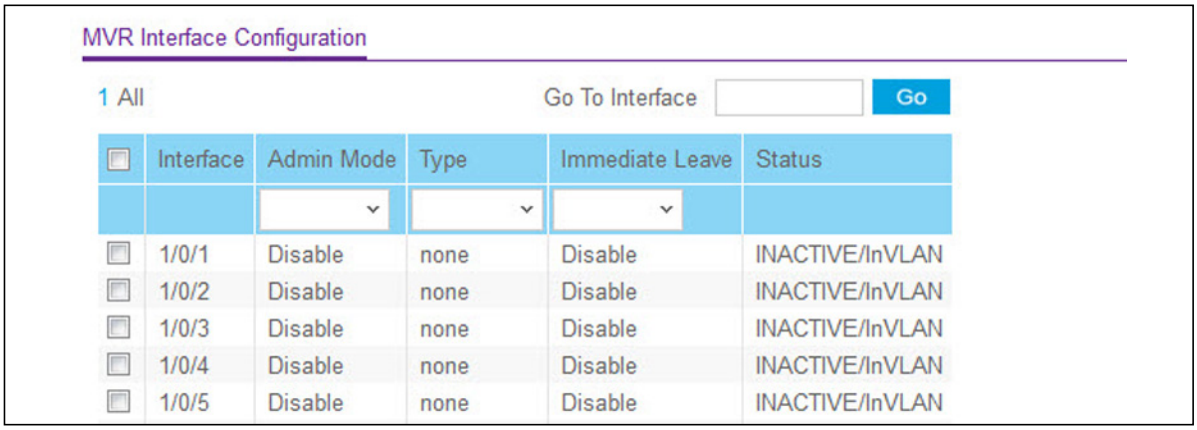


1. Use the **MVR Group IP** to specify the IP Address for the new MVR group.
2. Use the **Count** to specify the number of contiguous MVR groups. It is a service option helping user to create multiple MVR groups via single press of Add button. If the field is empty, then pressing the button creates only one new group. The field is displayed as empty for each particular group. The range is from 1 to 256.
3. Click **Add** to add a new MVR group.
4. Click **Delete** to delete a selected MVR group.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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 is displayed.



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 **Update** to update the page with the latest information on 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. 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

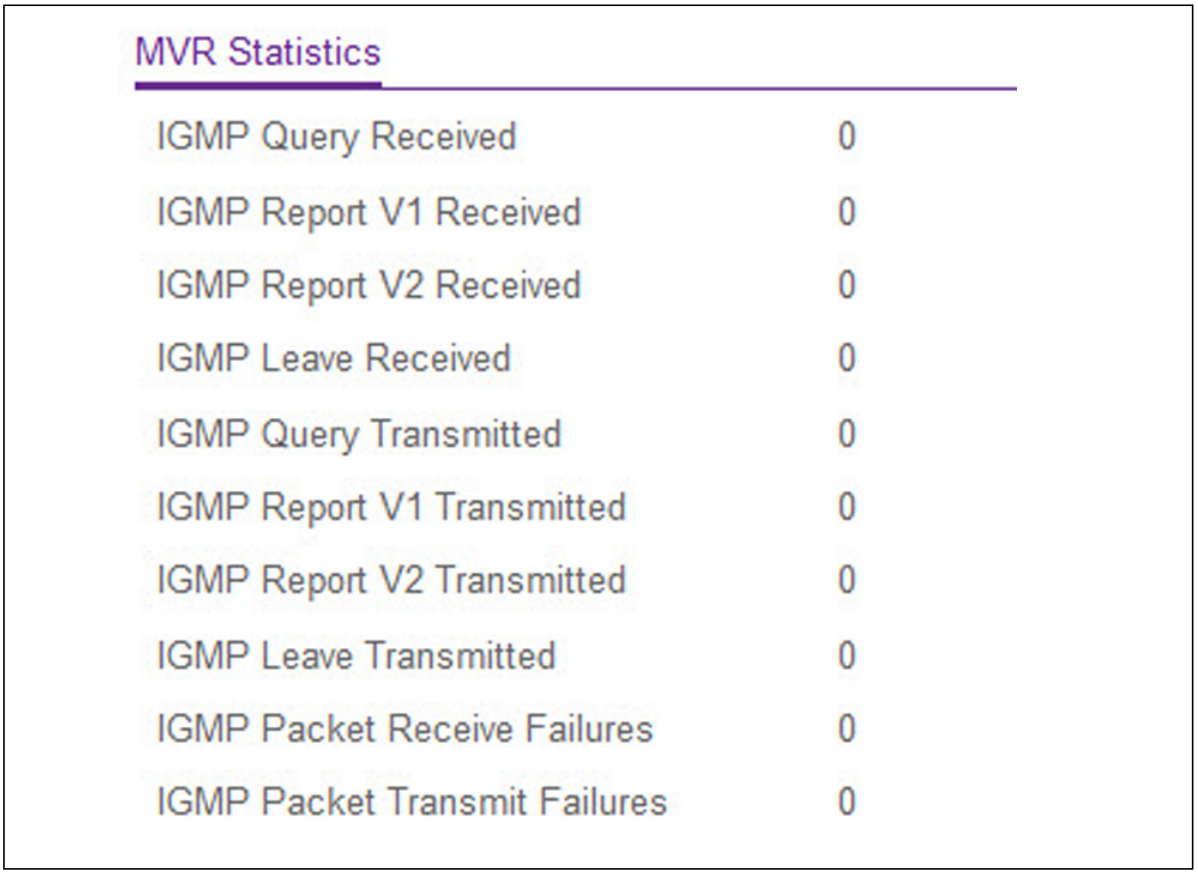
To display the MVR Configuration page, click **Switching** > **MVR** > **Advanced** > **MVR Group Membership**. A screen similar to the following is displayed.

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 show 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 is displayed.



1. Click **Update** to update the page with the latest information on the switch.

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.

Field	Definition
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 188
- *Advanced* on page 189

Basic

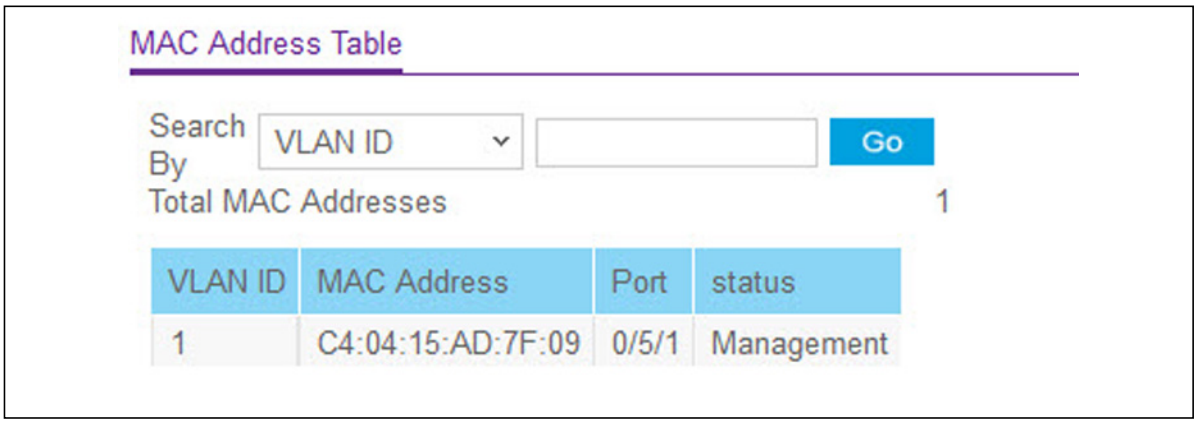
From the Basic link, you can access the following pages:

- *Address Table* on page 188

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**.



1. Use **Search By** to search for MAC Addresses by MAC Address, VLAN ID, and port:
   - **Searched by MAC Address** - Select MAC Address from the 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 the 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 the 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	The status of this entry. The meanings of the values are: • Static: the value of the corresponding instance was added by the system or a user and cannot be relearned. • Learned: the value of the corresponding instance was learned, and is being used. • Management: the value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress.

Advanced

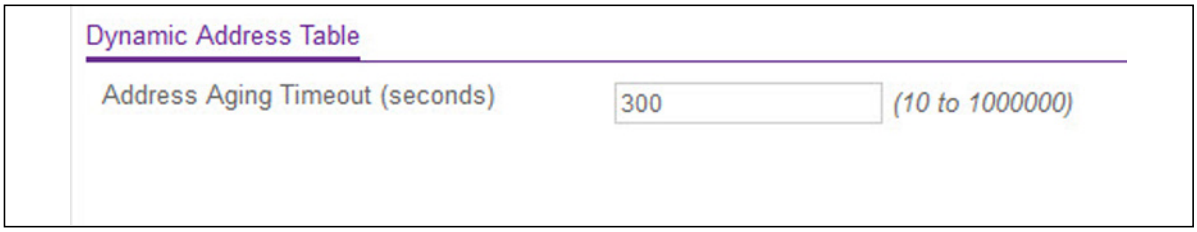
From the Advanced link, you can access the following pages:

- *Dynamic Addresses* on page 189
- *Address Table* on page 190
- *Static MAC Address* on page 191

Dynamic Addresses

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

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

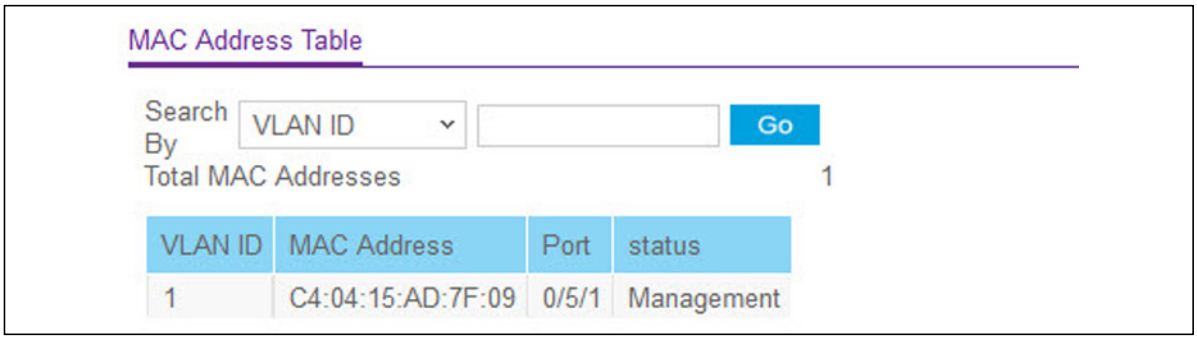


1. Use **Address Aging Timeout (seconds)** to specify the time-out period in seconds for aging out dynamically learned forwarding information. 802.1D-1990 recommends a default of 300 seconds. The value may be specified as any number between 10 and 1000000 seconds. The factory default is 300.

Address Table

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

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

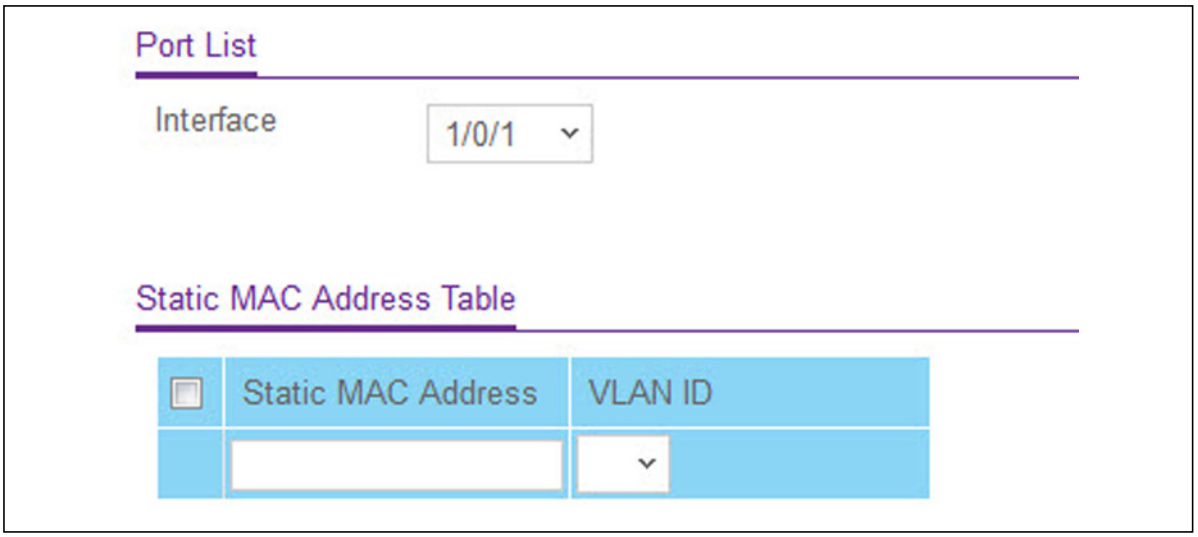


1. Use **Search By** to search for MAC Addresses by MAC Address, VLAN ID, and port.
   - **Searched by MAC Address** - Select MAC Address from the menu, enter the 6 byte hexadecimal MAC Address in two-digit groups separated by colons, for example 01:23:45:67:89:AB. Then click on the “Go” button. If the 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 the 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 the 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	The status of this entry. The meanings of the values are: • Static: the value of the corresponding instance was added by the system or a user and cannot be relearned. • Learned: the value of the corresponding instance was learned, and is being used. • Management: the value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress.

Static MAC Address

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



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

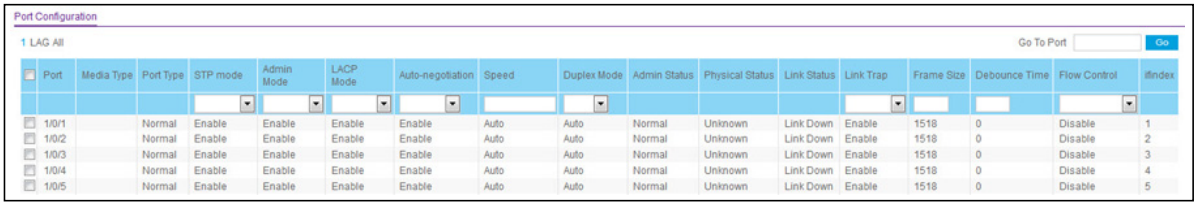
The pages on the Ports tab allow you to view and monitor the physical port information for the ports available on the switch. From the Ports link, you can access the following pages:

- *Port Configuration* on page 192
- *Port Description* on page 194

Port Configuration

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

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



To configure port settings:

1. Use **Port** to select the interface for which data is to be displayed or configured.
2. Use **STP Mode** to select the Spanning Tree Protocol Administrative Mode for the port or LAG. The possible values are:
   - **Enable** -Select this to enable the Spanning Tree Protocol for this port.
   - **Disable** -Select this to disable the Spanning Tree Protocol for this port.

   The default is Enable.
3. Use the **Admin Mode** 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 Enable.
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 drop-down entry field. The factory default is enabled.
5. From the **Auto-negotiation** menu, select **Enable** or **Disable** the auto-negotiation mode for this port. The default is Enable.

Note: After changing the Auto-negotiation mode, the switch may be inaccessible for some seconds due to applying the new settings.

6. From the **Speed** menu, select the speed value for the selected port. Possible field values are:
   - **Auto**—All supported speeds.
   - **100**—100 Mbits/second
   - **10G**—10 Gbits/second.

   The delimiter characters for setting different speed values are a comma (,), a period (.) and a space ( ).In order to set the auto-negotiation speed, the Auto-negotiation mode must be set to **Enable**. The default is **Auto**.

   Note: After changing the Speed value, the switch may be inaccessible for some seconds due to applying the new settings.

7. From the **Duplex Mode** menu, select the duplex mode for the selected port. Possible values are:
   - Auto—Indicates that speed is set by the auto-negotiation process.
   - Full—Indicates that the interface supports transmission between the devices in both directions simultaneously.
   - Half—Indicates that the interface supports transmission between the devices in only one direction at a time.

   The default is **Auto**.

   Note: After changing Duplex mode, the switch may be inaccessible for some seconds due to applying new settings.

8. Use the **Link Trap object** to determine whether to send a trap when link status changes. The factory default is enabled.
9. Use **Maximum Frame Size** to specify the maximum Ethernet frame size the interface supports or is configured, including ethernet header, CRC, and payload. The range is 1518 to 12288. The default maximum frame size is 1518.
10. Use **Debounce Time** to specify the timer value for port debouncing in a multiple of 100 milliseconds (msec) in the range to 100 to 5000. The default debounce timer value is 0 which means that debounce is disabled.
11. From the **Flow Control** menu, select to Enable or Disable IEEE 802.3 flow control. The default is Disable. Flow control helps to prevent data loss when the port cannot keep up with the amount of frames being switched. When enabled, the switch can send a Pause frame to stop traffic on a port if the amount of memory used by the packets on the port exceeds a preconfigured threshold and will respond to pause requests from partner devices. The paused port does not forward packets for the period of time specified in the Pause frame. When the Pause frame time elapses, or the utilization returns to a specified low threshold, the switch enables the port to again transmit frames. For LAG interfaces, Flow Control Mode is displayed as *blank* because Flow Control is not applicable.

12. 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.
13. Click **Apply** to update the switch with the values you entered. If you want the switch to retain the new values across a power cycle you must perform a save.

Table 74 describes the non-configurable data that is displayed.

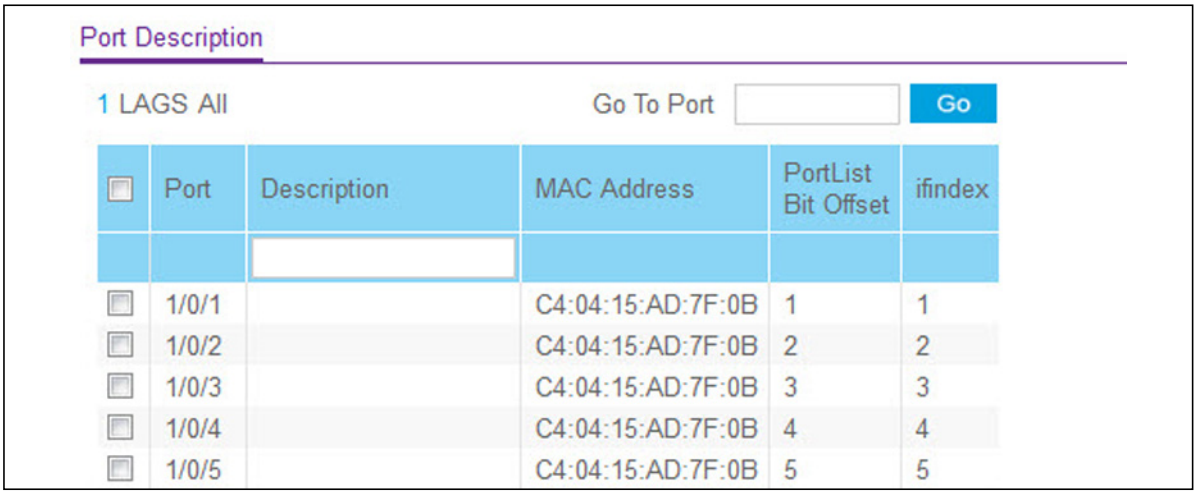
Table 74. Port Configuration

Field	Description
Media Type	The media type.
Port Type	For normal ports this field will be **Normal**. Otherwise the possible values are: • **Mirrored**—The port is a mirrored port on which all the traffic will be copied to the probe port. • **Probe**—Use this port to monitor a mirrored port. • **Trunk Member**—The port is a member of a Link Aggregation trunk. Look at the LAG screens for more information.
Admin Status	When the port's Admin mode is D-Disable, this field indicates the reason. Possible reasons are: • STP—Spanning Tree Protocol violation. • UDLD—UDLD protocol violation. • XCEIVER—Unsupported SFP/SFP+ inserted.
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 page 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.

Port Transceiver

This page displays the transceiver information for all fiber ports in the box.

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

To navigate the page:

- Select **Unit ID** to display physical ports of the selected unit.
- Select **All** to display physical ports of all units.

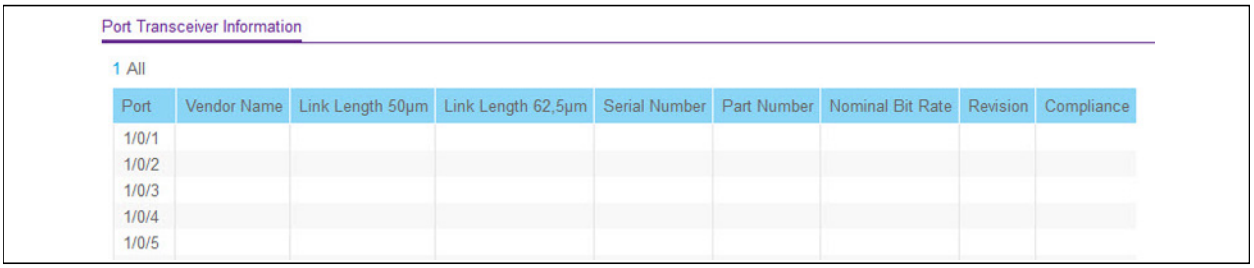


Table 75 describes the non-configurable data that is displayed.

Table 75. Port Transceiver

Field	Description
Port	Displays the interface for which data is to be displayed.
Vendor Name	Vendor name of the SFP.
Link Length 50 µm	Link length supported for 50 µm fiber.
Link Length 62, 5 µm	Link length supported for 50 µm fiber.
Serial Number	Serial number of the SFP.
Part Number	Part number of the SFP.
Nominal Bit Rate	Nominal signalling rate for SFP.
Revision	Vendor revision of the SFP.
Compliance	Compliance of the SFP.

Click **Update** to update the page with the latest information on the switch.

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.

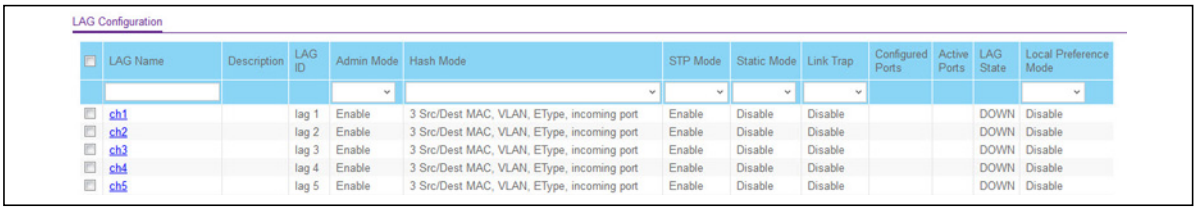
From the LAGs link, you can access the following pages:

- *LAG Configuration* on page 197
- *LAG Membership* on page 198

LAG Configuration

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

To access the LAG Configuration page, click **Switching** > **LAG** > **LAG Configuration**.



To configure LAG settings:

1. Use **LAG Name** to enter the name you want assigned to the LAG. You may enter any string of up to 15 alphanumeric characters. A valid name has to be specified in order to create the LAG.
2. Use **Admin Mode** to select enable or disable from the 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.
3. 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/Dest MAC,VLAN,EType,incoming port** is the default.
   - **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.

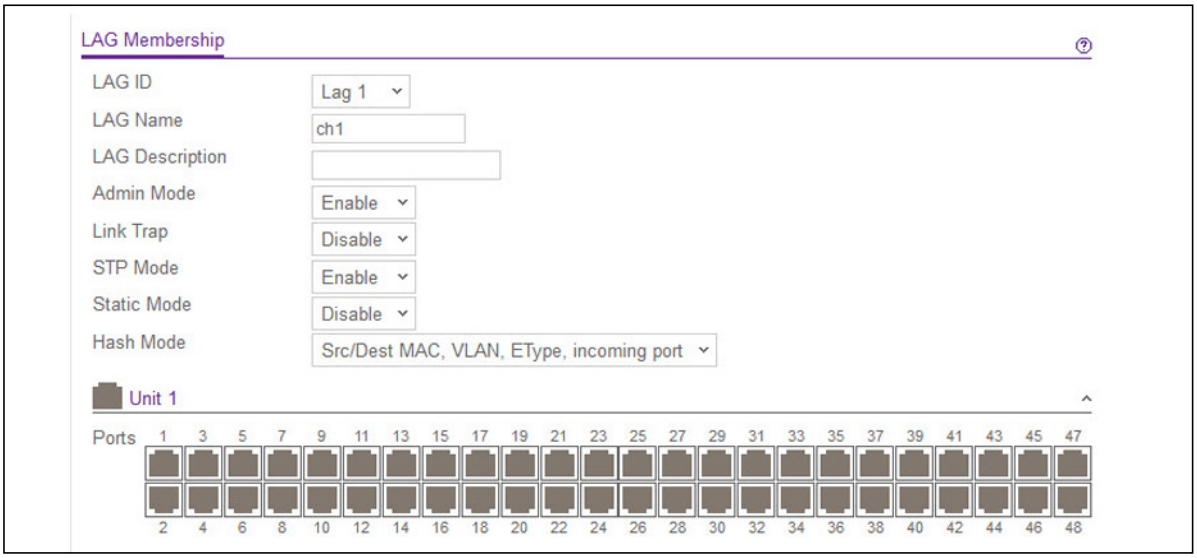
4. Use **STP Mode** to enable or disable the Spanning Tree Protocol Administrative Mode associated with the LAG. The possible values are:
   - **Disable** - Spanning tree is disabled for this LAG.
   - **Enable** - Spanning tree is enabled for this LAG. **Enable** is the default.
5. Use **Static Mode** to select enable or disable from the 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**.
6. 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.
7. Use **Local Preference Mode** to **Enable** or **Disable** the LAG interface's Local Preference Mode. The default is **Disable**.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. 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**.



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 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. Enable is the default.
7. Use **Static Mode** to select enable or disable from the 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. This option is the default.

- **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.

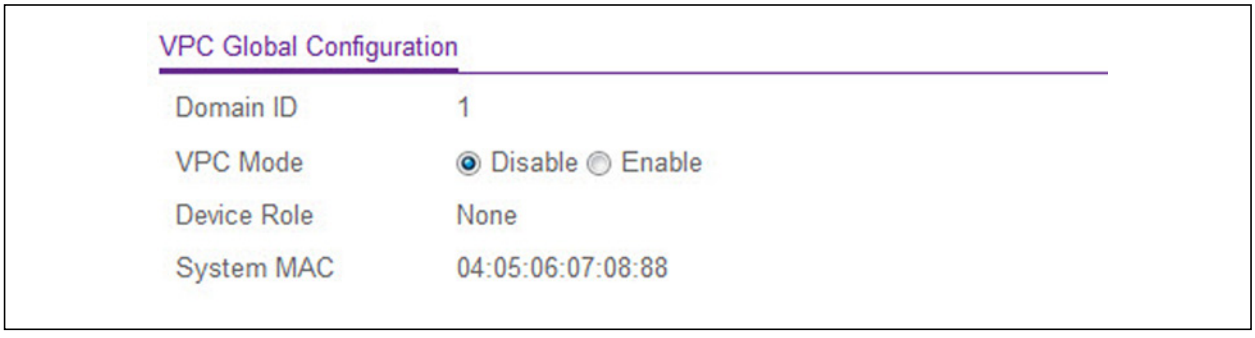
9. Use the **Port Selection Table** to select the ports as members of the LAG.

Multiswitch Link Aggregation Group

Use this page to view and manage global virtual port channel (VPC) settings on the device. VPCs are also known as multichassis or multiswitch link aggregation groups (MLAGs). Like port channels (also known as link aggregation groups or LAGs), VPCs allow one or more Ethernet links to be aggregated together to increase speed and provide redundancy. With port channels, the aggregated links must be on the same physical device, but VPCs do not share that requirement. The VPC feature allows links on two different switches to pair with links on a partner device. The partner device is unaware that it is pairing with two different devices to form a port channel.

Virtual Port Channel Global Configuration

➢ To display the Virtual Port Channel Global Configuration page, click **Switching > MLAG > Basic > VPC Global Configuration**. The following page is displayed.



- Globally configure the Virtual Port Channel settings.

  1. In the VPC Mode field, select **Enable** or **Disable** to globally enable or disable the VPC feature. By default, the VPC feature is **Disabled**.

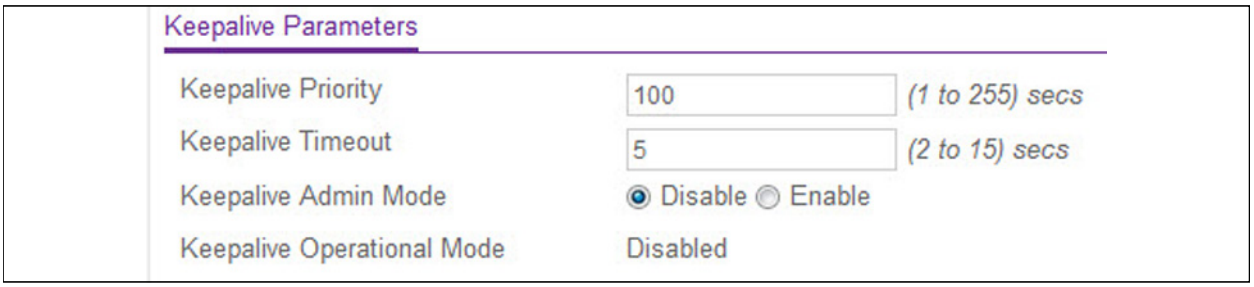
  The following table describes the non-configurable VPC Global Configuration fields.

Table 76. VPC Global Configuration

Field	Description
Domain ID	VPC Domain ID. Possible values are 1 to 1.
Device Role	Device Role is either **Primary**, **Secondary**, or **None**, based on an election between the two devices. The role is elected after a keepalive link is established. The default is **None**.
System MAC	The MAC address of the local system.

- **Configure the Keepalive Parameters.**

  The VPC feature sends periodic keepalive messages over the peer link between the primary and secondary devices in the VPC domain to determine the device roles (primary and secondary) and to monitor the health of the link.



  1. Enter the Keepalive Priority. Use this field to configure the priority value which is used on a switch for primary and secondary role selection. The primary switch is responsible for maintaining and propagating spanning-tree and link-aggregation state to the secondary switch. The range is 1 to 255 seconds. The default is 100. The device with a lower priority value becomes the Primary device in the VPC role election.
  2. Enter the Keepalive Timeout. Use this field to configure the number of seconds that must pass without receiving a keepalive message before the peer device is considered to be down. If an MLAG switch does not receive keepalive messages from the peer for this timeout value, it then transitions its role (if required). The range is 2 to 15 seconds. The default is 5 seconds.
  3. Use the Keepalive Admin Mode field to **Enable** or **Disable** the administrative mode of the keepalive component on the device. If a VPC switch does not receive keepalive messages from the peer within the timeout value, it begins the process of transitioning its role to primary (if standby). By default, the Keepalive Admin Mode is **Disabled**.

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

The following table describes the non-configurable Keepalive Parameter field.

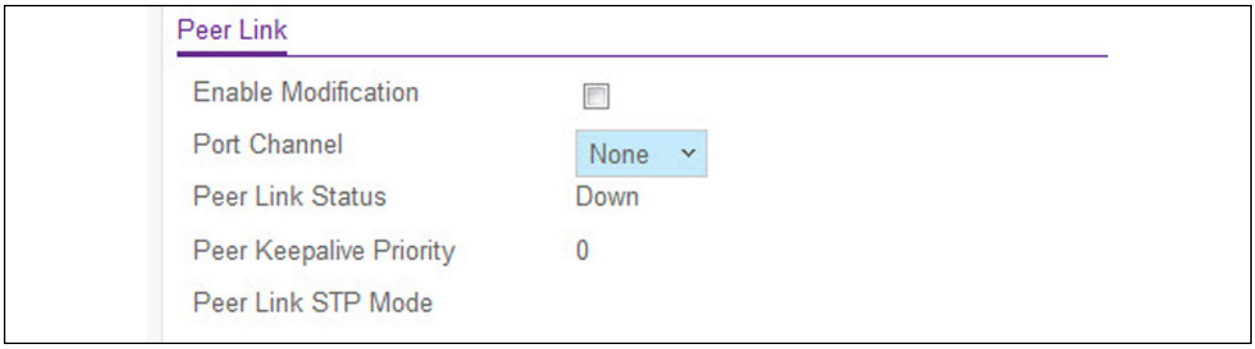
Table 77. VPC Keepalive Parameters

Field	Description
Keepalive Operational Mode	Displays the keepalive operational mode, which is either enabled or disabled.

➢ **Configure the Peer Link settings.**

The peer link is a port channel that serves as the link between the two devices in the VPC domain. Using a multimember port channel as the peer link helps protect it from link-level failures. The peer link is used:

- To carry the keepalive messages between the two peer devices.
- To carry the BPDUs and LACPDUs between the secondary and primary VPC devices.
- To carry control messages like VPC member port related events, FDB/MFDB entries, and configuration details.
- To carry data traffic over the peer's VPC member ports when the member ports of the VPC interface are all down on the local device.



1. Select the **Enable Modification** option to enable port channel modification.
2. Use the Port Channel list to configure a LAG interface as the VPC peer link and enable/disable the peer link protocol. The peer link protocol is disabled by default. Select **None** to remove the lag from a port channel.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

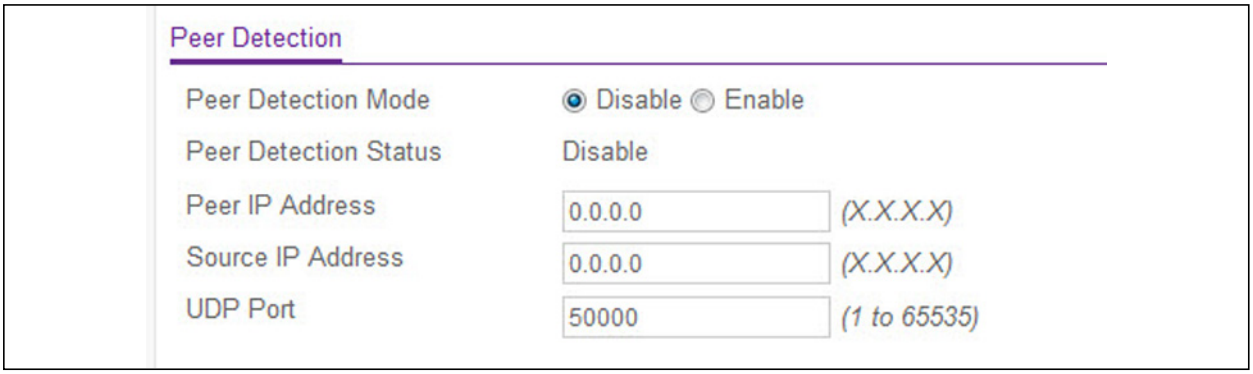
The following table describes the non-configurable Peer Link fields.

Table 78. Peer Link

Field	Description
Peer Link Status	Displays the peer status.
Peer Keepalive Priority	Displays the peer keepalive priority.
Peer Link STP Mode	Displays the Spanning Tree Protocol Administrative Mode associated with the LAG.

- **Configure the Peer Detection settings.**

The peer detection feature uses the dual control plane detection protocol (DCPDP), a UDP-based protocol, to detect peer links. You must configure peer detection on an IP interface with a VLAN that is not shared by any of the VPC interfaces.



1. Select the **Peer Detection Mode** option to **Enable** or **Disable** the dual control plane detection protocol (DCPDP). The mode is disabled by default. This configuration is used to enable the detection of peer VPC switches (and suppress state transitions out of the secondary state) in the presence of peer link failure.
2. In the **Peer IP Address** field, enter the IP address of the peer VPC device. This is the destination IP address in the DCPDP messages. The unconfigured value is 0.0.0.0.
3. Enter the local **Source IP Address** to be used by DCPDP. The unconfigured value is 0.0.0.0.
4. Enter the local **UDP Port** number which is used to listen for peer DCPDP packets. The range is 1 to 65535 seconds. The default is 50000. The unconfigured value is 50000.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The following table describes the non-configurable Peer Detection field.

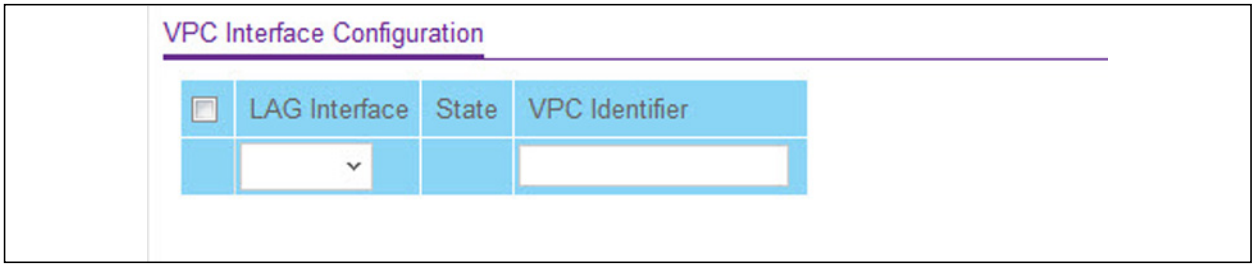
Table 79. Peer Detection

Field	Description
Peer Detection Status	Displays whether peer detection is enabled or disabled.

Virtual Port Channel Interface Configuration

Use this page to configure the VPC interfaces on the device. A VPC interface is created by combining a port channel on the local device with a port channel on the peer device. The VPC interface on the local and peer devices share a common VPC identifier. You can configure multiple instances of VPC interfaces on each peer device in the VPC domain.

- To display the Virtual Port Channel Interface Configuration page, click **Switching > MLAG > Advanced > VPC Interface Configuration**. The following page is displayed.



- Configure the VPC Interface.

1. From the **LAG Interface** list, select the ID of the local port channel to configure as a VPC interface.
2. Enter a VPC interface identifier value in the **VPC Identifier** field. The possible range is 1 to 63. To form a VPC interface with a port channel on the peer device, the port channel on the peer device must use the same VPC identifier.
3. Click **Add** to add a new interface configuration.
4. Click **Delete** to delete a selected interface configuration.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

The following table describes the non-configurable VPC Interface Configuration field.

Table 80. VPC Interface Configuration

Field	Description
State	The VPC interface's operational mode, which is one of the following: • Disabled—VPC functionality is operationally disabled on the VPC interface. • Wait—The port channel is waiting for VPC functionality to be enabled on a port channel on the peer device. • Error—VPC functionality is enabled on a port channel on both peer devices, but not all entry criteria are met for the port channel to be operational. For example, if the combined number of member ports for the VPC interface is more than the maximum allowed, then the state is set to Error on both devices. • Active—VPC functionality is enabled on a port channel on both peer devices, and all entry criteria are satisfied. The VPC interface is operationally enabled, and traffic is allowed to flow through the VPC member ports. • Inactive—The links connected to the VPC member ports are down, but the VPC interface on the peer remains active.

Virtual Port Channel Interface Details

➢ To display the Virtual Port Channel Interface Details page, click **Switching > MLAG > Advanced > VPC Interface Details**. The following page is displayed.

1. Select an interface from the list of LAG Interfaces which are configured as VPC interfaces.
2. The following table describes the non-configurable VPC details that are displayed.

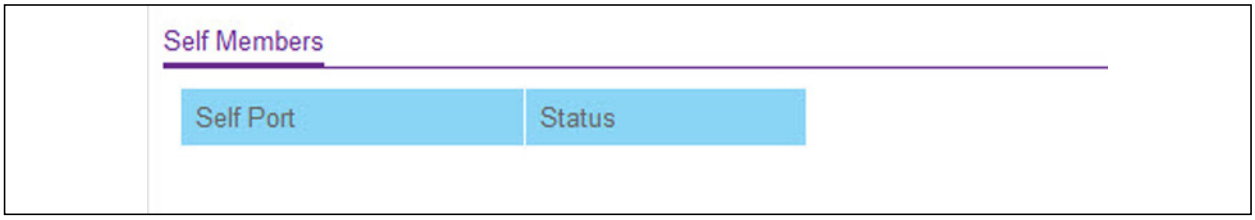
Table 81. VPC Interface Details

Field	Description
Status	The status of the VPC identifier.
VPC Identifier	The VPC interface identifier value. The range is 1 to 63.
Configured VLANs	The VLAN ID or list of VLAN IDs in which the LAG is a member. **Note:** If the VLAN Member or the VLAN Tag field exceeds the maximum number of displayable VLANs, an *Exceeded data limit to display* message is shown. Editing the values of these fields is prevented when at least one port reaches the maximum limit of VLANs during port multiselection.
Egress Tagging	The VLAN ID or list of VLAN IDs on which the LAG is tagged.
Peer Link STP Mode	The Spanning Tree Protocol Administrative Mode associated with the LAG.

3. Click **Update** to update the page with the latest information on the switch.

Self Members

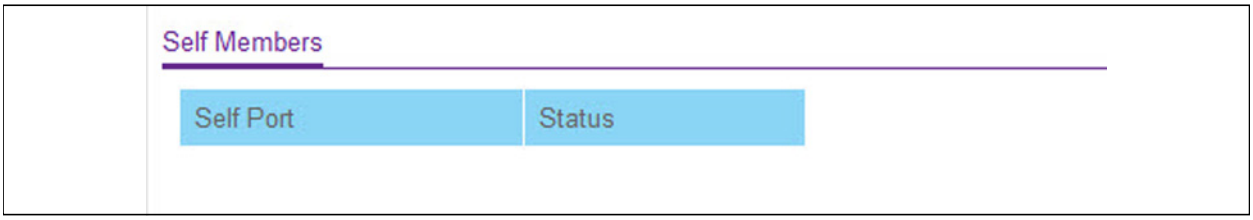
The Self Member fields provide information about the VPC member ports on the local device.



1. Select an ID in the **Self Port** field which lists the ID of each port that is a member of the port channel configured as a VPC interface on the current switch.
2. The operational status of the Self port is displayed in the **Status** field.
3. Click **Update** to update the page with the latest information on the switch.

Peer Members

The Peer Member fields provide information about the VPC member ports on the peer device.

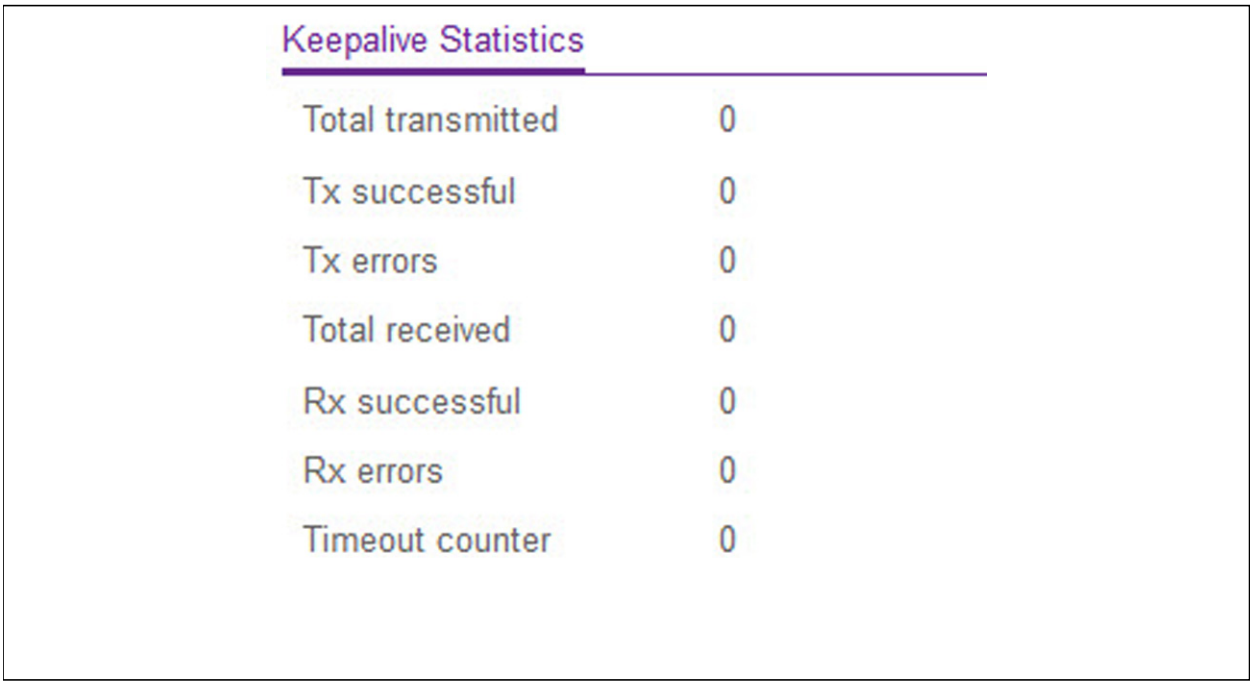


1. Select an ID in the **Peer Port** field which lists the ID of each port that is a member of the port channel configured as a VPC interface.
2. The operational status of the peer port is displayed in the **Status** field.
3. Click **Update** to update the page with the latest information on the switch.

Virtual Port Channel Keepalive Statistics

The VPC feature sends periodic keepalive messages over the peer link between the primary and secondary devices in the VPC domain to determine the device roles (primary and secondary) and to monitor the health of the link.

- To display the Virtual Port Channel Keepalive Statistics page, click **Switching > MLAG > Advanced > VPC Keepalive Statistics**. The following page is displayed.



The following table describes the non-configurable VPC Keepalive Statistics that are displayed.

Table 82. VPC Keepalive Statistics

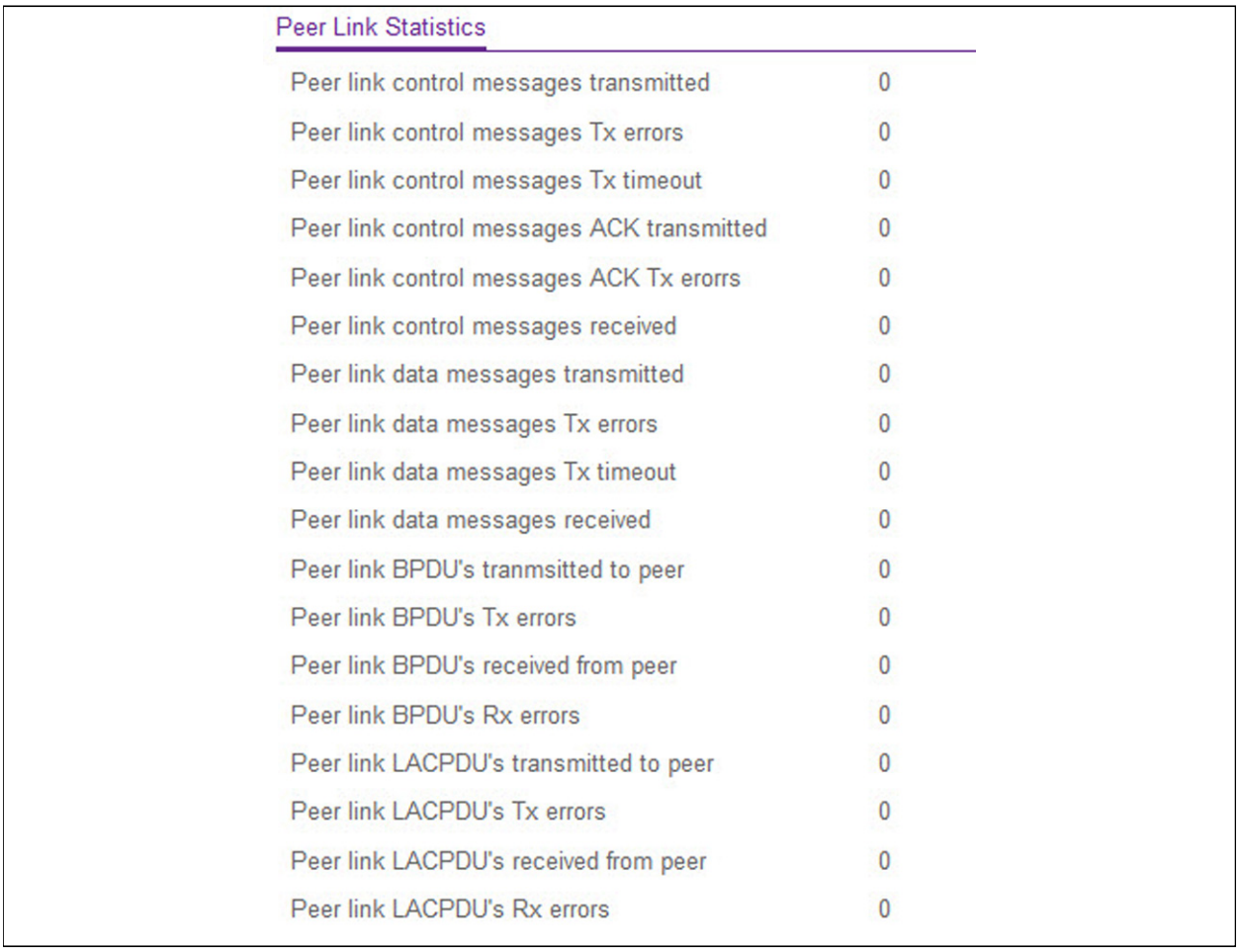
Field	Description
Total Transmitted	The total number of keepalive messages that the local device has sent to the peer device.
Tx Successful	The number of keepalive messages that have been successfully transmitted from the local device.
Tx Errors	The number of keepalive messages that the local device attempted to send to the peer device that were not transmitted due to an error.
Total Received	The total number of keepalive messages that the local device has received from the peer device.
Rx Successful	The number of keepalive messages that the local device has successfully received from the peer device.
Rx Errors	The number of keepalive messages that the local device has received from the peer device that contained errors.
Timeout Counter	The number of times the keepalive timeout timer has expired.

- Click **Clear** to clear all the counters and reset all switch summary statistics to the default values.
- Click **Update** to update the page with the latest information on the switch.

Virtual Port Channel Peer Link Statistics

In addition to keepalive messages, the peer link is used to send and receive control messages, data messages, BPDUs, and LACPDUs between the peer devices.

- To display the Virtual Port Channel Peer Link Statistics page, click **Switching > MLAG > Advanced > VPC Peer Link Statistics**. The following page is displayed.



The following table describes the non-configurable VPC Peer Link Statistics that are displayed.

Table 83. VPC Peer Link Statistics

Field	Description
Peer Link Control Messages Transmitted	The total number of control messages successfully sent from the local device to the peer device over the peer link.
Peer Link Control Messages Tx Errors	The total number of errors encountered when sending peer-link control messages from the local device to the peer device over the peer link.
Peer Link Control Messages Tx Timeout	The total number of peer-link control messages that did not receive an ACK from the peer device.

Field	Description
Peer Link Control Messages ACK Transmitted	The total number of ACKs sent to the peer device in response to peer-link control messages that were received.
Peer Link Control Messages ACK Tx Errors	The total number of errors encountered when sending ACKs in response to peer-link control messages.
Peer Link Control Messages Received	The total number of control messages successfully received by the local device from the peer device over the peer link.
Peer Link Data Messages Transmitted	The total number of data messages successfully sent from the local device to the peer device over the peer link.
Peer Link Data Messages Tx Errors	The total number of error encountered when sending peer-link data messages from the local device to the peer device over the peer link.
Peer Link Data Messages Tx Timeout	The total number of peer-link data messages that did not receive an ACK from the peer device.
Peer Link Data Messages Received	The total number of data messages successfully received by the local device from the peer device over the peer link.
Peer Link BPDU's Transmitted To Peer	The total number of BPDUs successfully sent to the peer device over the peer link.
Peer Link BPDU's Tx Errors	The total number of errors encountered when sending BPDUs to the peer device.
Peer Link BPDU's Received From Peer	The total number of BPDUs successfully received from the peer device over the peer link.
Peer Link BPDU's Rx Errors	The total number of errors encountered when receiving BPDUs from the peer device.
Peer Link LACPDU's Transmitted To Peer	The total number of LACPDUs successfully sent to the peer device over the peer link.
Peer Link LACPDU's Tx Errors	The total number of errors encountered when sending LACPDUs to the peer device.
Peer Link LACPDU's Received From Peer	The total number of LACPDUs successfully received from the peer device over the peer link.
Peer Link LACPDU's Rx Errors	The total number of errors encountered when receiving LACPDUs from the peer device.

- Click **Clear** to clear all the counters and reset all switch summary statistics to the default values.
- Click **Update** to update the page with the latest information on the switch.

Routing

4

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

Routing Table

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

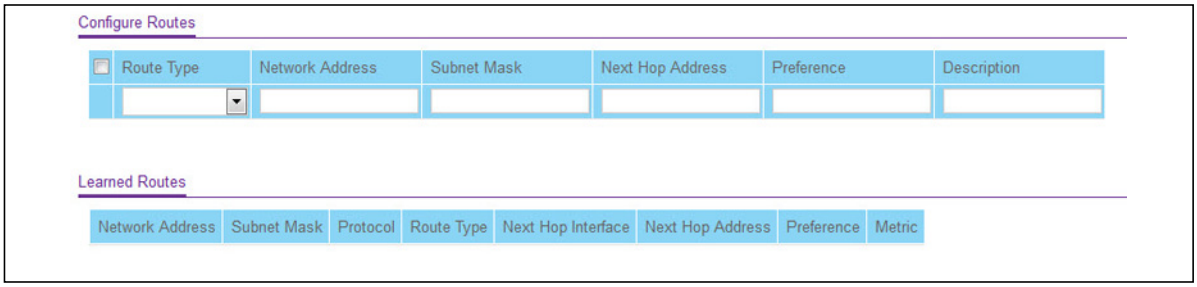
From the **Routing** > **Routing Table** link, you can access the following pages:

Basic

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

Route Configuration

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



Route Configuration

1. Select the **Route Type** from the menu. Possible values are:
   - Default—To create a default route, all that needs to be specified is the Next Hop Address, and Preference
   - Static—To create a static route, specify the Network Address, Subnet Mask, Next Hop Address, and Preference.
   - Static Reject—To create a static reject route, specify the Network Address, Subnet Mask, and Preference.
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 **Description** to specify the description of this route that identifies the route. Description must consist of alpha-numeric, dash or underscore characters and have length in the range from (0 to 31).
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.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Learned Routes

Table 84, Routing Table Basic Route Configuration on page 213 describes the non-configurable data that is displayed.

Table 84. Routing Table Basic Route Configuration

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are one of the following: Local Static
Route Type	This field can be Connected or Static or Dynamic based on the protocol.
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop 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.
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.
Metric	Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 - 255.

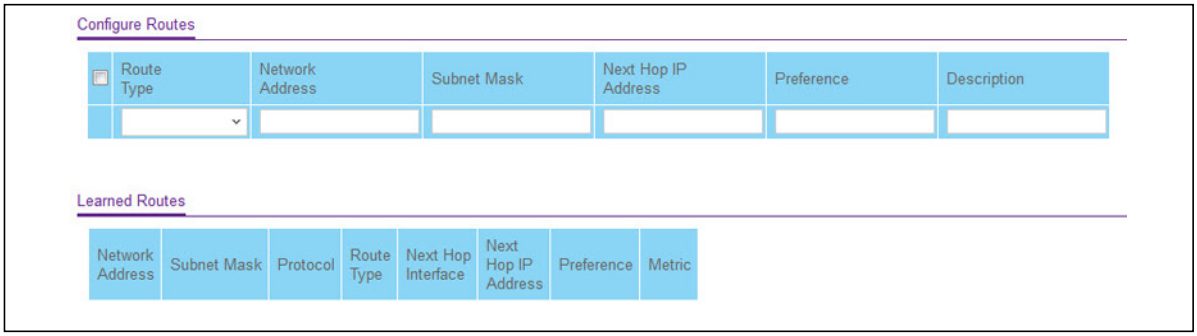
Click **Update** to update the page with the latest information on the switch.

Advanced

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

Route Configuration

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



Route Configuration

1. Use the **Route Type** field to specify default or static reject. 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 **Description** to specify the description of this route that identifies the route. Description must consist of alpha-numeric, dash or underscore characters and have length in the range from (0 to 31).
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
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are one of the following: • Local • Static
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.
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
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.
Metric	Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 - 255.

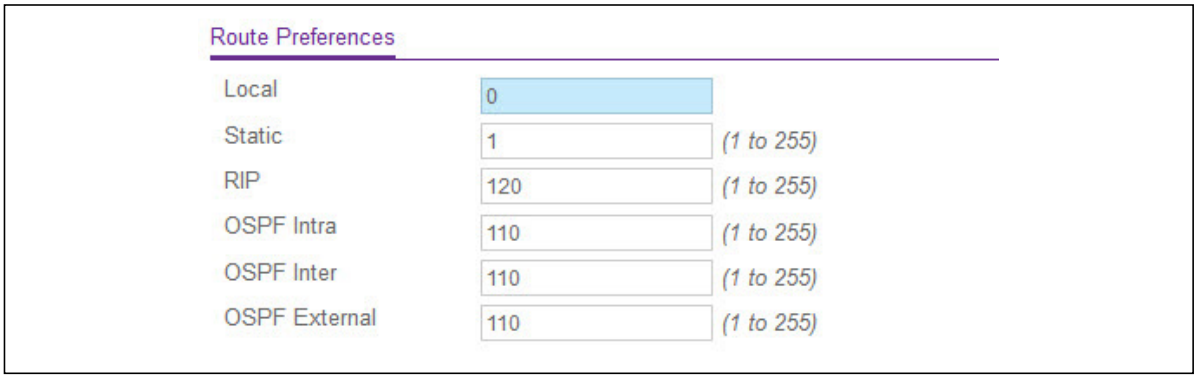
Click **Update** to update the page with the latest information on the switch.

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 Open Shortest Path First (OSPF) metrics are not directly comparable) you must configure different preference values for each of the protocols.

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



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

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

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

IP

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

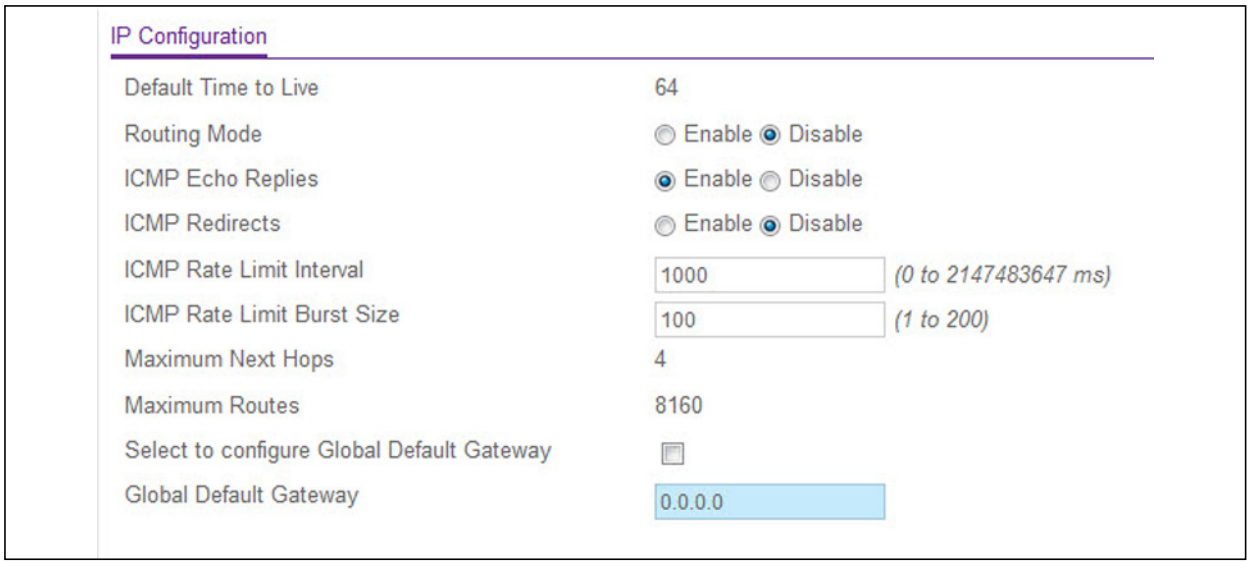
Basic

From the **Routing** > **IP > Basic** link, you can access the following pages:

IP Configuration

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

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



1. Use **Routing Mode** to select enable or disable. You must enable routing for the switch before you can route through any of the interfaces. The default value is disable.
2. Use **ICMP Echo Replies** to select enable or disable. If it is enable then only the router can send ECHO replies. By default ICMP Echo Replies are sent for echo requests.
3. Use **ICMP Redirects** to select enable or disable. If it is enabled globally and on interface level then only the router can send ICMP Redirects.
4. Use **ICMP Rate Limit Interval** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval. By default, Rate limit is 100 packets/sec i.e., burst interval is 1000 msec. To disable ICMP Rate limiting, set this field to '0'. Valid Rate Interval must be in the range 0 to 2147483647.

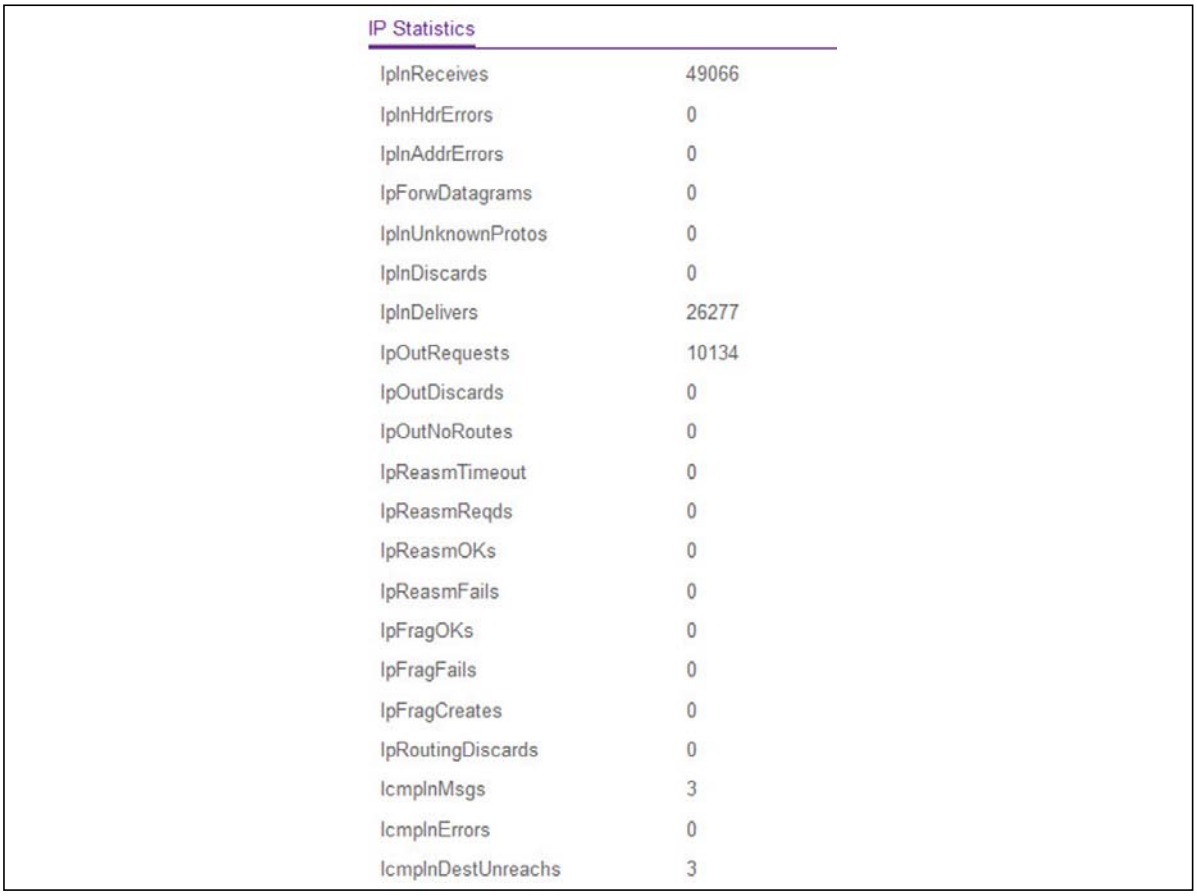
5. Use **ICMP Rate Limit Burst Size** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval. By default, burst size is 100 packets. When burst interval is 0 then configuring this field is not a valid operation. Valid Burst Size must be in the range 1 to 200.
6. Use **Select to configure Global Default Gateway** to edit the Global Default Gateway field.
7. Use **Global Default Gateway** to set the global default gateway to the manually configured value. A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

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.
Maximum Routes	The maximum number of routes (routing table size) supported by the switch. This is a compile-time constant.

Statistics

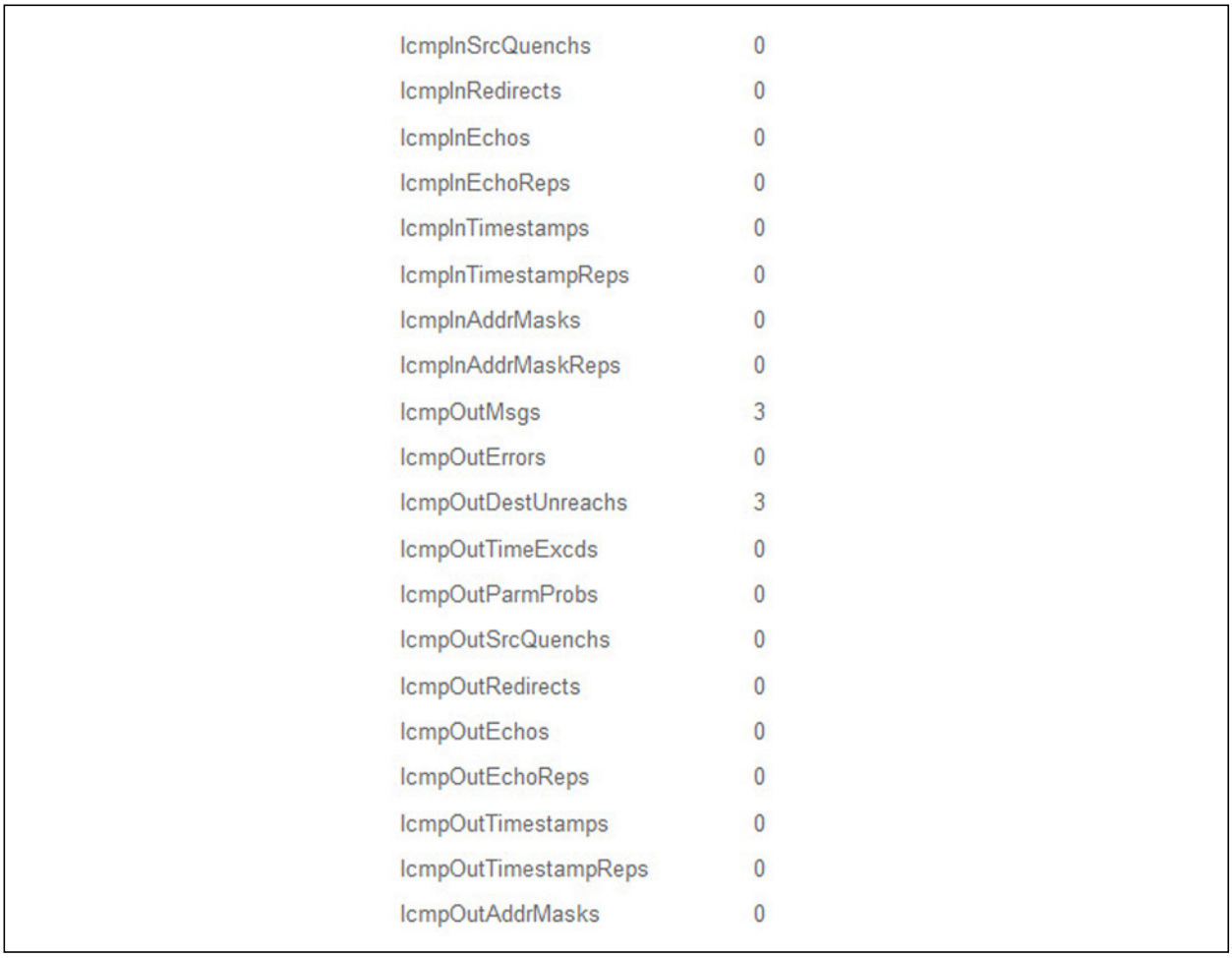
The statistics reported on this screen are as specified in RFC 1213.

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



IP Statistics

IpInReceives	49066
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	26277
IpOutRequests	10134
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	3
IcmpInErrors	0
IcmpInDestUnreachs	3



IcmpInSrcQuenchs	0
IcmpInRedirects	0
IcmpInEchos	0
IcmpInEchoReps	0
IcmpInTimestamps	0
IcmpInTimestampReps	0
IcmpInAddrMasks	0
IcmpInAddrMaskReps	0
IcmpOutMsgs	3
IcmpOutErrors	0
IcmpOutDestUnreachs	3
IcmpOutTimeExcds	0
IcmpOutParmProbs	0
IcmpOutSrcQuenchs	0
IcmpOutRedirects	0
IcmpOutEchos	0
IcmpOutEchoReps	0
IcmpOutTimestamps	0
IcmpOutTimestampReps	0
IcmpOutAddrMasks	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.

Field	Description
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.
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.

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

Field	Description
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object 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.

Advanced

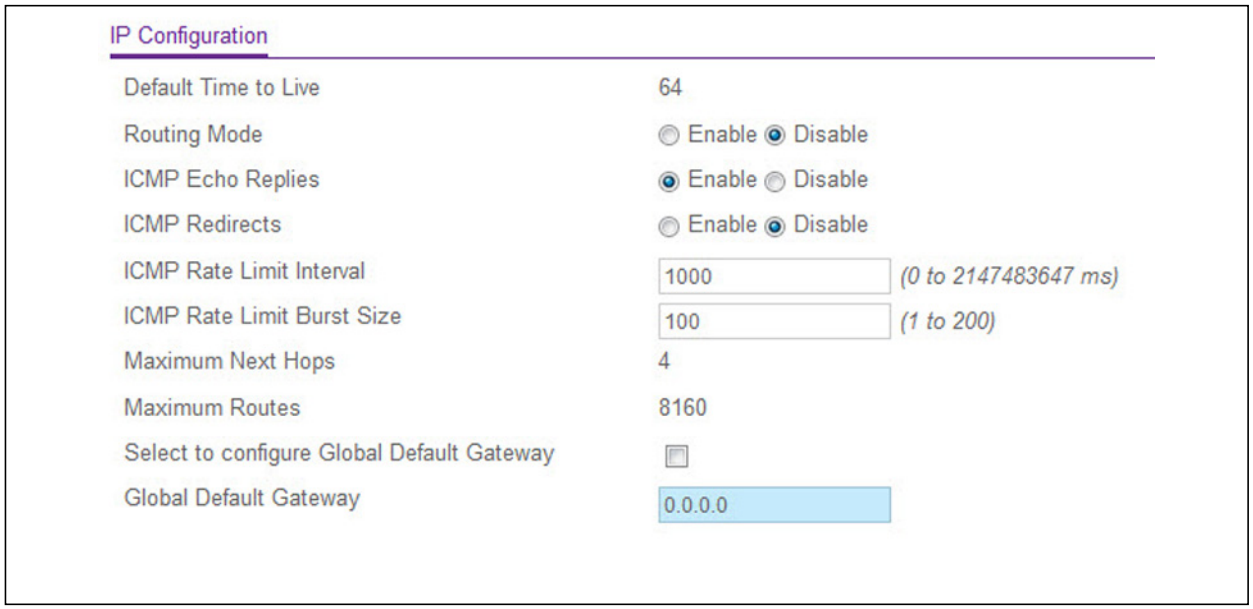
From the **Routing** > **IP > Advanced** link, you can access the following pages:

- *IP Configuration* on page 224

IP Configuration

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

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



1. Use **Routing Mode** to select enable or disable. You must enable routing for the switch before you can route through any of the interfaces. The default value is disable.
2. Use **ICMP Echo Replies** to select enable or disable. If it is enable, then only the router can send ECHO replies. By default ICMP Echo Replies are sent for echo requests.
3. Use **ICMP Redirects** to select enable or disable. If it is enabled globally and on interface level then only the router can send ICMP Redirects.
4. Use **ICMP Rate Limit** Interval to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval. By Default Rate limit is 100 packets/sec, i.e., burst interval is 1000 msec. To disable ICMP 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.
6. Use **Select to configure Global Default Gateway** to edit the Global Default Gateway field.
7. Use **Global Default Gateway** to set the global default gateway to the manually configured value. A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

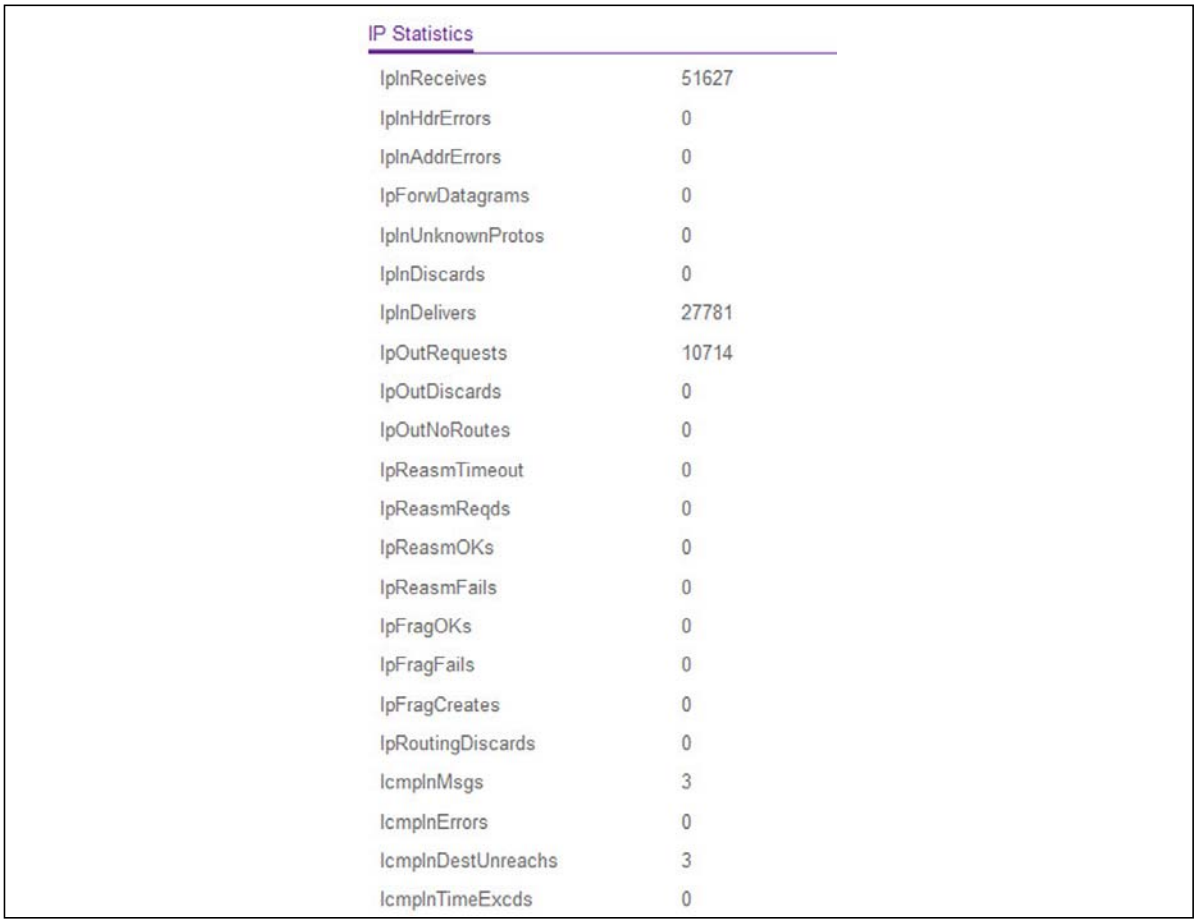
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Field	Description
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.
Maximum Routes	The maximum number of routes (routing table size) 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 IP Statistics page, click **Routing** > **IP**> **Advanced** > **Statistics**.



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.

Field	Description
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.
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.

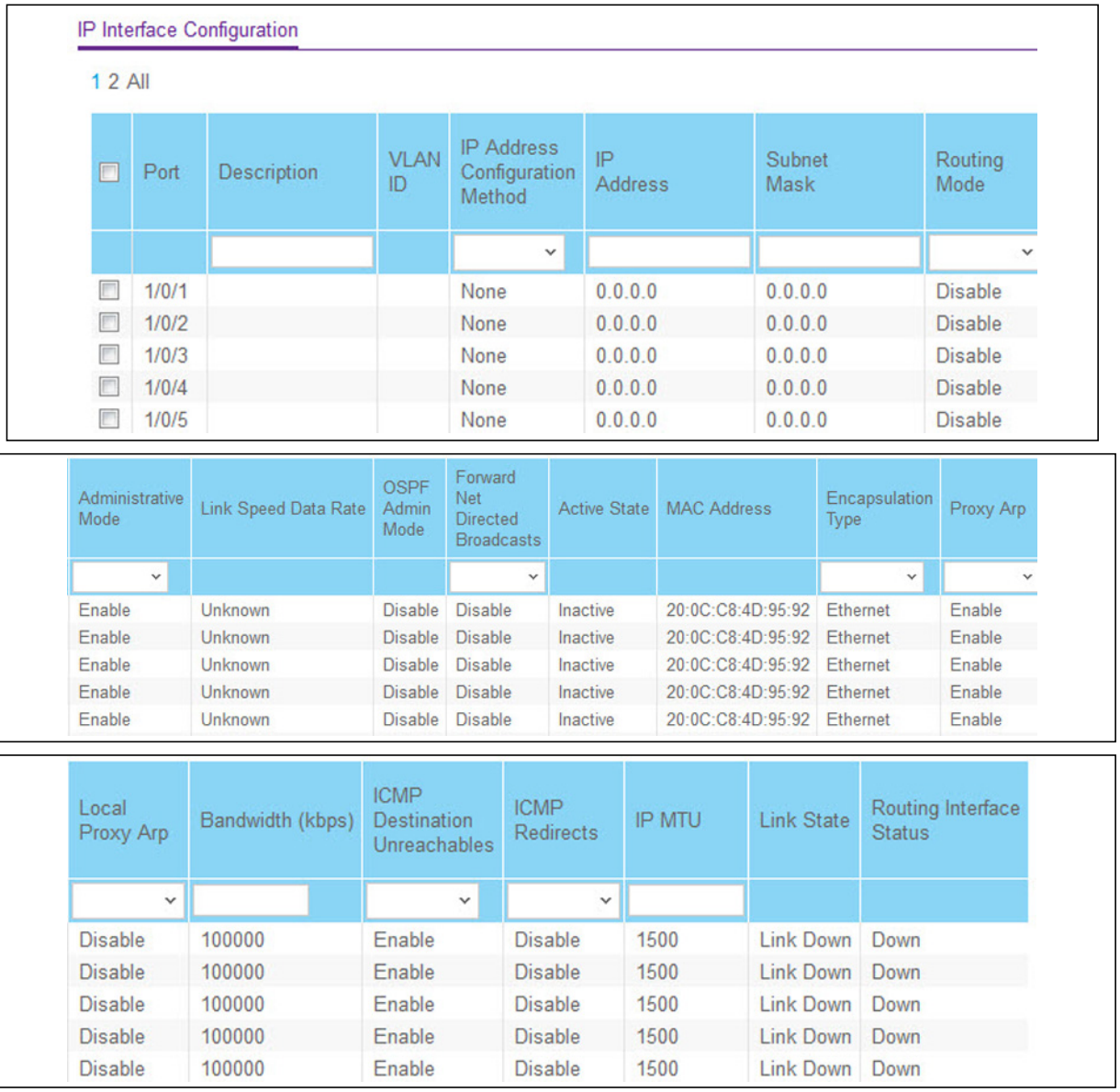
Field	Description
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are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

Field	Description
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object 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

1 2 All

Port	Description	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode
1/0/1			None	0.0.0.0	0.0.0.0	Disable
1/0/2			None	0.0.0.0	0.0.0.0	Disable
1/0/3			None	0.0.0.0	0.0.0.0	Disable
1/0/4			None	0.0.0.0	0.0.0.0	Disable
1/0/5			None	0.0.0.0	0.0.0.0	Disable

Administrative Mode	Link Speed Data Rate	OSPF Admin Mode	Forward Net Directed Broadcasts	Active State	MAC Address	Encapsulation Type	Proxy Arp
Enable	Unknown	Disable	Disable	Inactive	20:0C:C8:4D:95:92	Ethernet	Enable
Enable	Unknown	Disable	Disable	Inactive	20:0C:C8:4D:95:92	Ethernet	Enable
Enable	Unknown	Disable	Disable	Inactive	20:0C:C8:4D:95:92	Ethernet	Enable
Enable	Unknown	Disable	Disable	Inactive	20:0C:C8:4D:95:92	Ethernet	Enable
Enable	Unknown	Disable	Disable	Inactive	20:0C:C8:4D:95:92	Ethernet	Enable

Local Proxy Arp	Bandwidth (kbps)	ICMP Destination Unreachables	ICMP Redirects	IP MTU	Link State	Routing Interface Status
Disable	100000	Enable	Disable	1500	Link Down	Down
Disable	100000	Enable	Disable	1500	Link Down	Down
Disable	100000	Enable	Disable	1500	Link Down	Down
Disable	100000	Enable	Disable	1500	Link Down	Down
Disable	100000	Enable	Disable	1500	Link Down	Down

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**. Use the **None** method 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 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 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 menu.
12. Use **Local Proxy Arp** to disable or enable Local Proxy ARP for the specified interface from the menu.
13. Use **Bandwidth (kbps)** 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 IP MTU is the maximum frame size minus the length of the layer 2 header.
17. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
18. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
19. Click **Delete** to delete the IP Address from the selected interface.
20. Click **Update** to update the page with the latest information on the switch.

Table 85, IP Interface Configuration describes the non-configurable data that is displayed.

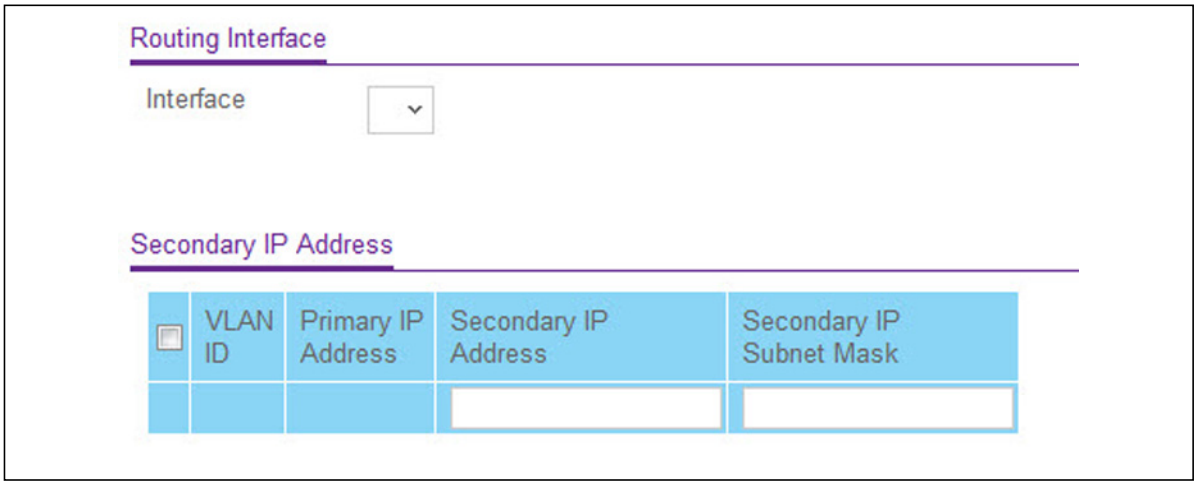
Table 85. IP Interface Configuration

Field	Description
VLAN ID	Displays the VLAN ID for the interface.
OSPF Admin Mode	Displays OSPF admin mode of the interface. The default value is disable.
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.
Routing Interface Status	Indicates whether the link status is up or down.

Secondary IP

Use the Secondary IP page to configure a secondary IP address for this switch.

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



- Configure the Secondary IP.

1. In the **Routing Interface** list, select the interface for which data is to be displayed or configured.
2. In the **Secondary IP Address** field, add a secondary IP address to the selected interface.
3. In the **Secondary IP Subnet Mask** field, enter the subnet mask associated with the secondary IP address. 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 readonly once configured.
4. Click **Add** to add a Secondary IP Address for the selected interface.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Delete** to delete the Secondary IP Address from the selected interface.

Table 86, Secondary IP describes the non-configurable data that is displayed.

Table 86. Secondary IP

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

IPv6

The **Routing** > **IPv6** folder contains links to the following web pages that configure and display IP routing data:

- *IPv6 Basic* on page 233
- *IPv6 Advanced* on page 235

IPv6 Basic

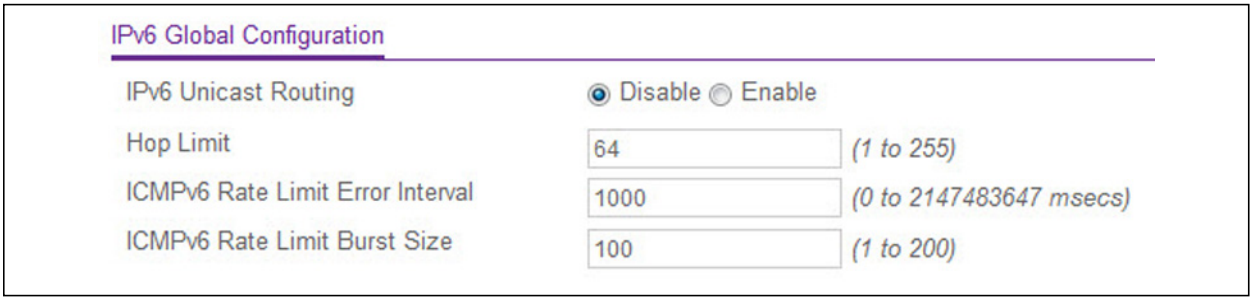
From the **Routing** > **IPv6 > Basic** link, you can access the following pages:

- *IPv6 Global Configuration*
- *IPv6 Route Table* on page 234

IPv6 Global Configuration

Use this page to configure IPv6 routing parameters for the switch, as opposed to an interface.

To display the IPv6 Global Configuration page, click **Routing** > **IPv6** > **Basic** > **Global Configuration**. The following page is displayed.



➢ Configure IPv6 Global Configuration.

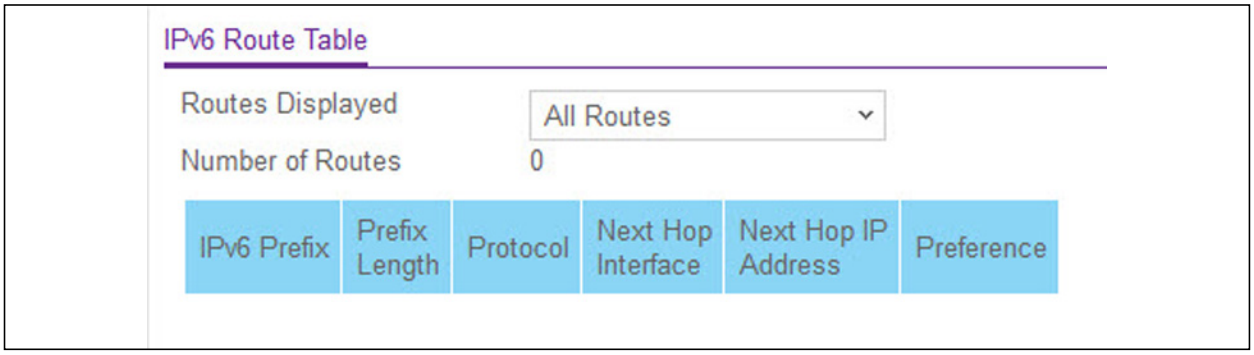
1. In the **IPv6 Unicast Routing** field, select the option to globally Enable or Disable IPv6 unicast routing.
2. In the **Hop Limit** field, enter a value for the unicast hop count used in IPv6 packets originated by the node. The value is also included in router advertisements. Valid values for hops are 1 to 255, inclusive. The default is Not Configured, which means that a value of zero is sent in router advertisements.

3. In the **ICMPv6 Rate Limit Error Interval** field, specify the number of ICMP error packets allowed per burst interval. This value controls the ICMPv6 error packets. The default Rate Limit is 100 packets per second, meaning that the burst interval is 1000 mseconds. To disable ICMP Rate Limiting, set this field to 0.The valid Rate Interval must be in the range 0 to 2147483647 mseconds.
4. In the **ICMPv6 Rate Limit Burst Size** field, specify the number of ICMP error packets allowed per burst interval. This value controls the ICMP error packets. Default burstsize 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 of 1 to 200.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IPv6 Route Table

Use this page to display the IPv6 Route Table.

To display the IPv6 Route Table page, click **Routing** > **IPv6** > **Basic** > **Route Table**. The following page is displayed.



- Select the IPv6 Route Table to display.

1. In the **Routes Displayed** list, select from the following:
   - All Routes—Shows all active Ipv6 routes.
   - Best Routes Only—Shows only the best active routes.
   - Configured Routes Only—Shows the routes configured by the user.

Table 87, IPv6 Route Table describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 87. IPv6 Route Table

Field	Description
Number of Routes	Displays the total number of active routes in the route table.
IPv6 Prefix	Displays the network prefix for the active route.
Prefix Length	Displays the prefix length for the active route.
Protocol	Displays the type of protocol for the active route.
Next Hop Interface	Displays the interface over which the route is active. For a reject route, the next hop would be a *Null0* interface.
Next Hop IP Address	Displays the next hop IPv6 address for the active route.
Preference	Displays the route preference of the configured route.

IPv6 Advanced

From the **Routing** > **IPv6 > Advanced** link, you can access the following pages:

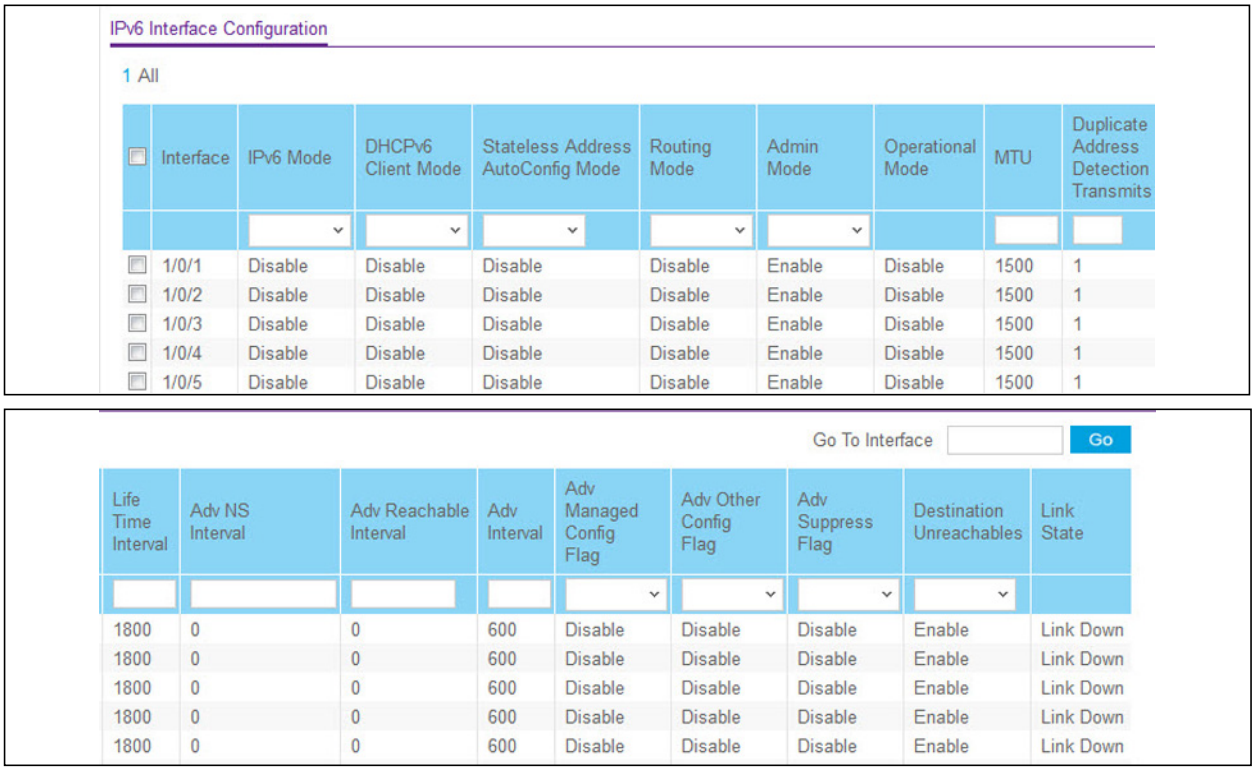
- *IPv6 Global Configuration*
- *IPv6 Interface Configuration*
- *IPv6 Prefix Configuration* on page 237
- *IPv6 Statistics* on page 239
- *IPv6 Neighbor Table* on page 243
- *IPv6 Static Route Configuration* on page 245
- *IPv6 Route Table* on page 246
- *IPv6 Route Preferences* on page 247
- *IPv6 Tunnel Configuration* on page 248

IPv6 Global Configuration

This page is the same as under *IPv6 Basic* on page 233.

IPv6 Interface Configuration

To display the IPv6 Interface Configuration page, click **Routing** > **IPv6** > **Advanced** > **Interface Configuration**. The following page is displayed.



IPv6 Interface Configuration

1 All

Interface	IPv6 Mode	DHCPv6 Client Mode	Stateless Address AutoConfig Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits
1/0/1	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
1/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
1/0/3	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
1/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
1/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1

Go To Interface Go

Life Time Interval	Adv NS Interval	Adv Reachable Interval	Adv Interval	Adv Managed Config Flag	Adv Other Config Flag	Adv Suppress Flag	Destination Unreachables	Link State
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down

- **Configure IPv6 Interface Configuration.**

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. Select the check box next to the **Interface** for which data is to be displayed or configured. All physical interfaces are valid.
3. Select **Enable** or **Disable** in the **IPv6 Mode** list. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used. The default value is disable.
4. In the **DHCPv6 Client Mode** list, select to **Enable** or **Disable** DHCPv6 Client mode on an interface. At any point in time, only one interface can act as a client. The default value is disable.
5. In the **Stateless Address AutoConfig Mode** list, select to **Enable** or **Disable** Stateless Address AutoConfig mode on an interface. The default value is disable.
6. In the **Routing Mode** list, select to **Enable** or **Disable** the routing mode of an interface. The default is disable.
7. In the **Admin Mode** list, select to **Enable** or **Disable** IPv6 mode. The default is disable. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used.
8. In the **MTU** field, specify the maximum transmit unit on an interface. If the value is 0, then this interface is not enabled for routing. It is not valid to set this value to 0 if routing is enabled. The MTU range 1280 to 1500. The default is 1500.

9. In the **Duplicate Address Detection Transmits** field, specify the number of duplicate address detection (DAD) transmits on an interface. DAD transmits values must be in the range 0 to 600. The default is 1.
10. Specify the router advertisement **Life Time Interval** sent from the interface. This value must be greater than or equal to the maximum advertisement interval. 0 means do not use the router as the default router. The range of router life time is 0 to 9000. The default is 1800.
11. In the **Adv NS Interval** field, specify the retransmission time field of router advertisement sent from the interface. A value of 0 means the interval is not specified for the router. The range of neighbor solicit interval is 1000 to 4294967295. The default is 0.
12. In the **Adv Reachable Interval** field, specify the router advertisement time to consider neighbor reachable after ND confirmation. The range of reachable time is 0 to 3600000. The default is 0.
13. Use the **Adv Interval** field to specify the maximum time allowed between sending router advertisements from the interface. The range of maximum advertisement interval is 4 to 1800. The default value is 600.
14. In the **Adv Other Config Flag** list, select **Enable** or **Disable** to specify router advertisement other stateful configuration flag. Default value of other config flag is disable.
15. In the **Adv Suppress Flag** list, select to **Enable** or **Disable** router advertisement suppression on an interface. The default value of suppress flag is disable.
16. In the **Destination Unreachables** list, select to **Enable** or **Disable** the Mode of Sending ICMPv6 Destination Unreachables on this interface. If **Disabled**, then this interface will not send ICMPv6 Destination Unreachables. By default, the IPv6 Destination Unreachables mode is enable.
17. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
18. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

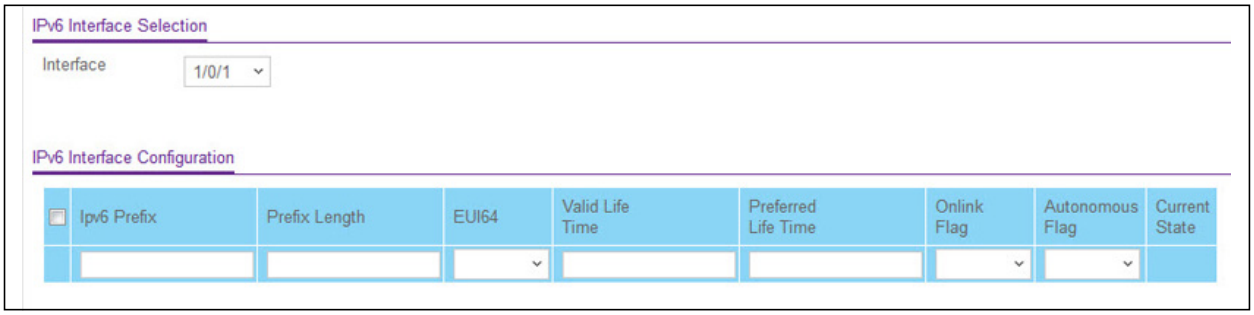
Table 88, IPv6 Advanced Interface Configuration describes the non-configurable data that is displayed.

Table 88. IPv6 Advanced Interface Configuration

Field	Description
Operational Mode	Specifies operational state of an interface. The default value is disable.
Link State	Indicates whether the link is up or down.

IPv6 Prefix Configuration

To display the IPv6 Prefix Configuration page, click **Routing** > **IPv6** > **Advanced** > **Prefix Configuration**. The following page is displayed.



- Configure IPv6 Prefix Configuration.

1. From the **Interface** list, select the interface to be configured. When the selection is changed, a screen update occurs, causing all fields to be updated for the newly selected port. All physical interfaces are valid.
2. In the **IPv6 Prefix** field, specify the IPv6 prefix for an interface.
3. In the **Prefix Length** field, specify the IPv6 prefix length for an interface.
4. In the EUI64 list, select to **Enable** or **Disable** the specified 64-bit unicast prefix.
5. In the **Valid Life Time** field, specify the router advertisement per prefix time to consider the prefix valid for the purpose of on-link determination. Valid life time must be in the range 0 to 4294967295.
6. In the **Preferred Life Time** field, specify the router advertisement per prefix time. An autoconfigured address generated from this prefix is preferred. Preferred life time must be in the range 0 to 4294967295.
7. From the **Onlink Flag** list, select **Enable** or **Disable** as to whether the selected prefix can be used for on-link determination. The default is enable.
8. In the Autonomous Flag list, select to **Enable** or **Disable** whether the selected prefix can be used for autonomous address configuration. The default value is enable.
9. Click **Add** to add a new IPv6 address to the interface.
10. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
11. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
12. Click **Delete** to delete a existing IPv6 address entry from the interface.

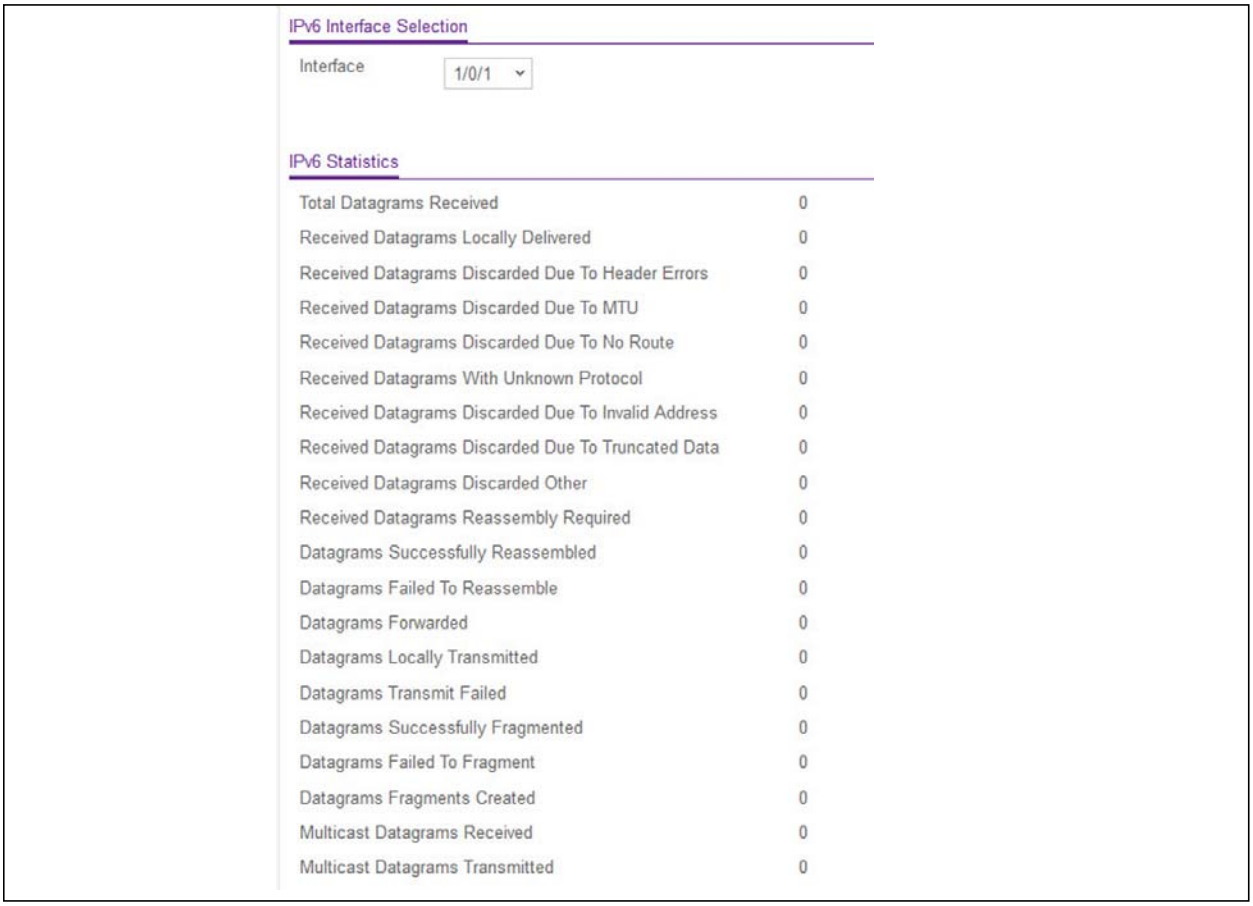
Table 89, IPv6 Advanced Interface Prefix Configuration on page 238 describes the non-configurable data that is displayed.

Table 89. IPv6 Advanced Interface Prefix Configuration

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

IPv6 Statistics

To display the IPv6 Interface Statistics page, click **Routing** > **IPv6** > **Advanced** > **Statistics**. The following page is displayed.



- Display IPv6 Interface Statistics.

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

  Table 90, IPv6 Advanced Interface Statistics on page 240 describes the non-configurable data that is displayed.

  Click **Update** to update the page with the latest information on the switch.

Table 90. IPv6 Advanced Interface Statistics

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

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

Table 91, ICMPv6 Statistics describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 91. ICMPv6 Statistics

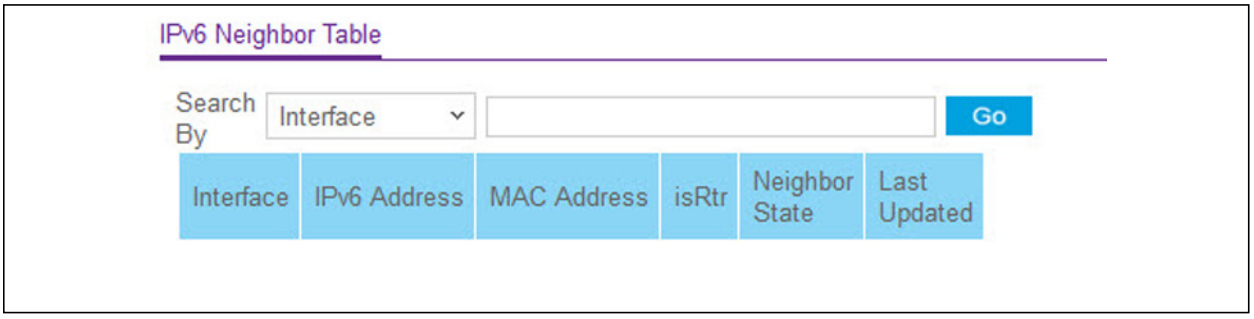
Field	Description
Total ICMPv6 Messages Received	The total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
ICMPv6 Messages With Errors Received	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.)
ICMPv6 Destination Unreachable Messages Received	The number of ICMP Destination Unreachable messages received by the interface.

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

Field	Description
ICMPv6 Time Exceeded Messages Transmitted	The number of ICMP Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	The number of ICMP Parameter Problem messages sent by the interface.
ICMPv6 Packet Too Big Messages Transmitted	The number of ICMP Packet Too Big messages sent by the interface.
ICMPv6 Echo Request Messages Transmitted	The number of ICMP Echo (request) messages sent by the interface.
ICMPv6 Echo Reply Messages Transmitted	The number of ICMP Echo Reply messages sent by the interface.
ICMPv6 Router Solicit Messages Transmitted	The number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	The number of ICMP Router Advertisement messages sent by the interface.
ICMPv6 Neighbor Solicit Messages Transmitted	The number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Neighbor Advertisement Messages Transmitted	The number of ICMP Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Transmitted	The number of Redirect messages sent.
ICMPv6 Group Membership Query Messages Transmitted	The number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Transmitted	The number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Transmitted	The number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	The number of duplicate Addresses detected by the interface.

IPv6 Neighbor Table

To display the IPv6 Neighbor Table page, click **Routing** > **IPv6** > **Advanced** > **Neighbor Table**. The following page is displayed.



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

- To search by IPv6 address, select **IPv6 Address** from the **Search By** list. Enter the 128-byte hexadecimal IPv6 address in four-digit groups separated by colons, for example 2001:231F:::1. Then click **Go**. If the address exists, that entry will be displayed. An exact match is required.
- To search by Interface, select **Interface** from the **Search By** list, enter the interface ID in unit/slot/port format, for example 2/1/1. Then click **Go**. If the address exists, that entry will be displayed.
- Click **Clear** to clear the IPv6 neighbors on a selected interface or on all interfaces.
- Click **Update** to update the page with the latest information on the switch.

Table 92, IPv6 Advanced Neighbor Table describes the non-configurable data that is displayed.

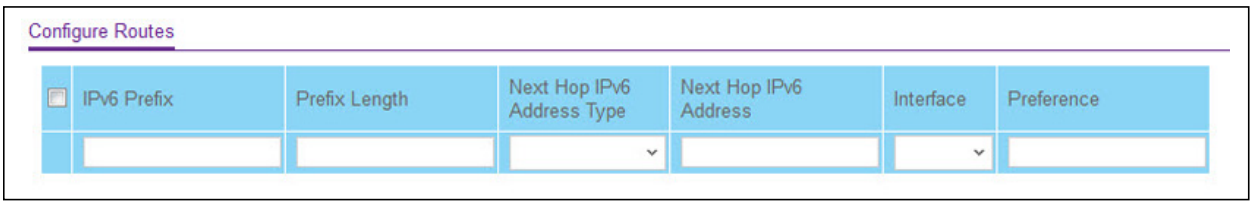
Table 92. IPv6 Advanced Neighbor Table

Field	Description
Interface	The interface whose settings are displayed in the current table row.
IPv6 Address	The IPv6 address of the neighbor or interface.
MAC Address	Specifies MAC address associated with an interface.
isRtr	Indicates whether the neighbor is a router. If the neighbor is a router, the value is **True**. If the neighbor is not a router, the value is **False**.

Field	Description
Neighbor State	Specifies the state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache: • Incmp—Address resolution is being performed on the entry.A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • Reach—Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • Stale—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • Delay—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. • Probe—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.
Last Updated	Time since the address was confirmed to be reachable.

IPv6 Static Route Configuration

To display the IPv6 Static Route Configuration page, click **Routing** > **IPv6** > **Advanced** > **Static Route Configuration**. The following page is displayed.



➢ Configure the IPv6 Static Route.

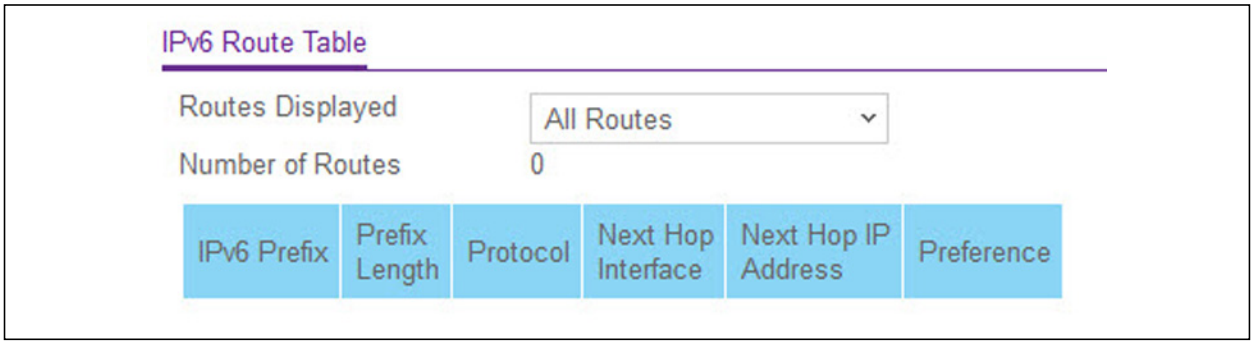
1. In the **IPv6 Prefix** field, specify the IPv6 prefix for the configured route.
2. In the **Prefix Length** field, specify the IPv6 prefix length for the configured route
3. Specify the **Next Hop IPv6 Address Type** by selecting one of the following options from the list:
   - **Global** IPv6 Address
   - **Link-Local** IPv6 Address. If the Next Hop IPv6 address specified is a Link-Local IPv6 Address, then specify the Interface for the Link-local IPv6 Next Hop Address.

- **Static-Reject**. Select **Static-Reject** to create a static-reject route for a destination prefix. No next hop address is specified in that case.

4. Enter the **Next Hop IPv6 Address** for the configured route.
5. Select from the **Interface** list, to specify in unit/slot/port format, the Link-Local IPv6 Next Hop Address. This field is enabled only if Link-Local is selected.
6. Specify the route **Preference** of the configured route.
7. Click **Add** to configure a new route.
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 **Delete** to delete the corresponding route.

IPv6 Route Table

To display the IPv6 Route Table page, click **Routing** > **IPv6** > **Advanced** > **Route Table**. The following page is displayed.



1. In the **Routes Displayed** field, select which routes to display from the following list:
   - All Routes—Show all active IPv6 routes.
   - Best Routes Only—Show only the best active routes.
   - Configured Routes Only—Show the routes configured by the user

Table 93, IPv6 Advanced Route Table on page 246 describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 93. IPv6 Advanced Route Table

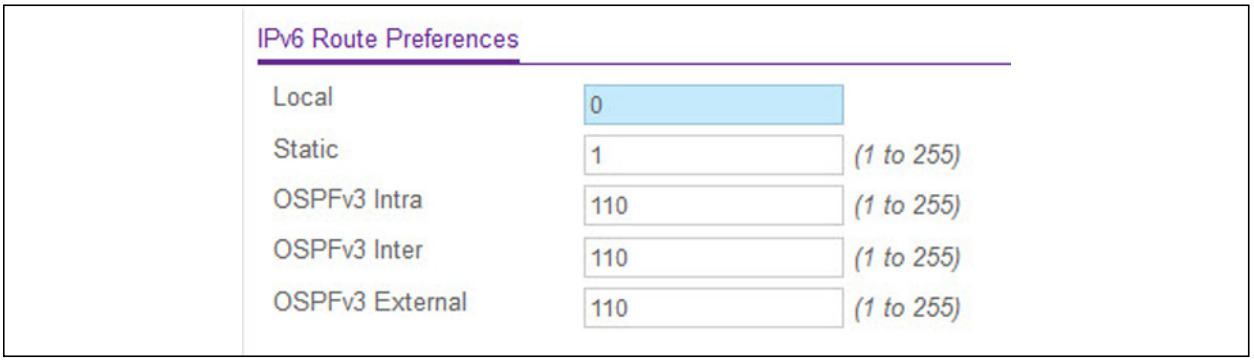
Field	Description
Number of Routes	Displays the total number of active routes in the route table.
IPv6 Prefix	Displays the network prefix for the active route.
Prefix Length	Displays the prefix length for the active route.
Protocol	Displays the type of protocol for the active route.

Field	Description
Next Hop Interface	Displays the interface over which the route is active. For a reject route, the next hop would be a *Null0* interface.
Next Hop IP Address	Displays the next hop IPv6 address for the active route.
Preference	Displays the route preference of the configured route.

IPv6 Route Preferences

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

To display the IPv6 Route Preferences page, click **Routing** > **IPv6** > **Advanced** > **Route Preference**. The following page is displayed.



- Configure the IPv6 Route Preferences.

1. In the **Static** field, specify the static route preference value for the router. The range is 1 to 255. The default value is 1.
2. In the **OSPFv3 Intra** field, specify the OSPFv3 intra route preference value in the router. The range is 1 to 255. The default value is 110.
3. In the **OSPFv3 Inter** field, specify the OSPFv3 inter route preference value in the router. The range is 1 to 255. The default value is 110.
4. In the **OSPFv3 External** field, specify the OSPFv3 external route preference value in the router. The range is 1 to 255. The default value is 110.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 94, IPv6 Advanced Route Preferences describes the non-configurable data that is displayed.

Table 94. IPv6 Advanced Route Preferences

Field	Description
Local	The local preference.

IPv6 Tunnel Configuration

Use this screen to create, configure, and delete tunnels.

To display the IPv6 configure page, click **Routing** > **IPv6** > **Advanced** > **Tunnel Configuration**. The following page is displayed.

- Configure IPv6 Tunnel.

1. In the **Tunnel ID** field, select from the list of available tunnel IDs.
2. Select the tunnel Mode from the list of supported modes:
   - 6-in-4-configured
   - 6-to-4
3. Select the **IPv6 Mode** from the list. **Enable** IPv6 on this interface using the IPv6 address. This option is only configurable prior to specifying an explicit IPv6 address.
4. From the **IPv6 Unreachables** list, select to **Enable** or **Disable** the mode of sending ICMPv6 Destination Unreachables on this interface. If Disabled then this interface will not send ICMPv6 Destination Unreachables. By default IPv6 Destination Unreachables mode is enable.
5. In the **IPv6 Address/Prefix Length** field, enter a configured IPv6 address for the selected interface. The address must be entered in the format prefix/length.
6. From the EUI64 list, select to **Enable** or **Disable** the 64-bit extended unique identifier (EUI-64). For 6to4 tunnels, configure the ipv6 address with first 48-bits in the format 2002:tunnel-source-ipv4-address::/48.
7. Specify the desired **Source Address** for this tunnel. This value must be entered in dotted decimal notation.
8. Select the **Source Interface** for this tunnel. The address associated with the selected interface will be used as the source address.
9. Enter the **Destination Address** for this tunnel in dotted decimal notation.
10. Click **Add** to add a new tunnel configuration.
11. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

12. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
13. Click **Delete** to delete the corresponding tunnel.

Table 95, IPv6 Advanced Tunnel Configuration describes the non-configurable data that is displayed.

Table 95. IPv6 Advanced Tunnel Configuration

Field	Description
Interface Link Status	Indicates whether the tunnel interface link status is up or down.

VLAN

You can configure M6100 Chassis switch software with some ports supporting VLANs and some supporting routing. You can also configure the software to allow traffic on a VLAN to be treated as if the VLAN were a router port.

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

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required. This section shows how to configure 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 **Routing > VLAN** link, you can access the following pages:

- *VLAN Routing Wizard* on page 249
- *VLAN Routing Configuration* on page 250

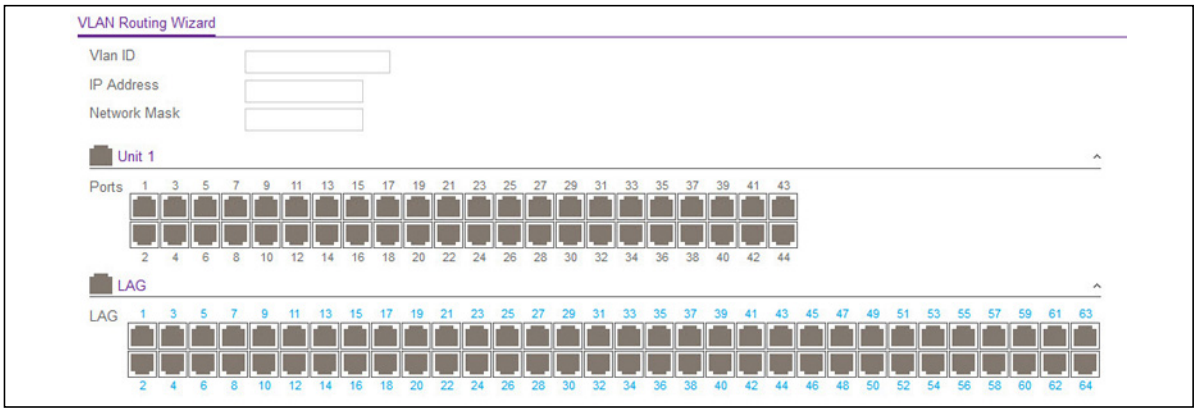
VLAN Routing Wizard

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

- Create a VLAN and generate a unique name for VLAN.

- Add selected ports to the newly created VLAN and remove selected ports from the default VLAN.
- Create a LAG, add selected ports to a LAG, then add LAG to the newly created VLAN.
- Enable tagging on selected ports if the port is in another VLAN. Disable tagging if a selected port does NOT exist in another VLAN.
- Exclude ports NOT selected from the VLAN.
- Enable routing on the VLAN using the IP address and subnet mask entered.

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

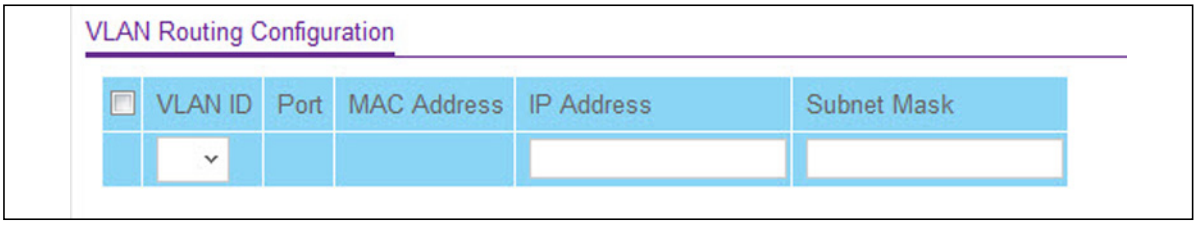


1. Use **VLAN ID** to specify the VLAN Identifier (VID) associated with this VLAN. The range of the VLAN ID is 1 to 4093.
2. Use **Ports** to display selectable physical ports and LAGs (if any). Selected ports will be added to the Routing VLAN. Each port has three modes:
   - T**(Tagged)** - Select the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

VLAN Routing Configuration

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

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



1. From the menu, select the **VLAN ID** that you want to configure for VLAN Routing. This field displays the IDs of all the VLANs 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 **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. 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. M6100 Chassis switch software features both dynamic and manual ARP configuration. With manual ARP configuration, you can statically add entries into the ARP table.

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

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

information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The 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 **Routing > ARP** link, you can access the following pages:

- *Basic* on page 252
- *Advanced* on page 252

Basic

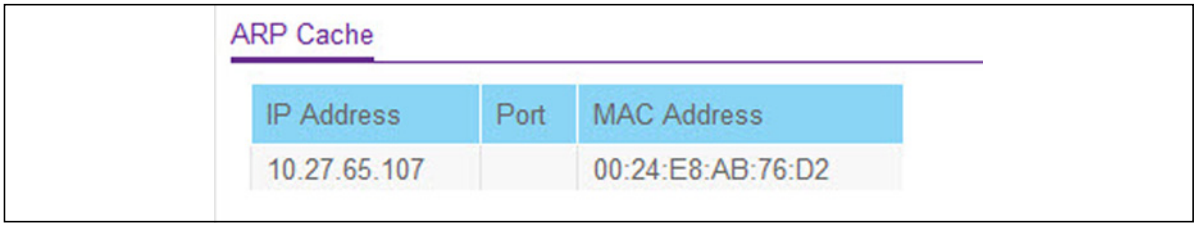
From the **Routing > ARP > Basic** link, you can access the following pages:

- *ARP Cache* on page 252

ARP Cache

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

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



1. **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.
2. The **Port** field displays the associated Unit/Slot/Port of the connection.
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 **Update** to update the page with the latest information on the switch.

Advanced

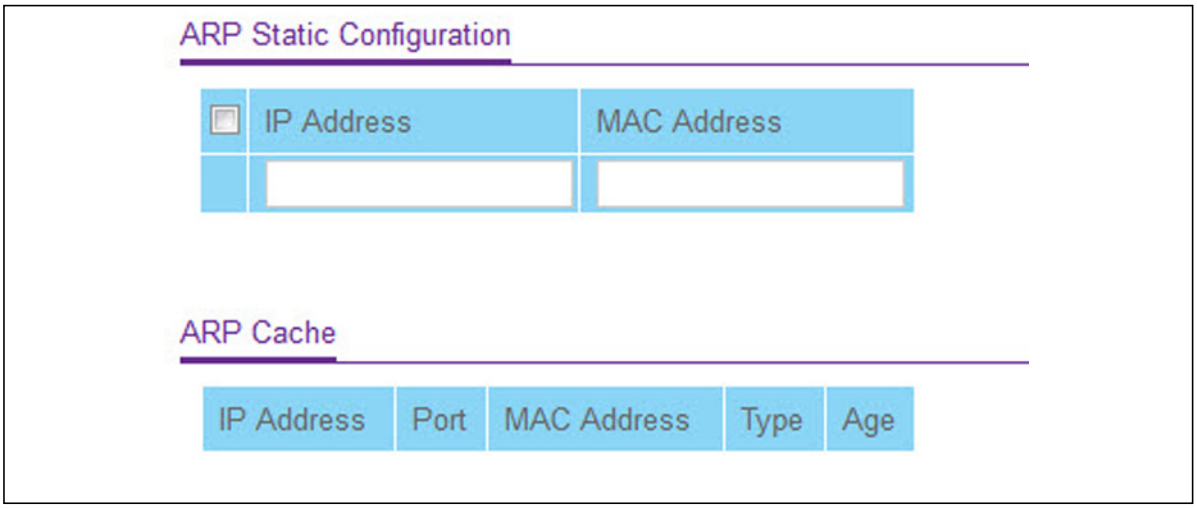
.From the **Routing > ARP > Advanced** link, you can access the following pages:

- *ARP Create* on page 253
- *ARP Table Configuration* on page 254

ARP Create

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

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



ARP Static Configuration

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

1. Use **IP Address** to enter the IP address you want to add. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
2. Use **MAC Address** to specify the unicast MAC address of the device. Enter the address as six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
3. Click **Add** to add a new static ARP entry to the switch.
4. Click **Delete** to delete an existing static ARP entry from the switch.
5. Click **Update** to update the page with the latest information on 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. 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.

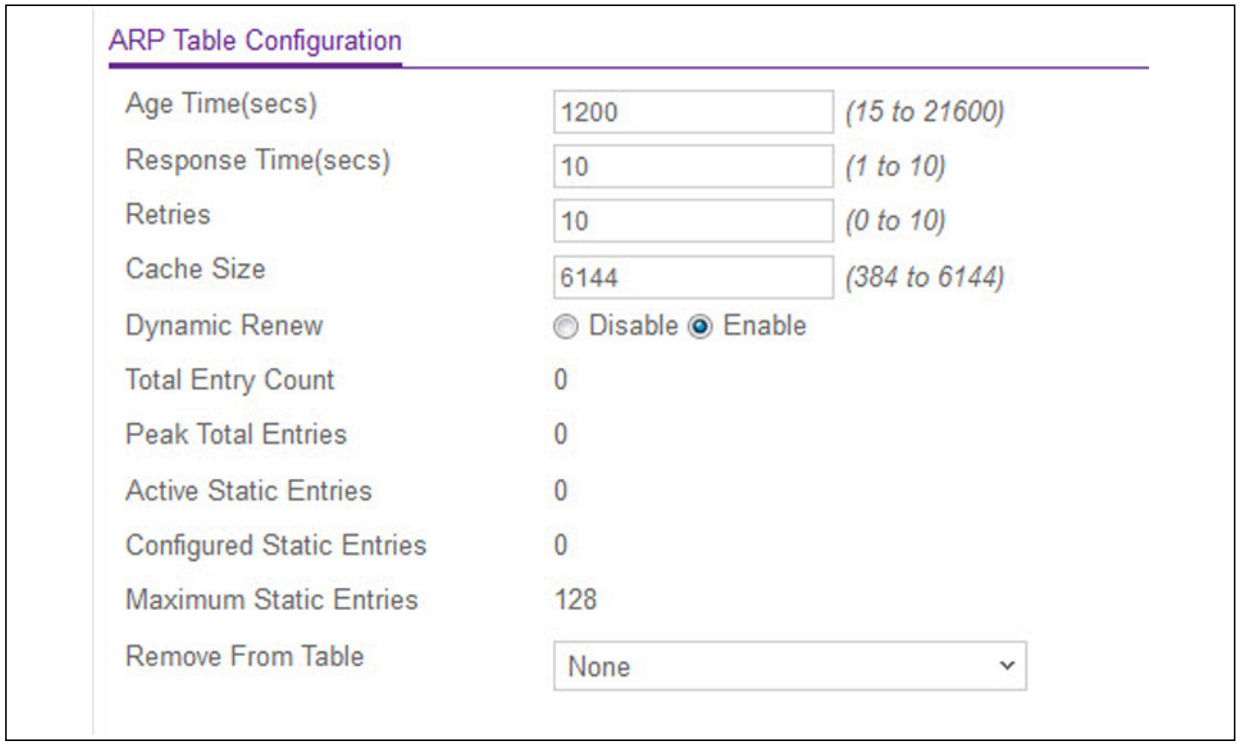
Field	Description
Port	The associated unit/slot/port of the connection.
MAC Address	The unicast MAC address of the device. The address is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
Type	The type of ARP entry. Possible values are: • **Local**—An ARP entry associated with one of the switch's routing interface's MAC addresses. • **Gateway**—A dynamic ARP entry whose IP address is that of a router. • **Static**—An ARP entry configured by the user. • **Dynamic**—An ARP entry that has been learned by the router.
Age	Age since the entry was last refreshed in the ARP table (in seconds).

Click **Update** to update the page with the latest information on the switch.

ARP Table Configuration

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

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



1. Use **Age Time** to enter the value for the switch to use for the ARP entry ageout time. You must enter a valid integer, which represents the number of seconds it will take for an ARP entry to age out. The range for this field is 15 to 21600 seconds. The default value for Age Time is 1200 seconds.
2. Use **Response Time** to enter the value for the switch to use for the ARP response time-out. You must enter a valid integer, which represents the number of seconds the switch will wait for a response to an ARP request. The range for this field is 1 to 10 seconds. The default value for Response Time is 1 second.
3. Use **Retries** to enter an integer that specifies the maximum number of times an ARP request will be retried. The range for this field is 0 to 10. The default value for Retries is 4.
4. Use **Cache Size** to enter an integer that specifies the maximum number of entries for the ARP cache. The range for this field is 64 to 512. 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.

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

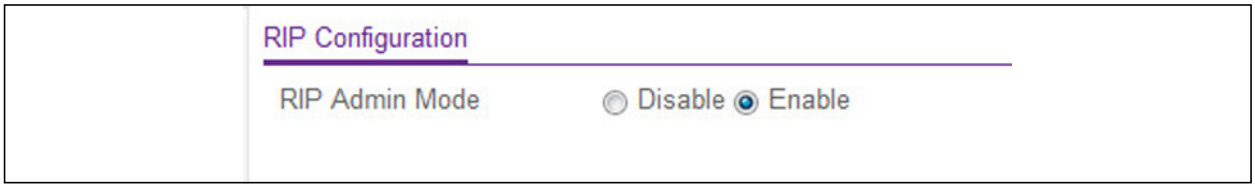
RIP

The **Routing > RIP** tab contains links to the following web pages that you use to configure and display RIP data:

- *Basic RIP Configuration*
- *Advanced RIP Configuration* on page 256

Basic RIP Configuration

➢ To display the Basic RIP Configuration page, click **Routing > RIP > Basic > RIP Configuration**. The following page is displayed.



➢ Configure the RIP settings.

- In the **RIP Admin Mode** field, select the **Enable** or **Disable** option. If you select enable, RIP will be activated for the switch. The default is **Enable**.

Advanced RIP Configuration

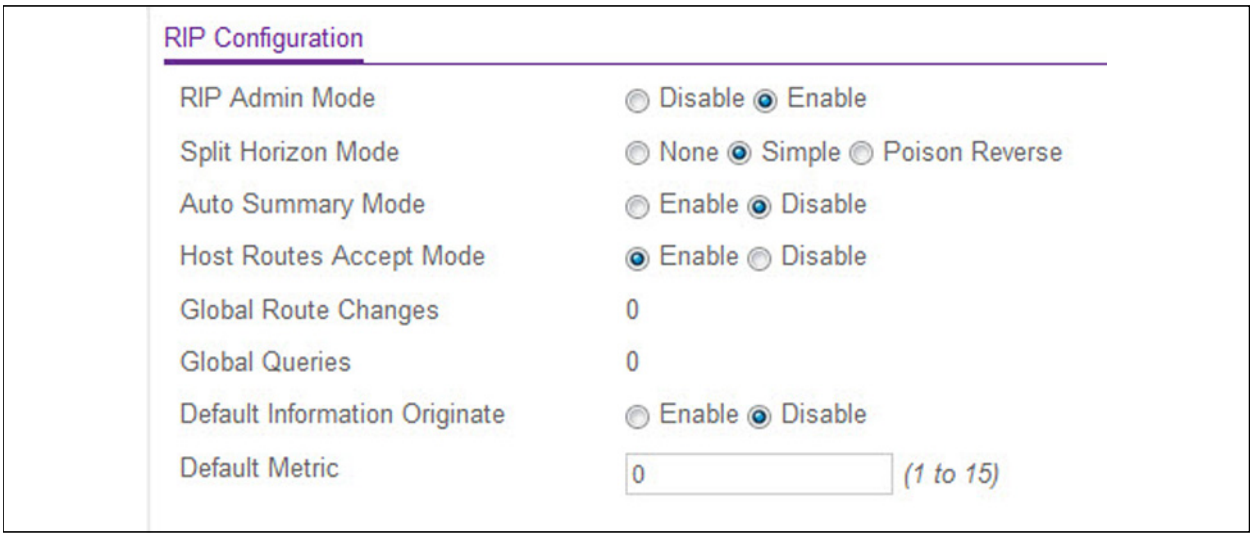
.From the **Routing > RIP > Advanced** link, you can access the following pages:

- *RIP Configuration*
- *Advanced RIP Interface Configuration* on page 258

- *Route Redistribution* on page 260

RIP Configuration

➢ To display the Advanced RIP Configuration page, click **Routing > RIP > Advanced > RIP Configuration**. The following page is displayed.



➢ Configure the advanced RIP settings.

1. In the **RIP Admin Mode** field, select the **Enable** or **Disable** option. If you select enable, RIP will be activated for the switch. By default, RIP is enabled.
2. In the **Split Horizon Mode**, select from the following options:
   - None—No special processing for this case.
   - Simple—A route will not be included in updates sent to the router from which it was learned. The default is simple.
   - Poison Reverse— A route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

   Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned
3. In the **Auto Summary Mode** field, select the **Enable** or **Disable** option. If you select enable, groups of adjacent routes will be summarized into single entries in order to reduce the total number of entries. The default is **Disable**.
4. In the **Host Routes Accept Mode** field, select the **Enable** or **Disable** option. If you select enable, the router will accept host routes. The default is **Enable**.
5. In the **Default Information Originate** field, select to **Enable** or **Disable** default route advertise.
6. In the **Default Metric** field, specify a default value for the metric of redistributed routes. This field displays the default metric if one has already been set, or 0 if one was not configured earlier. The valid values are 1 to 15.

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

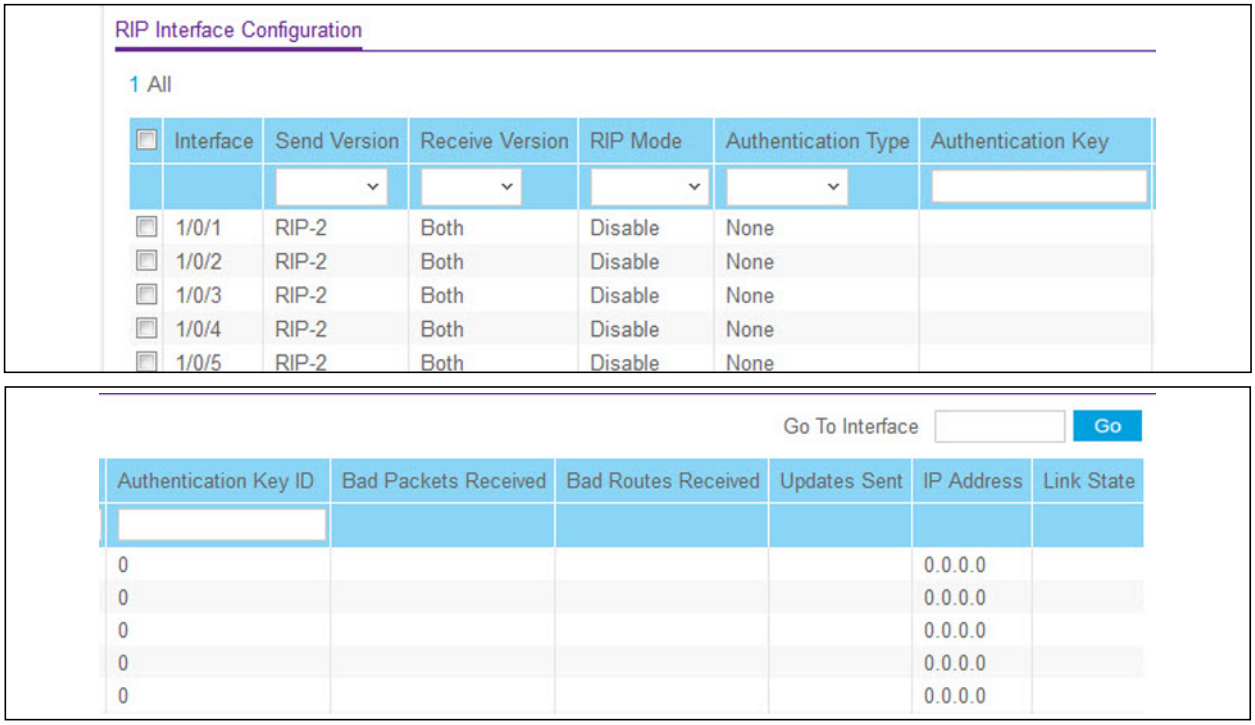
Table 96, RIP Advanced RIP Configuration describes the non-configurable data that is displayed.

Table 96. RIP Advanced RIP Configuration

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

Advanced RIP Interface Configuration

- To display the Advanced RIP Interface Configuration page, click **Routing > RIP > Advanced > Interface Configuration**. The following page is displayed.



- **Configure the advanced RIP Interface Configuration settings.**

1. Select the check box next to the **Interface** for which data is to be displayed or configured.
2. In the **Go To Interface** field, enter the Interface in unit/slot/port format and click the **Go** button. The entry corresponding to the specified interface will be selected.

3. From the **Send Version** list, select the version of RIP control packets that the interface should send. The value is one of the following:
   - **None**—No RIP control packets will be sent.
   - RIP-1—Send RIP version 1 formatted packets via broadcast.
   - RIP-1c—RIP version 1 compatibility mode. Send RIP version 2 formatted packets via broadcast.
   - RIP-2—Send RIP version 2 packets using multicast. The default is RIP-2.
4. From the **Receive Version** list, select which RIP control packets the interface will accept. The value is one of the following:
   - RIP-1—Accept only RIP version 1 formatted packets.
   - RIP-2—Accept only RIP version 2 formatted packets.
   - Both—Accept packets in either format. The default is Both.
   - None—No RIP control packets will be accepted.
5. Select **Enable** or **Disable** from the **RIP Mode** list. Before you enable RIP version 1 or version 1c on an interface, you must first enable network directed broadcast mode on the corresponding interface. The default value is disable.
6. Select the **Authentication Type** from the list. The types are:
   - **None**—This is the initial interface state. If you select this option, no authentication protocols will be run.
   - **Simple**—If you select **Simple**, you will be prompted to enter an authentication key. This key will be included, in the clear, in the RIP header of all packets sent on the network. All routers on the network must be configured with the same key.
   - **Encrypt**— If you select **Encrypt**, you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.
7. Enter the RIP **Authentication Key** for the specified interface. If you choose **Authentication Type None** above, you will not be prompted to enter a key. If you choose **Simple** or **Encrypt**, the key may be up to 16 octets long. The key value will only be displayed if you are logged on with Read/Write privileges.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. Click **Update** to update the page with the latest information on the switch.

Table 97, RIP Advanced Interface Configuration describes the non-configurable data that is displayed.

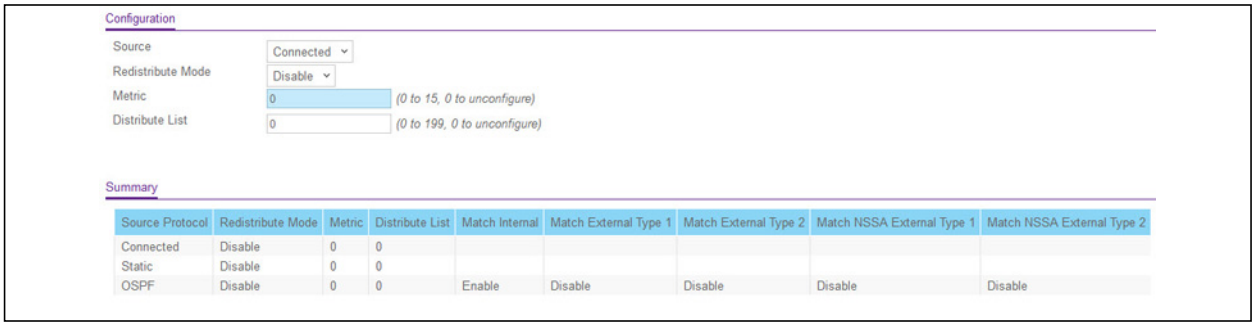
Table 97. RIP Advanced Interface Configuration

Field	Description
Bad Packets Received	The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.
Bad Routes Received	The number of routes, in valid RIP packets, which were ignored for any reason (for example, unknown address family, or invalid metric).
Updates Sent	The number of triggered RIP updates actually sent on this interface. This explicitly does *not* include full updates sent containing new information.
IP Address	The IP Address of the router interface.
Link State	Indicates whether the RIP interface is up or down.

Route Redistribution

Use this screen to configure the RIP Route Redistribution parameters. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

- To display the Advanced RIP Route Redistribution Configuration page, click **Routing > RIP > Advanced > Route Redistribution**. The following page is displayed.



- Configure the Advanced RIP Route Redistribution Configuration settings.

1. The **Source** list is populated by only those source routes that have already been configured for redistribution by RIP. This allows you to configure another source route among the available source routes. Valid values are:
   - **Connected**
   - **Static**
   - **OSPF**
2. From the **Redistribute Mode** list, select to Enable or Disable RIP Redistribute Mode. The default is disable.
3. Enter the **Metric** of redistributed routes for the given source route. Valid value for the Metric is 0 to 15; 0 means unconfigure.
4. Use the **Distribute List** field to set the Access List that filters the routes to be redistributed by the destination protocol. Only permitted routes are redistributed. If this command refers to

a non-existent access list, all routes are permitted. The valid values for Access List IDs are 0 to 199. When used for route filtering, the only fields in an access list that get used are:

- Source IP Address and netmask
- Destination IP Address and netmask
- Action (permit or deny)

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

The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route.

Note: A 1 in the mask indicates a *do not care* in the corresponding address bit.

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

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

Table 98, RIP Route Redistribution Summary describes the RIP Route Redistribution non-configurable data that is displayed.

Table 98. RIP Route Redistribution Summary

Field	Description
Source Protocol	The source route to be redistributed by RIP. The valid values are: • Connected • Static • OSPF
Redistribute Mode	The route-redistribution mode for a particular source protocol. By default this is disabled.
Metric	The metric of redistributed routes for the given source route. The field displays **0** when the metric is not configured.
Distribute List	The Access List that filters the routes to be redistributed by the Destination Protocol. The field displays **0** when not configured.
The following list of redistributed routes is valid when **OSPF** is selected as source. The list may include one or more of:	
Match Internal	Sets Internal OSPF Routes to be redistributed.

Field	Description
Match External Type 1	Sets External Type 1 OSPF Routes to be redistributed.
Match External Type 2	Sets External Type 2 OSPF Routes to be redistributed.
Match NSSA External Type 1	Sets NSSA External Type 1 OSPF Routes to be redistributed.
Match NSSA External Type 2	Sets NSSA External Type 2 OSPF Routes to be redistributed.

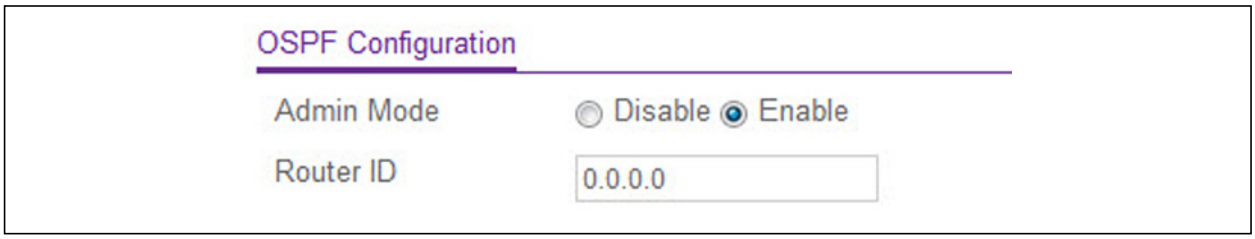
OSPF

The **Routing > OSPF** folder contains links to the following web pages that you use to configure and display OSPF data:

- *Basic OSPF Configuration* on page 262
- *Advanced OSPF Configuration* on page 263

Basic OSPF Configuration

➢ To display the Basic OSPF Configuration page, click **Routing > OSPF > Basic > OSPF Configuration**. The following page is displayed.



➢ Configure the OSPF settings.

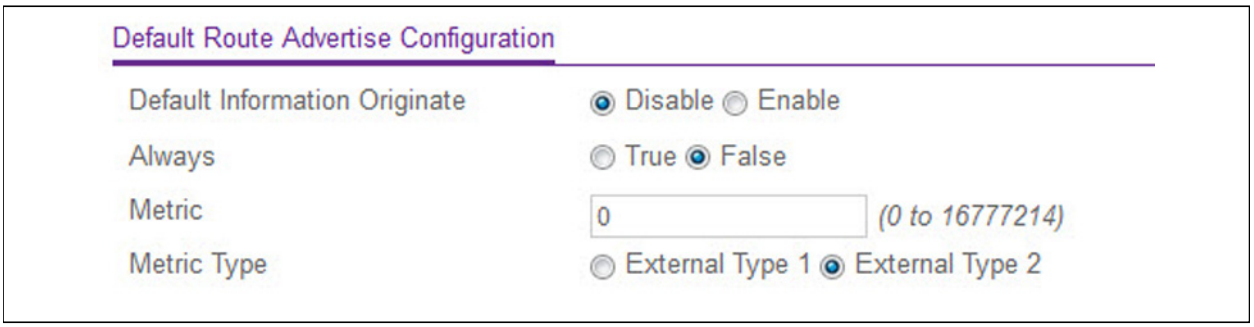
1. In the **Admin Mode** field, select the **Enable** or **Disable** option. If you select enable, OSPF will be activated for the switch. By default, OSPF is **Enabled**. You must configure a Router ID before OSPF can become operational. Use the IP Configuration page to configure a Router ID or issue the CLI command **config router id**. For more information, see *IP Configuration* on page 217.
2. The Router ID is the 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID, you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

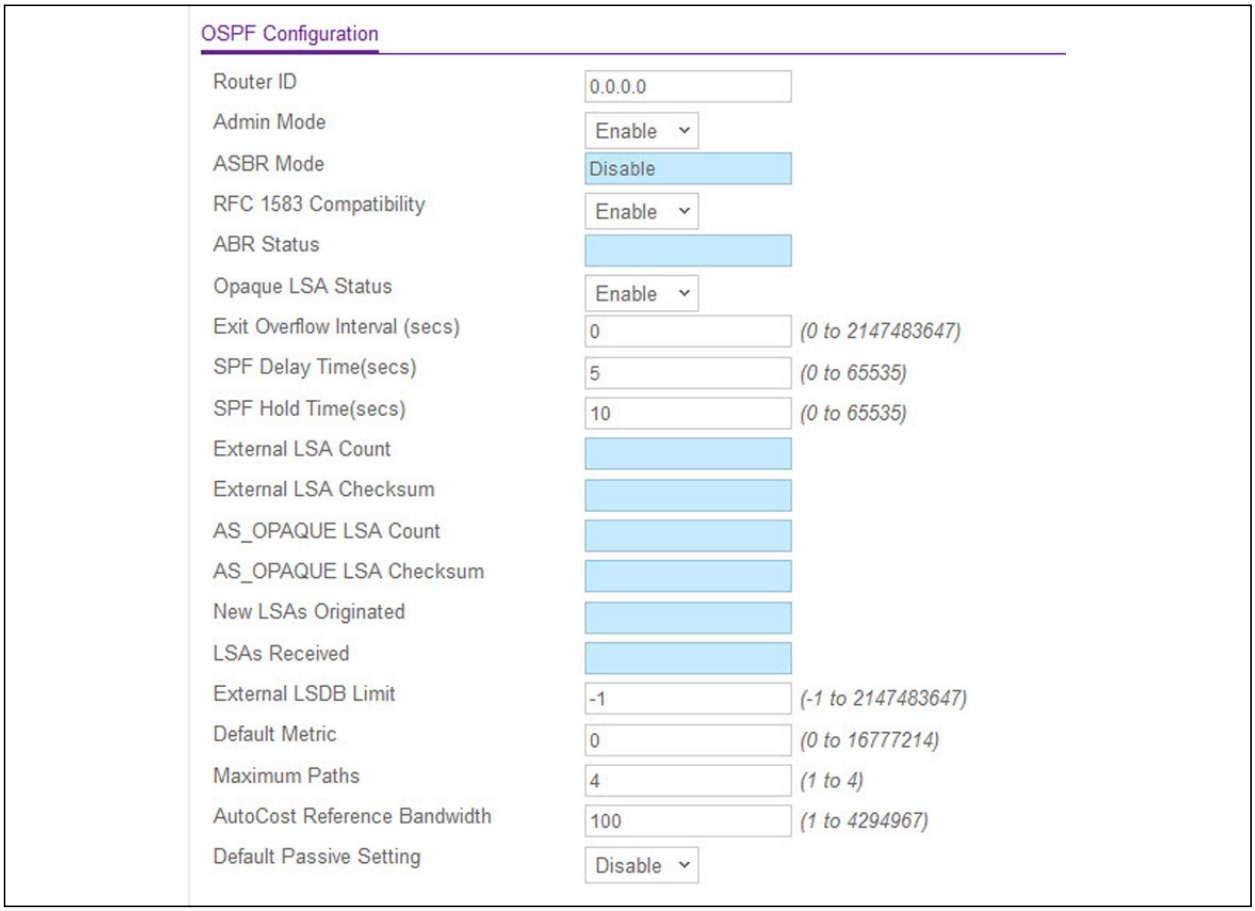
Advanced OSPF Configuration

From the **Routing > OSPF > Advanced** link, you can access the following pages:

OSPF Configuration

➢ To display the Default Route Advertise Configuration page, click **Routing > OSPF > Advanced > OSPF Configuration**. The following page is displayed.





- **Configure the Default Route Advertise settings.**

  1. In the **Default Information Originate** field, select the **Enable** or **Disable** option. If you select enable, OSPF originates an external LSA advertising a default route (0.0.0.0/0.0.0.0). Default Information Originate is **Disabled** by default.
  2. In the **Always** field, select **True** or **False**. If **Default Information Originate** is enabled, but the **Always** option is **False**, OSPF will only originate a default route if the router already has a default route in its routing table. Set **Always** to **True** to force OSPF to originate a default route regardless of whether the router has a default route. The default is **False**.
  3. In the **Metric** field, specify the metric of the default route. Valid values range from 0 to 16777214. The default is **0**.
  4. In the **Metric Type** field, select the OSPF metric type of the default route. Two types are supported: **External Type 1** and **External Type 2**. The default is **External Type 2**.
  5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
  6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

- Configure the OSPF Configuration settings.

7. In the **Router ID** field, enter the 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID, you must first disable OSPF. After you set the new Router ID, you must reenable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
8. In the **Admin Mode** field, select **Enable** or **Disable** from the list. If you select **Enable**, OSPF will be activated for the switch. The default value is **Enable**. You must configure a Router ID before OSPF can become operational. You do this on the **IP Configuration** page, or by issuing the CLI command: **config router id**. For more information, see *IP Configuration* on page 217.
9. In the **RFC 1583 Compatibility** field, select **Enable** or **Disable** from the list to specify the preference rules that will be used when choosing among multiple AS-external-LSAs advertising the same destination. If you select **Enable**, the preference rules will be those defined in Section 16.4.1 of the OSPF-2 standard (RFC 2328), which prevents routing loops when AS-external-LSAs for the same destination have been originated from different areas. The default value is **Enable**. All routers in the OSPF domain must be configured the same. If all OSPF routers are capable of operating according to RFC 2328, **RFC 1583 Compatibility** should be disabled.
10. Set the **Opaque LSA Status** to **Enable** if OSPF should store and flood opaque LSAs. An opaque LSA is used for flooding user-defined information within an OSPF router domain.
11. When the number of non-default external LSAs exceeds a configured limit, the router enters an overflow state as defined in RFC 1765. Use the **Exit Overflow Interval** field to specify how long in seconds OSPF must wait before attempting to leave overflow state. In overflow state, OSPF cannot originate non-default external LSAs. If the Exit Overflow Interval is 0, OSPF will not leave overflow state until it is disabled and reenabled. The range is 0 to 2,147,483,647 seconds. The default is **0**.
12. Configure the **SPF Delay Time** - the number of seconds from when OSPF receives a topology change to the start of the next SPF calculation. Delay Time is an integer from 0 to 65535 seconds. The default is **5 seconds**. A value of 0 means that there is no delay; that is, the SPF calculation is started upon a topology change.
13. Configure the **SPF Hold Time** - the minimum time in seconds between two consecutive SPF calculations. The range is 0 to 65,535 seconds. The default time is **10 seconds**. A value of 0 means that there is no delay; that is, two SPF calculations can be done, one immediately after the other.
14. Use the **External LSDB Limit** field to set the number of the external LSDB limit for OSPF. If the value is –1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit none-default AS-external-LSAs in the database. The external LSDB limit must be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for the External LSDB Limit field is –1 to 2147483647. The default value is **–1**.
15. Use the **Default Metric** field to set a default for the metric of redistributed routes. This field is blank if a default metric has not been configured. The range of valid values is 1 to 16777214. The default value is **0**.
16. Use the **Maximum Paths** field to set the number of paths that OSPF can report for a given destination. The range of valid values is 1 to 16. The default value is **4**.

17. Configure the **AutoCost Reference Bandwidth** to control how OSPF calculates link cost. Specify the reference bandwidth in megabits per second. Unless a link cost is configured, the link cost is computed by dividing the reference bandwidth by the interface bandwidth. The range is 1 to 4294967. The default is **100**.
18. In the **Default Passive Setting** field, select **Enable** or **Disable** from the list to configure the global passive mode setting for all OSPF interfaces. Configuring this field overwrites any present interface level passive mode setting. OSPF does not form adjacencies on passive interfaces, but does advertise attached networks as stub networks. The default is **Disabled**.
19. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
20. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 99, OSPF Configuration describes the non-configurable data that is displayed.

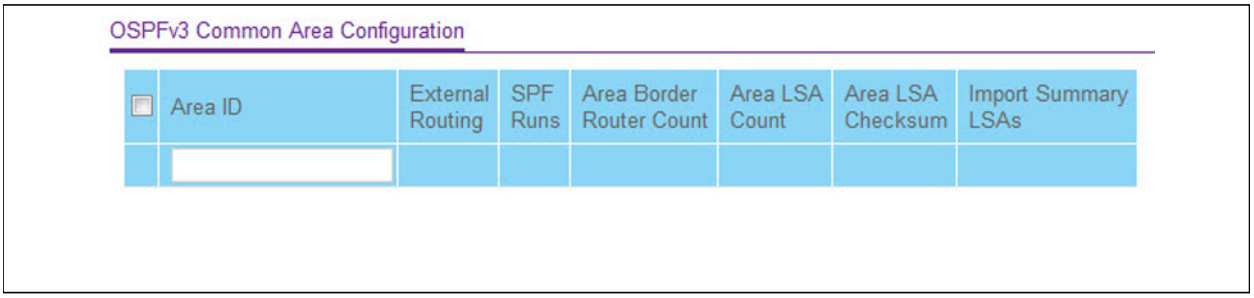
Table 99. OSPF Configuration

Field	Description
ASBR Mode	The router is an Autonomous System Boundary Router if it is configured to redistribute routes from another protocol, or if it is configured to originate an external LSA advertising the default route.
ABR Status	The router is an Autonomous System Boundary Router if it is configured to redistribute routes from another protocol, or if it is configured to originate an external LSA advertising the default route.The router is an Autonomous System Boundary Router if it is configured to redistribute routes from another protocol, or if it is configured to originate an external LSA advertising the default route.
External LSA Count	The number of external (LS type 5) LSAs (link state advertisements) in the link state database.
External LSA Checksum	The sum of the LS checksums of the external LSAs (link state advertisements) contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers. This value is in hexadecimal.
AS_OPAQUE LSA Count	The number of opaque LSAs with domain-wide flooding scope.
AS_OPAQUE LSA Checksum	The sum of the LS checksums of the opaque LSAs with domain wide flooding scope. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers. This value is in hexadecimal.

Field	Description
New LSAs Originated	In any given OSPF area, a router will originate several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it will originate network-LSAs for those networks. This value represents the number of LSAs originated by this router.
LSAs Received	The number of LSAs (Link State Advertisements) received that were determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.

OSPF Common Area Configuration

- To display the OSPF Common Area Configuration page, click **Routing > OSPF > Advanced > Common Area Configuration**. The following page is displayed.



- Configure the Area ID.

1. Enter the OSPF **Area ID.** An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Click **Add** to add the Area ID.
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 **Delete** to delete a selected Area ID.

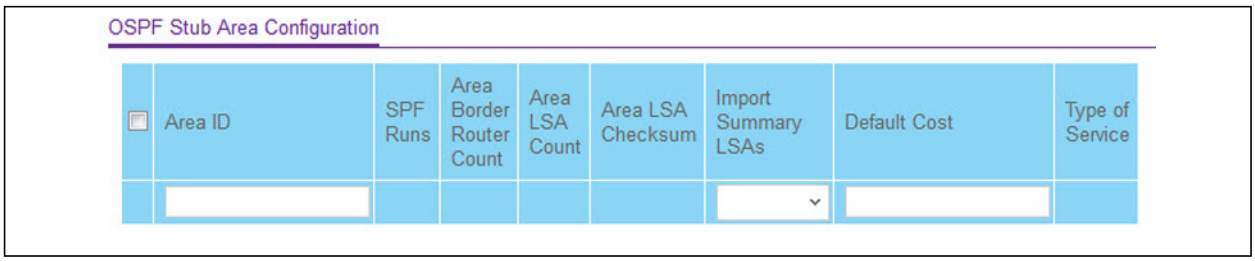
Table 100, OSPF Common Area Configuration on page 268 describes the non-configurable data that is displayed.

Table 100. OSPF Common Area Configuration

Field	Description
External Routing	A definition of the router's capabilities for the area, including whether or not AS-external-LSAs are flooded into/throughout the area. If the area is a stub area, then these are the possible options for which you may configure the external routing capability, otherwise the only option is *Import External LSAs*. • Import External LSAs—Import and propagate external LSAs. • Import No LSAs—Do not import and propagate external LSAs.
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Flood List Length	This is the number of LSAs on this area's flood list.
Import Summary LSAs	The summary LSAs will be enabled/disabled imported into this area.

OSPF Stub Area Configuration

➢ To display the OSPF Stub Area Configuration page, click **Routing > OSPF > Advanced > Stub Area Configuration**. The following page is displayed.



- Configure the Stub Area.

  1. Enter the OSPF **Area ID.** An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
  2. Configure the **Import Summary LSAs** by selecting **Enable** or **Disable** from the list. If you select **Enable**, summary LSAs will be imported into stub areas.
  3. Configure the **Default Cost** by entering the metric value you want applied for the default route advertised to the stub area. Valid values range from 1 to 16,777,215.
  4. Click **Add** to configure the area as a stub area.
  5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
  6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
  7. Click **Delete** to delete the stub area designation. The area will be returned to normal state.

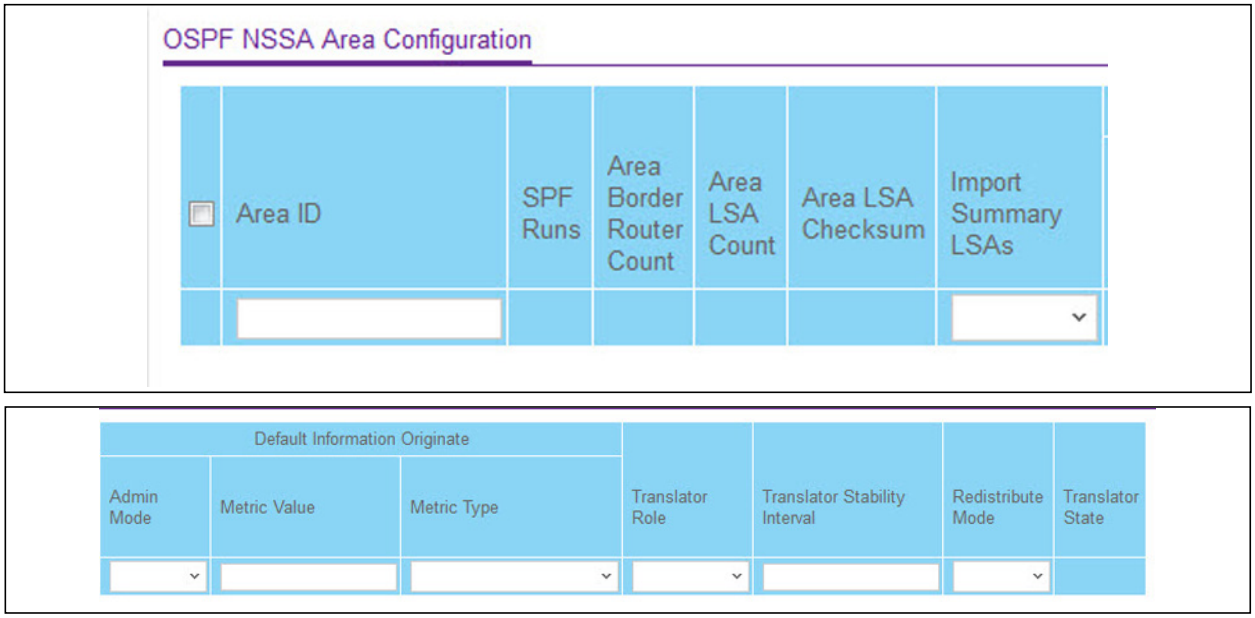
  Table 101, OSPF Stub Area Configuration on page 269 describes the non-configurable data that is displayed.

Table 101. OSPF Stub Area Configuration

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

OSPF NSSA Area Configuration

➢ To display the OSPF NSSA Area Configuration page, click **Routing > OSPF > Advanced > NSSA Area Configuration**. The following page is displayed.



➢ **Configure the NSSA Area.**

1. Enter the OSPF **Area ID.** An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Configure the **Import Summary LSAs** by selecting **Enable** or **Disable** from the list. If you select **Enable**, summary LSAs will be imported into NSSA areas.
3. Configure the **Default Information Originate**—The default Route Information. This option permits you to advertise a default route into the NSSA when Import Summary LSAs is disabled. This can also be applied by the CLI command **area (area-id) NSSA default-info-originate** in the IP router OSPF config mode.
   a. In the **Admin Mode** list, select to **Enable** or **Disable** the default information originate.
   b. In the **Metric Value** field, set the default metric value for default information originate. The value range of values is 1 to 16777214.
   c. In the **Metric Type** field, select the type of metric specified in the Metric Value field. Options are:
      - **Comparable Cost—**External Type 1 metrics that are comparable to the OSPF metric.
      - **Non-comparable Cost**—External Type 2 metrics that are assumed to be larger than the cost of the OSPF metric.
4. Select the **Translator Role** of the NSSA. Options are:
   a. **Always**—Cause the router to assume the role of the translator the instant it becomes a border router.

   b. **Candidate**—Cause the router to participate in the translator election process when it attains border router status.
5. In the **Translator Stability Interval** field, configure the translator of the NSSA. The value is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router. The valid range is 0 to 3600.
6. In the **Redistribute Mode** field, select to **Enable** or **Disable** from the list to configure the NSSA ABR so that learned external routes will be redistributed to the NSSA.
7. Click **Add** to configure the area as an NSSA area.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. Click **Delete** to delete the NSSA area designation. The area will be returned to normal state.

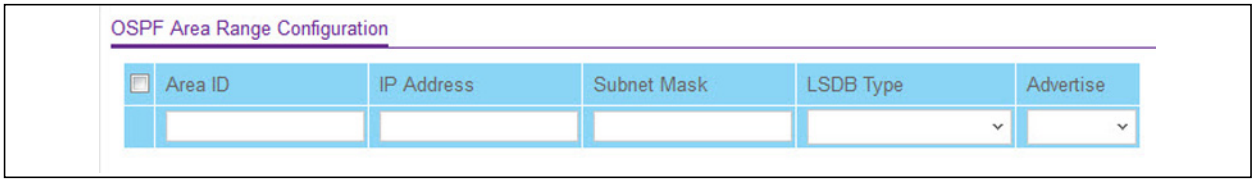
Table 102, OSPF NSSA Area Configuration describes the non-configurable data that is displayed.

Table 102. OSPF NSSA Area Configuration

Field	Description
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Translator State	This field displays if and how the NSSA border router translates type-7 into type-5. Possible options are: • Enabled—The NSSA border router's translator role has been set to always. • Elected—The candidate NSSA border router is translating type-7 LSAs into type-5. • Disabled—The candidate NSSA border router is not translating type-7 LSAs into type-5.

OSPF Area Range Configuration

- To display the OSPF Area Range Configuration page, click **Routing > OSPF > Advanced > Area Range Configuration**. The following page is displayed.

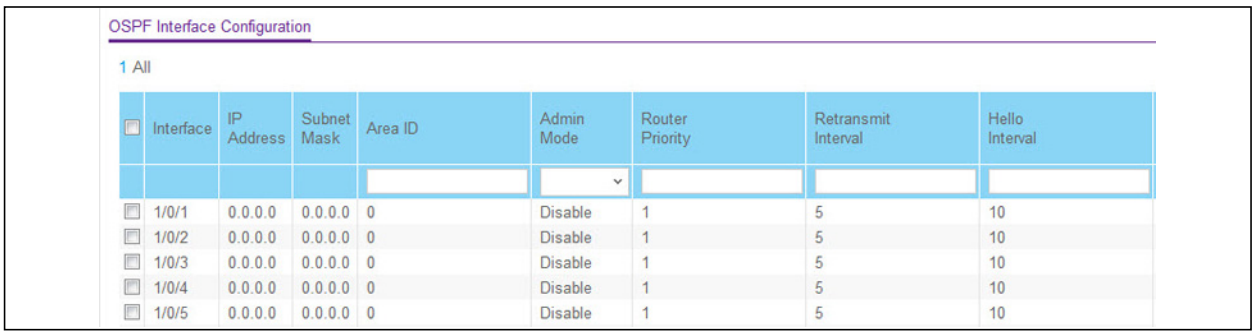


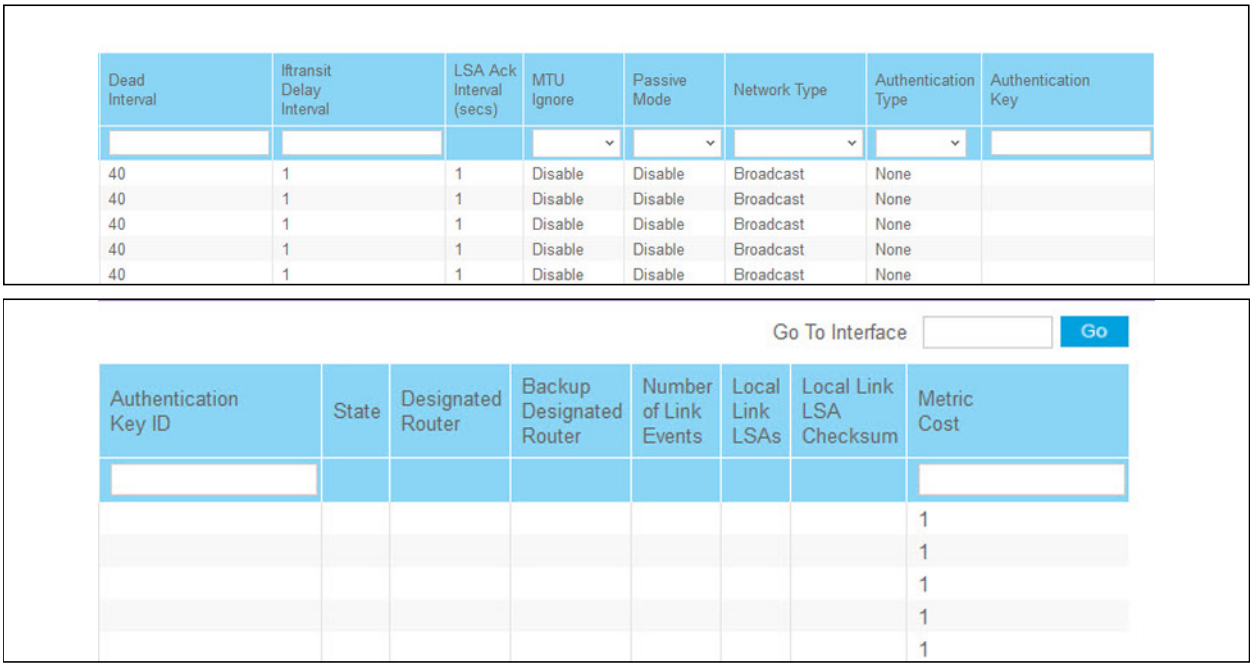
- Configure the OSPF Area Range.

1. Enter the OSPF **Area ID.** An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Enter the **IP Address** for the address range for the selected area.
3. Enter the **Subnet Mask** for the address range for the selected area.
4. From the list in the **LSDB Type** field, select the type of Link Advertisement associated with the specified area and address range. Options are: **Network Summary** or **NSSA External**. The default type is **Network Summary**.
5. Configure the **Advertise** field by selecting **Enable** or **Disable** from the list. If you select **Enable**, the address range is advertised outside the area via a Network Summary LSA. The default is **Enable**.
6. Click **Add** to add the new address range to the switch.
7. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
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 **Delete** to remove the specified address range from the area configuration.

OSPF Interface Configuration

- To display the OSPF Interface Configuration page, click **Routing > OSPF > Advanced > Interface Configuration**. The following page is displayed.





Dead Interval	Iftransit Delay Interval	LSA Ack Interval (secs)	MTU Ignore	Passive Mode	Network Type	Authentication Type	Authentication Key
40	1	1	Disable	Disable	Broadcast	None	
40	1	1	Disable	Disable	Broadcast	None	
40	1	1	Disable	Disable	Broadcast	None	
40	1	1	Disable	Disable	Broadcast	None	
40	1	1	Disable	Disable	Broadcast	None	

➢ **Configure the OSPF Interface.**

1. In the **Go To Interface** field, enter the Interface in unit/slot/port format and click the **Go** button. The entry corresponding to the specified interface will be selected.
2. Select the check box next to the **Interface** for which data is to be displayed or configured.
3. In the OSPF **Area ID** field, enter the 32-bit integer in dotted decimal format that uniquely identifies the OSPF area to which the selected router interface connects. If you assign an Area ID which does not exist, the area will be created with default values.
4. Configure the **Admin Mode** by selecting **Enable** or **Disable** from the list. The default value is **Disable**. You can configure OSPF parameters without enabling OSPF Admin Mode, but they will have no effect until you enable Admin Mode. The following information will be displayed only if Admin Mode is enabled:
   - State
   - Designated Router
   - Backup Designated Router
   - Number of Link Events
   - LSA Ack Interval
   - Metric Cost

   For OSPF to be fully functional, you must enter a valid ID address and subnet mask using either the **IP Interface Configuration** page or the CLI command **config ip interface network**. For more information, see *IP Interface Configuration* on page 229.

Note: Once OSPF is initialized on the router, it will remain initialized until the router is reset.

5. Configure the **Router Priority** by entering the OSPF priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. The default is **1**, which is the highest router priority. A value of 0 indicates that the router is not eligible to become the designated router on this network.
6. Configure the **Retransmit Interval** by entering the OSPF retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 1 to 3600 seconds (1 hour). The default is **5 seconds**.
7. Configure the **Hello Interval** by entering the OSPF hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Value values range from 1 to 65,535. The default is **10 seconds**.
8. Enter the OSPF **Dead Interval** for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should be a multiple of the Hello Interval (for example, 4). Valid values range from 1 to 65,535. The default is **40 seconds**.
9. In the **Iftransit Delay Interval** field, enter the OSPF Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is **1 second**.
10. Configure **MTU Ignore** by selecting **Enable** or **Disable** from the list. MTU Ignore disables OSPF MTU mismatch detection on received database description packets. The default value is **Disable** (MTU mismatch detection is enabled).
11. Configure **Passive Mode** by selecting **Enable** or **Disable** from the list. Make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default, meaning that the Passive Mode default is Disable.
12. Set the OSPF **Network Type** on the interface by selecting either **Broadcast** or **Point-to-Point** from the list. OSPF only selects a designated router and originates network LSAs for broadcast networks. No more than two OSPF routers can be present on a point-to-point link. The default network type for Ethernet interfaces is **Broadcast.**
13. Select an **Authentication Type** other than **None** by selecting from the list. The choices are:
    - **None**—This is the initial interface state. If you select this option from the list, no authentication protocols will be run. The default is None.
    - **Simple**—If you select Simple, you will be prompted to enter an authentication key. This key will be included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
    - **Encrypt**—If you select Encrypt, you will be prompted to enter an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.
14. Enter the **Authentication Key ID** to be used for authentication. You will only be prompted to enter an ID when you select Encrypt as the authentication type. The ID is a number between 0 and 255, inclusive.
15. In the **Metric Cost** field, enter the link cost. OSPF uses this value in computing shortest paths. The range is from 1 to 65,535. The default is **1**.

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

Table 103, OSPF Interface Configuration describes the non-configurable data that is displayed.

Table 103. OSPF Interface Configuration

Field	Description
IP Address	The IP address of the interface.
Subnet Mask	The network mask, indicating the portion of the IP address that identifies the attached network.
LSA Ack Interval (secs)	The number of seconds to wait before sending a delayed acknowledgement.

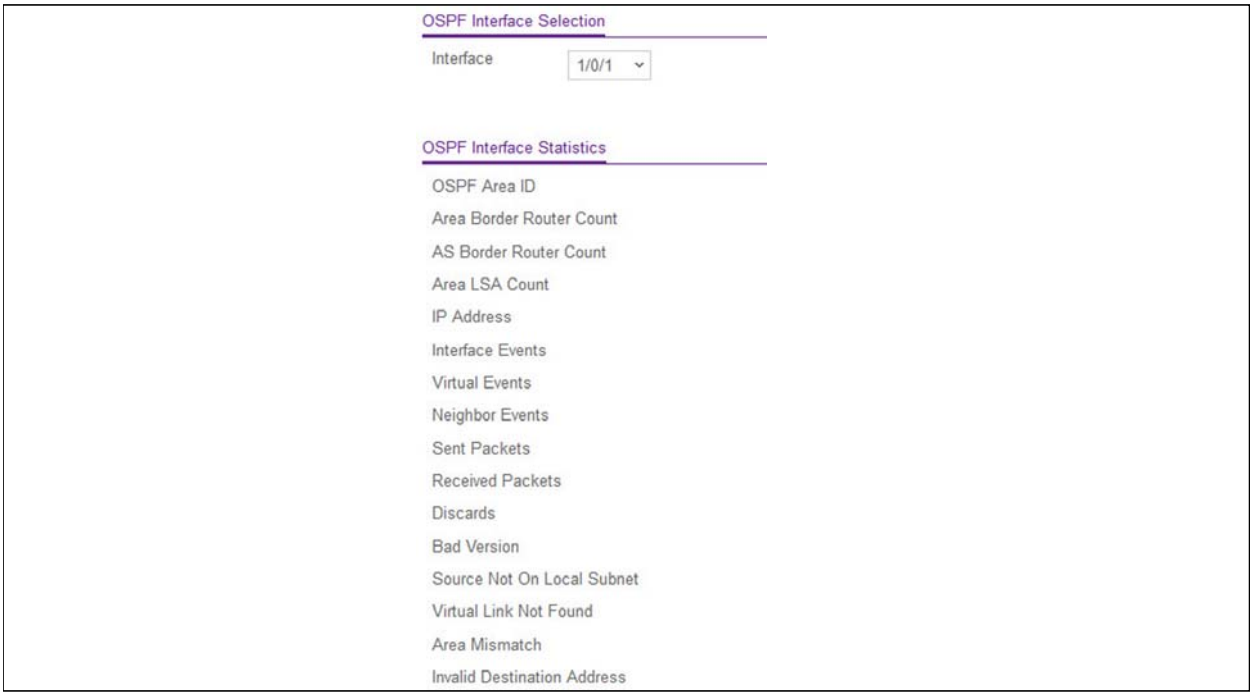
Field	Description
State	The current state of the selected router interface.State is one of the following: • **Down**—This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface. • **Loopback**—In this state, the router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. However, it may still be desirable to gain information on the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets may still be addressed to an interface in Loopback state. To facilitate this, such interfaces are advertised in router- LSAs as single host routes, whose destination is the IP interface address. • **Waiting**—The router is trying to determine the identity of the (Backup) Designated Router for the network by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router. • **Designated Router**—This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network. • **Backup Designated Router**—This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the LSA flooding, as compared to the Designated Router. • Other Designated Router—The interface is connected to a broadcast on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.

Field	Description
Designated Router	The identity of the Designated Router for this network, in the view of the advertising router. The Designated Router is identified here by its router ID. The value 0.0.0.0 means that there is no Designated Router. This field is only displayed if the OSPF admin mode is enabled.
Backup Designated Router	The identity of the Backup Designated Router for this network, in the view of the advertising router. The Backup Designated Router is identified here by its router ID. Set to 0.0.0.0 if there is no Backup Designated Router.
Number of Link Events	This is the number of times the specified OSPF interface has changed its state.
Local Link LSAs	The number of opaque LSAs whose flooding scope is the link on this interface.
Local Link LSA Checksum	The sum of the checksums of local link LSAs for this link.

OSPF Interface Statistics

This screen displays statistics for the selected interface. The information will be displayed only if OSPF is enabled.

- To display the OSPF Interface Statistics page, click **Routing > OSPF > Advanced > Interface Statistics**. The following page is displayed.



1. In the OSPF Interface Selection area of the screen, from the list in the **Interface** field, select the interface for which data is to be displayed.
2. Click **Clear** to clear all the statistics of the OSPF interface.
3. Click **Update** to update the page with the latest information on the switch.

Table 104, OSPF Interface Statistics on page 278 describes the non-configurable OSPF Interface Statistics data that is displayed.

Table 104. OSPF Interface Statistics

Field	Description
OSPF Area ID	The OSPF area to which the selected router interface belongs. An OSPF Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which the interface connects.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass
AS Border Router Count	The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IP Address	The IP address of the interface.
Interface Events	The number of times the specified OSPF interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that have occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Sent Packets	The number of OSPF packets transmitted on the interface.

Field	Description
Received Packets	The number of valid OSPF packets received on the interface.
Discards	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
Source Not on Local Subnet	The number of received packets discarded because the source IP address is not within a subnet configured on a local interface.
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.
Area Mismatch	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
Wrong Authentication Type	The number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface.
Authentication Failure	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
Invalid OSPF Packet Type	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

Field	Description
Hellos Sent	The number of Hello packets sent on this interface by this router.
Hellos Received	The number of Hello packets received on this interface by this router.
DD Packets Sent	The number of Database Description packets sent on this interface by this router.
DD Packets Received	The number of Database Description packets received on this interface by this router.
LS Requests Sent	The number of LS Requests sent on this interface by this router.
LS Requests Received	The number of LS Requests received on this interface by this router.
LS Updates Sent	The number of LS updates sent on this interface by this router.
LS Updates Received	The number of LS updates received on this interface by this router.
LS Acknowledgements Sent	The number of LS acknowledgements sent on this interface by this router.
LS Acknowledgements Received	The number of LS acknowledgements received on this interface by this router.

OSPF Neighbor Table

This screen displays the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information will be displayed only if OSPF is enabled.

- To display the OSPF Neighbor Table page, click **Routing > OSPF > Advanced > Neighbor Table**. The following page is displayed.

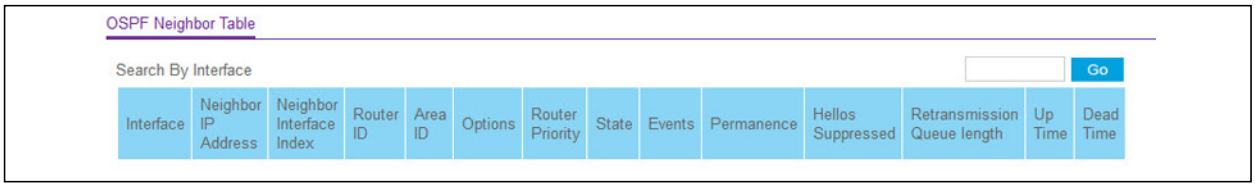


Table 105, OSPF Neighbor Table describes the non-configurable data that is displayed.

Table 105. OSPF Neighbor Table

Field	Description
Interface	Displays the interface for which data is to be displayed or configured. Slot 0 is the base unit.
Neighbor IP Address	The IP address of the neighboring router's interface to the attached network. It is used as the destination IP address when protocol packets are sent as unicasts along this adjacency. Also used in router-LSAs as the Link ID for the attached network if the neighboring router is selected to be designated router. The Neighbor IP address is learned when Hello packets are received from the neighbor. For virtual links, the Neighbor IP address is learned during the routing table build process.
Neighbor Interface Index	A Unit/Slot/Port identifying the neighbor interface index.
Router ID	A 32-bit integer in dotted decimal format representing the neighbor interface.
Area ID	The area ID of the OSPF area associated with the interface.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (for example, neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Field	Description
State	The state of a neighbor can be the following: • **Down**—This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor. On NBMA networks, Hello packets may still be sent to *Down* neighbors, although at a reduced frequency. • **Attempt**—This state is only valid for neighbors attached to NBMA networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor. This is done by sending the neighbor Hello packets at intervals of Hello Interval. • **Init**—In this state, a Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor (i.e., the router itself did not appear in the neighbor's Hello packet). All neighbors in this state (or greater) are listed in the Hello packets sent from the associated interface. • **2-Way**—In this state, communication between the two routers is bidirectional. This has been assured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The (Backup) Designated Router is selected from the set of neighbors in state 2-Way or greater. • **Exchange Start**—This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies. • **Exchange**—In this state the router is describing its entire link state database by sending Database Description packets to the neighbor. In this state, Link State Request Packets may also be sent asking for the neighbor's more recent LSAs. All adjacencies in Exchange state or greater are used by the flooding procedure. These adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets. • **Loading**—In this state, Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. • **Full**—In this state, the neighboring routers are fully adjacent. These adjacencies will now appear in router-LSAs and network-LSAs.

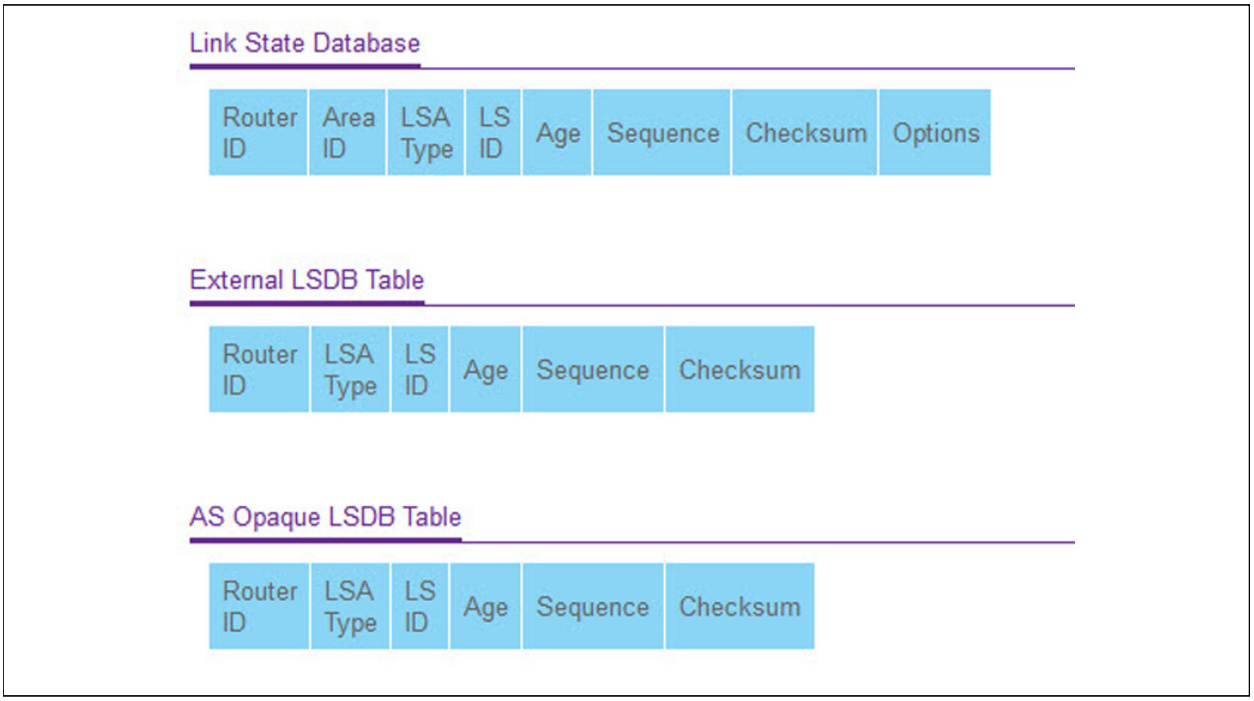
Field	Description
Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Permanence	This variable displays the status of the entry. **Dynamic** and **Permanent** refer to how the neighbor became known
Hellos Suppressed	This indicates whether Hellos are being suppressed to the neighbor.
Retransmission Queue Length	An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.
Up Time	Neighbor uptime; how long since the adjacency last reached the Full state.
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

- Click **Clear** to clear all the neighbors in the table.
- Click **Update** to update the page with the latest information on the switch.

OSPF Link State Database

This screen displays the OSPF Link State Database information.

➢ To display the OSPF Link State Database page, click **Routing > OSPF > Advanced > Link State Database**. The following page is displayed.



OSPF Link State Database

Table 106, OSPF Link State Database on page 284 describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 106. OSPF Link State Database

Field	Description
Router ID	The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the IP Configuration page. If you want to change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
Area ID	The ID of an OSPF area to which one of the router interfaces is connected. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which an interface is connected.
LSA Type	The format and function of the link state advertisement. LSA Type is one of the following: • Illegal • Router Links • Network Links • Network Summary • ASBR Summary • AS-external • Group Member • NSSA • TMP2 • Link Opaque • Area Opaque • AS Opaque • Unknown
LS ID	The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.

Field	Description
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.
Options	The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. The options are: • Q—This enables support for QoS Traffic Engineering. • E—This describes the way AS-external-LSAs are flooded. • MC—This describes the way IP multicast datagrams are forwarded according to the standard specifications. • O—This describes whether Opaque-LSAs are supported. • V—This describes whether OSPF++ extensions for VPN/COS are supported.

External Link State Database Table

Table 107, OSPF External Link State Database Table describes the non-configurable data that is displayed in the External Link State Database (LSDB) table.

Click **Update** to update the page with the latest information on the switch.

Table 107. OSPF External Link State Database Table

Field	Description
Router ID	The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the IP Configuration page. If you want to change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
LSA Type	The format and function of the link state advertisement. LSA Type is one of the following: • ASBR Summary • AS-external • NSSA • TMP2
LS ID	The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

AS Opaque Link State Database Table

Table 108, OSPF AS Opaque Link State Database Table describes the non-configurable data that is displayed in the AS Opaque Link State Database (LSDB) table.

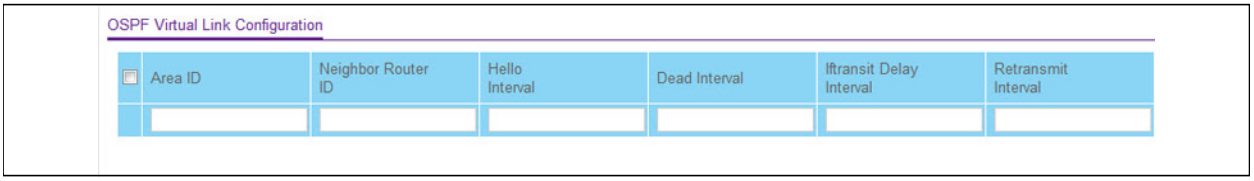
Click **Update** to update the page with the latest information on the switch.

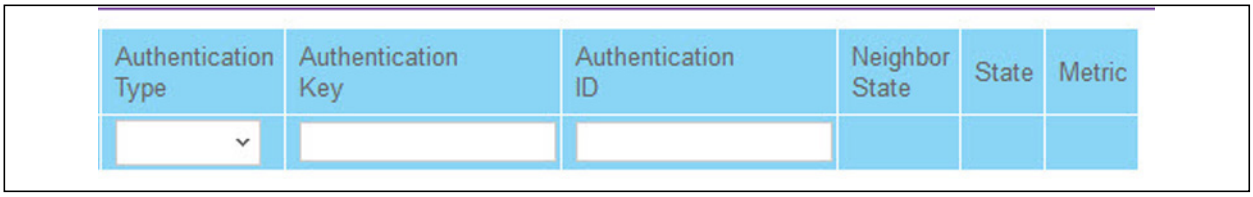
Table 108. OSPF AS Opaque Link State Database Table

Field	Description
Router ID	The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the IP Configuration page. If you want to change the Router ID you must first disable OSPF. After you set the new Router ID, you must re-enable OSPF to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
LSA Type	The format and function of the link state advertisement. LSA Type is one of the following: • Area Opaque • AS Opaque • Link Opaque
LS ID	The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

OSPF Virtual Link Configuration

➢ To display the OSPF Virtual Link Configuration page, click **Routing > OSPF > Advanced > Virtual Link Configuration**. The following page is displayed.





- **Configure the OSPF Virtual Link.**

1. Enter the **Area ID** of the OSPF area. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.
2. Configure the **Neighbor Router ID** by entering the neighbor portion of a Virtual Link specification. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.
3. In the **Hello Interval** field, enter the OSPF hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.
4. In the **Dead Interval** field, enter the OSPF dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should a multiple of the Hello Interval (for example, 4). Valid values range from 1 to 65,535. The default is 40.
5. In the **Iftransit Delay Interval field**, enter the OSPF Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
6. In the **Retransmit Interval** field, enter the OSPF retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.
7. From the **Authentication Type** menu, select one of the following authentication types:
   - **None**—This is the initial interface state.
   - **Simple**—If you select Simple, you will be prompted to enter an authentication key. This key will be included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
   - **Encrypt**—If you select Encrypt you will be prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.
8. In the **Authentication Key** field, enter the OSPF Authentication Key for the specified interface. If you do not choose to use authentication, you will not be prompted to enter a key.
   - If you choose **Simple** authentication you cannot use a key of more than 8 octets.
   - If you choose **Encrypt** the key may be up to 16 octets long.

The key value will only be displayed if you are logged on with Read/Write privileges, otherwise it will be displayed as asterisks.

9. In the **Authentication ID** field, enter the ID to be used for authentication. You will only be prompted to enter an ID when you select **Encrypt** as the authentication type. The ID is a number between 0 and 255, inclusive.
10. Click **Add** to add a new virtual link to the switch.
11. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
12. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
13. Click **Delete** to remove the specified virtual link from the switch configuration.

Table 109, OSPF Virtual Link Configuration on page 290 describes the non-configurable data that is displayed.

Table 109. OSPF Virtual Link Configuration

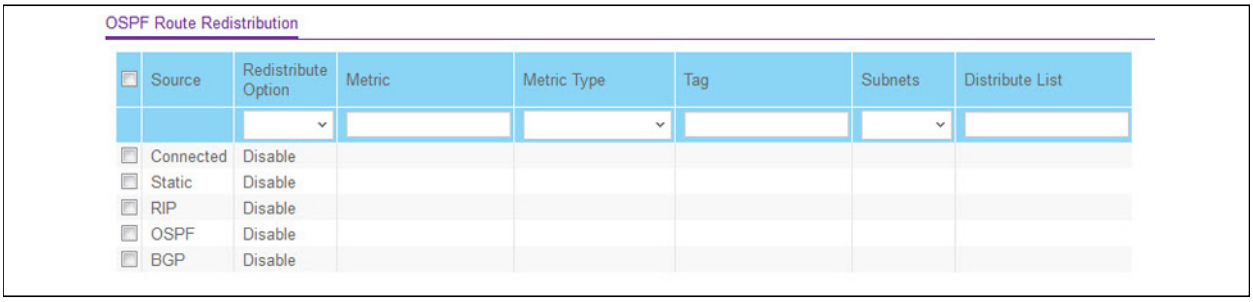
Field	Description
Neighbor State	The OSPF interface state, it can be these values: • **Down**—This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface. • **Waiting**—The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router. • **Point-to-Point**—The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every Hello Interval seconds. • **Designated Router**—This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network. • **Backup Designated Router**—This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router. • **Other Designated Router**—The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.
State	Displays the State of the interface. It takes one the following values: • **Down**—This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface. • **Waiting**—The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router. • **Point-to-Point**—The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every HelloInterval seconds.

Field	Description
State (continued)	• **Designated Router**—This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network. • **Backup Designated Router**—This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router. • **Other Designated Router**—The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.
Metric	The metric value used by the Virtual Link.

OSPF Route Redistribution

Use this screen to configure the OSPF Route Redistribution parameters. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

➢ To display the OSPF Route Redistribution page, click **Routing > OSPF > Advanced > Route Redistribution**. The following page is displayed.



➢ Configure the OSPF Route Redistribution.

1. From the **Source** menu, select from the list of available source routes that have not previously been configured for redistribution by OSPF. The valid values are:
   - BGP
   - Connected
   - OSPF
   - RIP
   - Static

2. In the **Redistribute** list, select to **Enable** or **Disable** the redistribution for the selected source protocol.
3. Set the **Metric** value to be used as the metric of redistributed routes. This fields displays the metric if the source was preconfigured and can be modified. Valid values are 0 to 16777214.
4. From the **Metric Type** list, select the OSPF metric type of redistributed routes
5. Set the **Tag** field in routes redistributed. This field displays the tag if the source was preconfigured, otherwise the tag is 0 and can be modified. Valid values are 0 to 4294967295.
6. From the **Subnets** list, select whether the subnetted routes should be redistributed (Enable) or not (Disable).
7. In the **Distribute List** field, set the Access List that filters the routes to be redistributed by the destination protocol. Only permitted routes are redistributed. If this command refers to a nonexistent access list, all routes are permitted. Valid values for Access List IDs are 1 to 199.

   When used for route filtering, the only fields in an access list that get used are:

   - Source IP Address and netmask
   - Destination IP Address and netmask
   - Action (permit or deny)

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

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

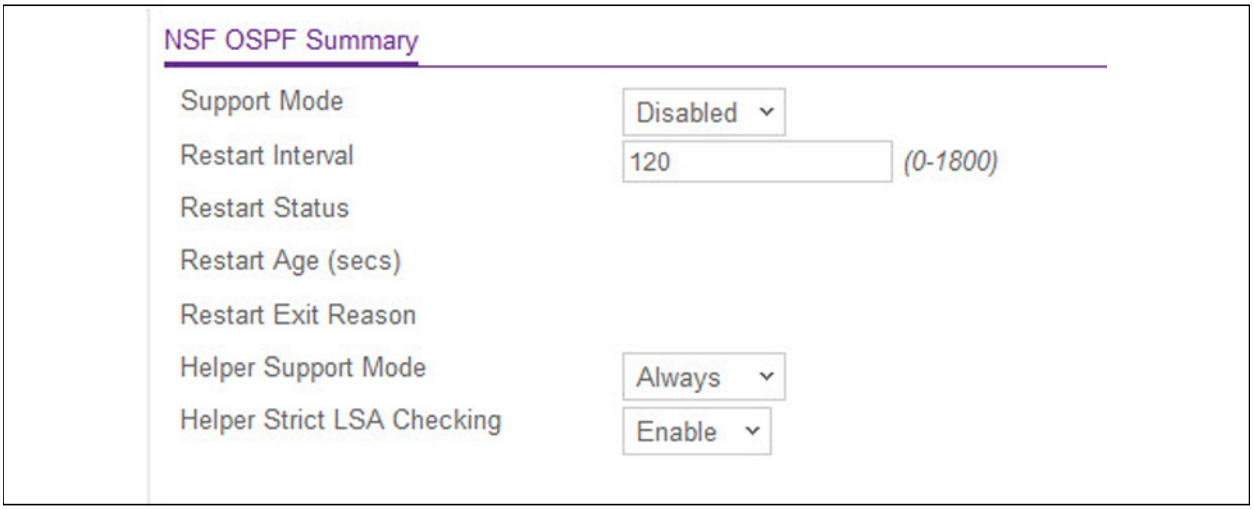
   Note: A 1 in the mask indicates a *do not care* in the corresponding address bit.

   When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the destination of the route. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route's destination mask are significant for the filtering operation.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

NSF OSPF Summary

Use this screen to see the NSF OSPF Summary. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

- To display the NSF OSPF Summary page, click **Routing > OSPF > Advanced > NSF OSPF Summary**. The following page is displayed.



- Configure the NSF OSPF Summary.

1. From the **Support Mode** list, configure how the unit performs graceful restarts by selecting from the following possible values:
   - **Always**—Indicates that OSPF should perform a graceful restart for all planned and unplanned warm restart events.
   - **Disabled**—Disables OSPF from performing graceful restarts.
   - **Planned**—Indicates that OSPF should only perform a graceful restart when a restart is planned (for example, due to an **initiate failover** command).

   The default is **Disabled**.
2. Configure the **Restart Interval**. Valid values are (0 to 1800) in seconds. The default is 120 seconds.
3. Use the **Helper Support Mode** field to configure how the unit will act when a neighbor performs a warm restart. The possible values are:
   - **Always**—Indicates that OSPF should help a restarting neighbor during all planned and unplanned warm restart events.
   - **Disabled**—Disables OSPF from acting as a helpful neighbor.
   - **Planned**—Indicates that OSPF should only help a restarting neighbor during planned events.

   The default is **Always**.
4. Configure **Helper Strict LSA Checking** by selecting **Enable** or **Disable**. When enabled, the unit will exit helper mode whenever the topology changes.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

7. Click **Update** to update the page with the latest information on the switch.

Table 110, NSF OSPF Summary describes the non-configurable data that is displayed.

Table 110. NSF OSPF Summary

Field	Description
Restart Status	Displays the restart status of OSPF Helper feature. The possible values are: • Not Restarting • Planned Restart • Unplanned Restart
Restart Age (seconds)	Displays the amount of time since the last restart occurred.
Restart Exit Reason	Displays how the master unit on the chassis last started up. The possible values are: • Not Attempted—Graceful restart has not been attempted. • In Progress—Restart is in progress. • Completed—The previous graceful restart completed successfully. • Timed Out—The previous graceful restart timed out. • Topology Changed—The previous graceful restart terminated prematurely because of a topology change.

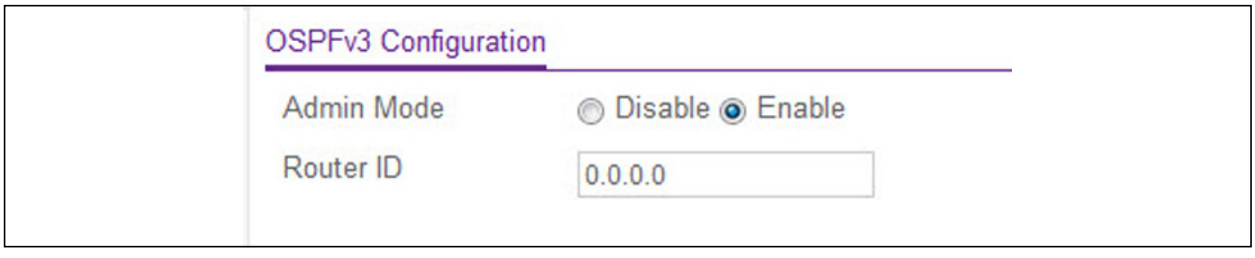
OSPFv3

The **Routing > OSPFv3** folder contains links to the following web pages that you use to configure and display OSPFv3 data:

- *Basic OSPFv3 Configuration* on page 294
- *Advanced OSPFv3 Configuration* on page 295

Basic OSPFv3 Configuration

➢ To display the Basic OSPFv3 Configuration page, click **Routing > OSPFv3 > Basic > OSPFv3 Configuration**. The following page is displayed.



- Configure the OSPFv3 settings.

  1. In the **Admin Mode** field, select the **Enable** or **Disable** option. If you select enable, OSPFv3 will be activated for the switch. By default, OSPFv3 is **Enabled**. You must configure a Router ID before OSPFv3 can become operational. This can also be done by issuing the CLI command **config router id** in ipv6 router ospf mode. For more information, see *IP Configuration* on page 217.

     Note: Once OSPFv3 is initialized on the router, it will remain initialized until the router is reset.

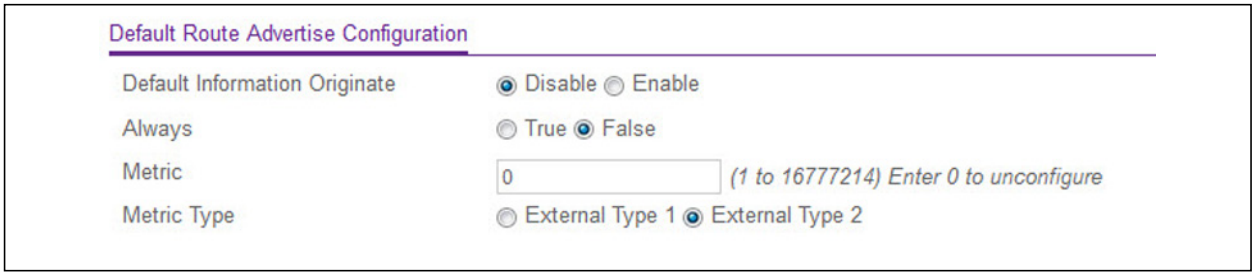
  2. Enter the **Router ID** as a 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID, you must first disable OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
  3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
  4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Advanced OSPFv3 Configuration

From the **Routing > OSPFv3 > Advanced** link, you can access the following pages:

OSPFv3 Configuration

- To display the Default Route Advertise Configuration page, click **Routing > OSPFv3 > Advanced > OSPFv3 Configuration**. The following page is displayed.



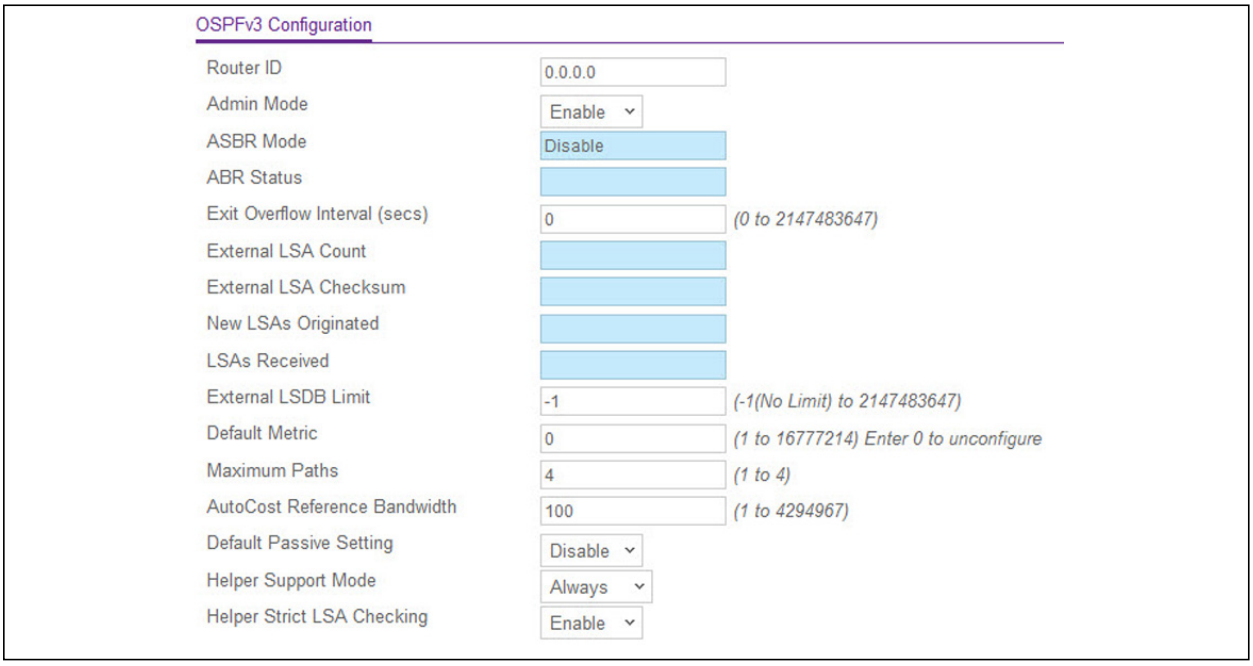
- **Configure the Default Route Advertise Configuration settings.**

1. In the **Default Information Originate** field, select to **Enable** or **Disable** Default Route Advertise. Default Information Originate is **Disabled** by default.

Note: The values for **Always**, **Metric**, and **Metric Type** can only be configured after **Default Information Originate** is set to enable**.** If **Default Information Originate** is set to enable**,** and values for **Always**, **Metric**, and **Metric Type** are already configured, then setting **Default Information Originate** back to disable will set the **Always**, **Metric**, and **Metric Type** values to the default.

---

2. In the **Always** field, select **True** or **False**. When set to True, this field sets the router advertise. The default is **False**.
3. In the **Metric** field, specify the metric of the default route. Valid values range from 0 to 16777214. The default is **0**.
4. In the **Metric Type** field, select the OSPFv3 metric type of the default route. Two types are supported: **External Type 1** and **External Type 2**. The default is **External Type 2**.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.



➢ **Configure the Advanced OSPFv3 Configuration settings.**

7. Enter the **Router ID** in 32-bit integer, dotted decimal format that uniquely identifies the router within the autonomous system (AS). If you want to change the Router ID you must first disable OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
8. In the **Admin Mode** field, select **Enable** or **Disable** from the list. If you select **Enable**, OSPFv3 will be activated for the switch. The default value is **Enable**. You must configure a Router ID before OSPFv3 can become operational. You do this on the **IP Configuration** page, or by issuing the CLI command: **config router id** in ipv6 router ospf mode. For more information, see *IP Configuration* on page 217.

Note: Once OSPFv3 is initialized on the router, it will remain initialized until the router is reset.

9. When the number of non-default external LSAs exceeds a configured limit, the router enters an overflow state as defined in RFC 1765. Use the **Exit Overflow Interval** field to specify the number of seconds that, after entering overflow state, the router must wait before attempting to leave overflow state. Because OSPFv3 cannot originate non-default external LSAs while in overflow state, this allows the router to again originate non-default AS-external-LSAs. If you enter an Exit Overflow Interval of 0, the router will not leave overflow state until it is restarted. The range is 0 to 2,147,483,647 seconds. The default is **0**.
10. Enter the **External LSDB Limit**. This is the maximum number of AS-External-LSAs that can be stored in the database. A value of –1 implies there is no limit on the number that can be saved. The valid range of values is –1 to 2147483647. The default is –1 (no limit).

11. Use the **Default Metric** field to set a default for the metric of redistributed routes. This field displays the default metric if one has already been set, or blank if one was not configured earlier. The valid values are 1 to 16777214. The default is 0 (unconfigure).
12. Use the **Maximum Paths** field to configure the maximum number of paths that OSPFv3 can report to a given destination. The valid values are 1 to 4.
13. Configure the **AutoCost Reference Bandwidth** to control how OSPF calculates default metrics for the interface. The valid values are 1 to 4294967. The default is 100.
14. In the **Default Passive Setting**, select the **Enable** or **Disable** option to configure the global passive mode setting for all OSPF interfaces. Configuring this field overwrites any present interface-level passive mode setting. OSPF does not form adjacencies on passive interfaces, but does advertise attached networks as stub networks.
15. Use **Helper Support Mode** to configure how the unit will act when a neighbor performs a warm restart. The possible values are:
    - Planned—Indicates that OSPF should only help a restarting neighbor during planned events.
    - Always—Indicates that OSPF help a restarting neighbor during all planned and unplanned warm restart events.
    - Disabled—Disables OSPF from acting as a helpful neighbor.
16. Configure **Helper Strict LSA Checking** by selecting the **Enable** or **Disable** option. When enabled, the unit will exit helper mode whenever the topology changes.
17. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
18. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 111, Advanced OSPFv3 Configuration describes the non-configurable data that is displayed.

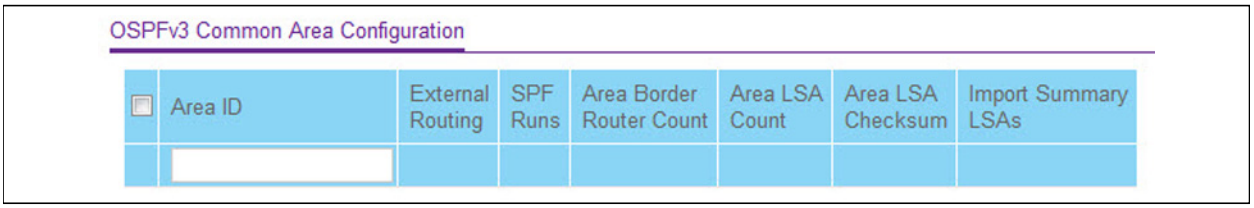
Table 111. Advanced OSPFv3 Configuration

Field	Description
ASBR Mode	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol.
ABR Status	The values of this are enabled or disabled. Enabled implies that the router is an area border router. Disabled implies that it is not an area border router.
External LSA Count	The number of external (LS type 5) link state advertisements (LSAs) in the link state database.
External LSA Checksum	The sum of the LS checksums of the external LSAs contained in the link-state database. This sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state databases of two routers.

Field	Description
New LSAs Originated	In any given OSPFv3 area, a router will originate several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it will originate network-LSAs for those networks. This value represents the number of LSAs originated by this router.
LSAs Received	The number of LSAs received that were determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.

OSPFv3 Common Area Configuration

- To display the OSPFv3 Common Area Configuration page, click **Routing > OSPFv3 > Advanced > Common Area Configuration**. The following page is displayed.



- **Configure the Advanced OSPFv3 Common Area Configuration settings.**

1. In the **Area ID** field, enter the OSPF area ID. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Click **Add** to configure the area as a common area.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. Click **Delete** to delete the common area designation. The area will be returned to normal state.

Table 112, Advanced OSPFv3 Common Area Configuration describes the non-configurable data that is displayed.

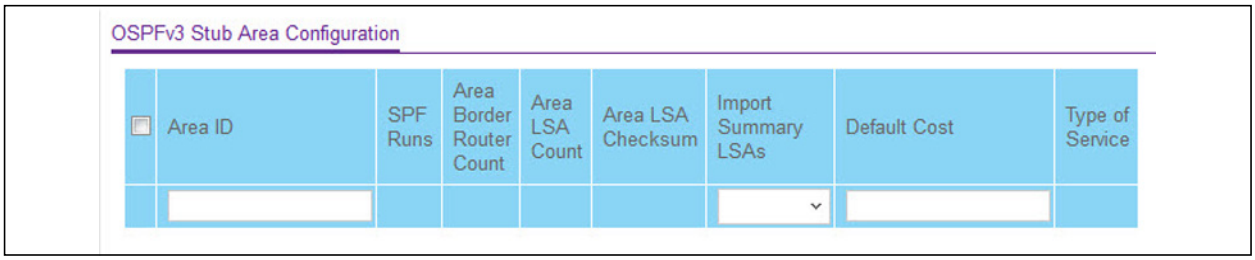
Table 112. Advanced OSPFv3 Common Area Configuration

Field	Description
External Routing	A definition of the router's capabilities for the area, including whether or not AS-external-LSAs are flooded into or throughout the area.
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

Field	Description
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Import Summary LSAs	The summary LSAs will be enabled or disabled imported into this area.

OSPFv3 Stub Area Configuration

- To display the OSPFv3 Stub Area Configuration page, click **Routing > OSPFv3 > Advanced > Stub Area Configuration**. The following page is displayed.



- **Configure the Advanced OSPFv3 Stub Area Configuration settings.**

1. In the **Area ID** field, enter the OSPF area ID. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. In the **Import Summary LSAs** list, select the **Enable** or **Disable** option. If you select enable, summary LSAs will be imported into areas. The default is enable.
3. In **Default Cost**, enter the metric value you want applied for the default route advertised into the stub area. Valid values range from 1 to 16,777,215. This value is applicable only to stub areas.
4. Click **Add** to configure the area as a stub area.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. Click **Delete** to delete the stub area designation. The area will be returned to normal state.

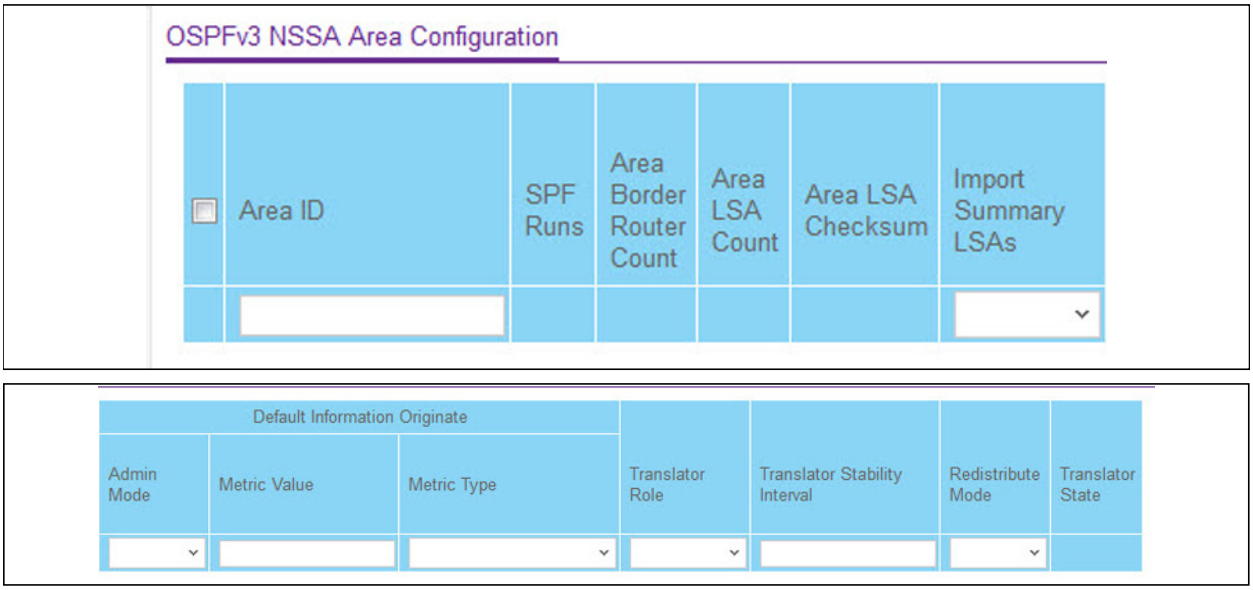
Table 113, Advanced OSPFv3 Stub Area Configuration describes the non-configurable data that is displayed.

Table 113. Advanced OSPFv3 Stub Area Configuration

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

OSPFv3 NSSA Area Configuration

- To display the OSPFv3 NSSA Area Configuration page, click **Routing > OSPFv3 > Advanced > NSSA Area Configuration**. The following page is displayed.



- **Configure the Advanced OSPFv3 NSSA Area Configuration settings.**

1. In the **Area ID** field, enter the OSPF area ID. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Configure the **Import Summary LSAs** by selecting **Enable** or **Disable** from the list. If you select **Enable**, summary LSAs will be imported into stub areas.
3. Configure the **Default Information Originate**—The default Route Information. This option permits you to advertise a default route into the NSSA when Import Summary LSAs is

disabled. This can also be applied by the CLI command **area (area-id) NSSA default-info-originate** in the IP router OSPF config mode.

a. In the **Admin Mode** list, select to **Enable** or **Disable** the default information originate.

b. In the **Metric Value** field, set the default metric value for default information originate. The value range of values is 1 to 16777214.

c. In the **Metric Type** field, select the type of metric specified in the Metric Value field. Options are:

- **Comparable Cost—**External Type 1 metrics that are comparable to the OSPF metric.
- **Non-comparable Cost**—External Type 2 metrics that are assumed to be larger than the cost of the OSPF metric.

4. Select the **Translator Role** of the NSSA. Options are:

a. **Always**—Cause the router to assume the role of the translator the instant it becomes a border router.

b. **Candidate**—Cause the router to participate in the translator election process when it attains border router status.

5. In the **Translator Stability Interval** field, configure the translator of the NSSA. The value is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router. The valid range is 0 to 3600.
6. In the **Redistribute Mode** field, select to **Enable** or **Disable** from the list to configure the NSSA ABR so that learned external routes will be redistributed to the NSSA.
7. Click **Add** to configure the area as an NSSA area.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. Click **Delete** to delete the NSSA area designation. The area will be returned to normal state.

Table 114, Advanced OSPFv3 NSSA Area Configuration describes the non-configurable data that is displayed.

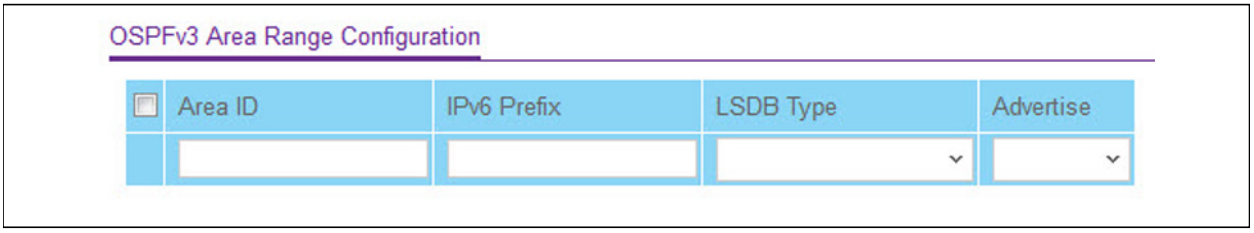
Table 114. Advanced OSPFv3 NSSA Area Configuration

Field	Description
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.

Field	Description
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.
Translator State	The field tells you if and how the NSSA border router translates type-7 into type-5. Possible values are: • Enabled—The NSSA border router's translator role has been set to always. • Elected—The candidate NSSA border router is translating type-7 LSAs into type-5. • Disabled—The candidate NSSA border router is NOT translating type-7 LSAs into type-5.

OSPFv3 Area Range Configuration

➢ To display the OSPFv3 Area Range Configuration page, click **Routing > OSPFv3 > Advanced > Area Range Configuration**. The following page is displayed.

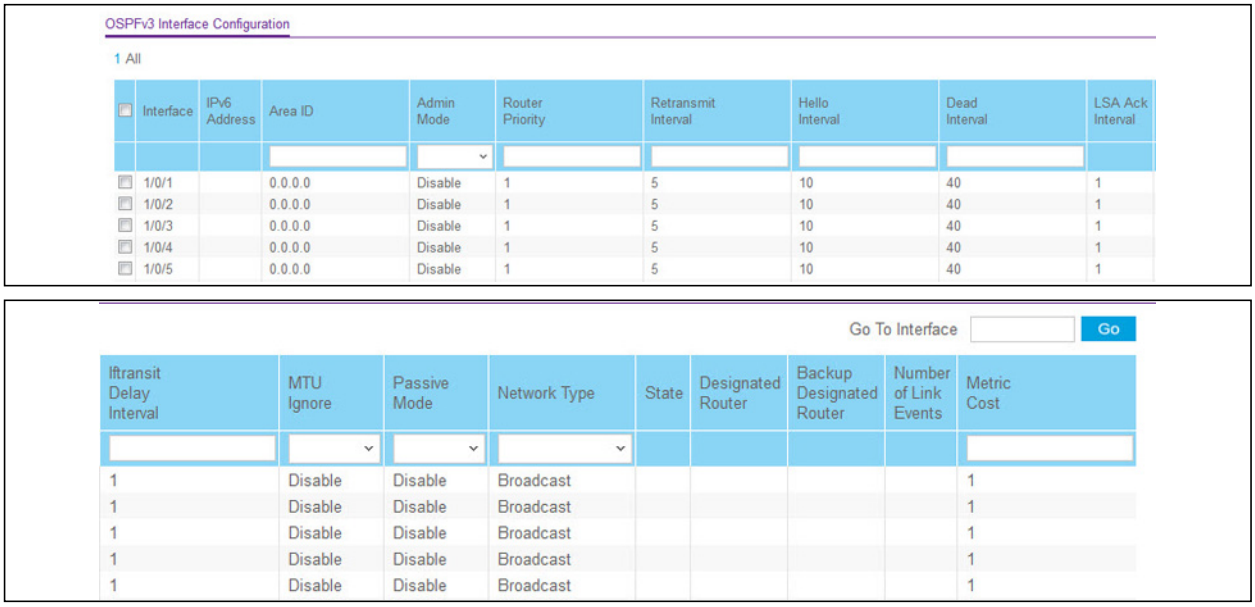


➢ **Configure the OSPFv3 Area Range Configuration settings.**

1. Enter the OSPFv3 **Area ID.** An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.
2. Enter the **IPv6 Prefix** for the address range for the selected area.
3. From the list in the **LSDB Type** field, select the type of Link Advertisement associated with the specified area and address range. Options are: **Network Summary** or **NSSA External**. The default type is **Network Summary**.
4. In the **Advertise** field, select the **Enable** or **Disable** option. If you select **Enable**, the address range is advertised outside the area via a Network Summary LSA. The default is **Enable**.
5. Click **Add** to add the new address range to the switch.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. Click **Delete** to remove the specified address range from the area configuration.

OSPFv3 Interface Configuration

- To display the OSPFv3 Interface Configuration page, click **Routing > OSPFv3 > Advanced > Interface Configuration**. The following page is displayed.



- **Configure the OSPFv3 Interface Configuration settings.**

1. In the **Go To Interface** field, enter the Interface in unit/slot/port format and click the **Go** button. The entry corresponding to the specified interface will be selected.
2. Select the check box next to the **Interface** for which data is to be displayed or configured.
3. In the **Area ID** field, enter the 32-bit integer in dotted decimal format that uniquely identifies the OSPFv3 area to which the selected router interface connects. If you assign an Area ID which does not exist, the area will be created with default values.
4. Configure the **Admin Mode** by selecting the **Enable** or **Disable** option from the list. The default value is **Disable**. You can configure OSPFv3 parameters without enabling OSPFv3 Admin Mode, but they will have no effect until you enable Admin Mode. The following information will be displayed only if Admin Mode is enabled:
   - State
   - Designated Router
   - Backup Designated Router
   - Number of Link Events
   - LSA Ack Interval
   - Metric Cost

   For OSPFv3 to be fully functional, you must enter a valid IPv6 Prefix/Prefix Length. This can be done using the CLI **ipv6 address** command.

Note: Once OSPFv3 is initialized on the router, it will remain initialized until the router is reset.

5. Configure the **Router Priority** by entering the OSPFv3 priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. The default is **1**, which is the highest router priority. A value of 0 indicates that the router is not eligible to become the designated router on this network.
6. Configure the **Retransmit Interval** by entering the OSPFv3 retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 0 to 3600 seconds (1 hour). The default is **5 seconds**.
7. Configure the **Hello Interval** by entering the OSPFv3 hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Value values range from 1 to 65,535. The default is **10 seconds**.
8. Enter the OSPFv3 **Dead Interval** for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should be a multiple of the Hello Interval (for example, 4). Valid values range from 1 to 65,535. The default is **40 seconds**.
9. In the **Iftransit Delay Interval** field, enter the OSPFv3 Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is **1 second**.
10. Configure **MTU Ignore** by selecting **Enable** or **Disable** from the list. MTU Ignore disables OSPF MTU mismatch detection on receiving database description packets. The default value is **Disable** (MTU mismatch detection is enabled).
11. Configure **Passive Mode** by selecting **Enable** or **Disable** from the list. Make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default, meaning that the Passive Mode default is Disable.
12. Set the OSPFv3 **Network Type** on the interface by selecting either **Broadcast** or **Point-to-Point** mode from the list. OSPFv3 only selects a designated router and originates network LSAs for broadcast networks. No more than two OSPFv3 routers can be present on a point-to-point link. The default network type for Ethernet interfaces is **Broadcast.**
13. In the **Metric Cost** field, enter the value for the cost type of service (TOS). OSPF uses this value in computing shortest paths. The range is from 1 to 65,535. The default is **1**. Metric Cost is only configurable if OSPFv3 is initialized on the interface.
14. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
15. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 103, OSPF Interface Configuration describes the non-configurable data that is displayed.

Table 115. Advanced OSPFv3 Interface Configuration

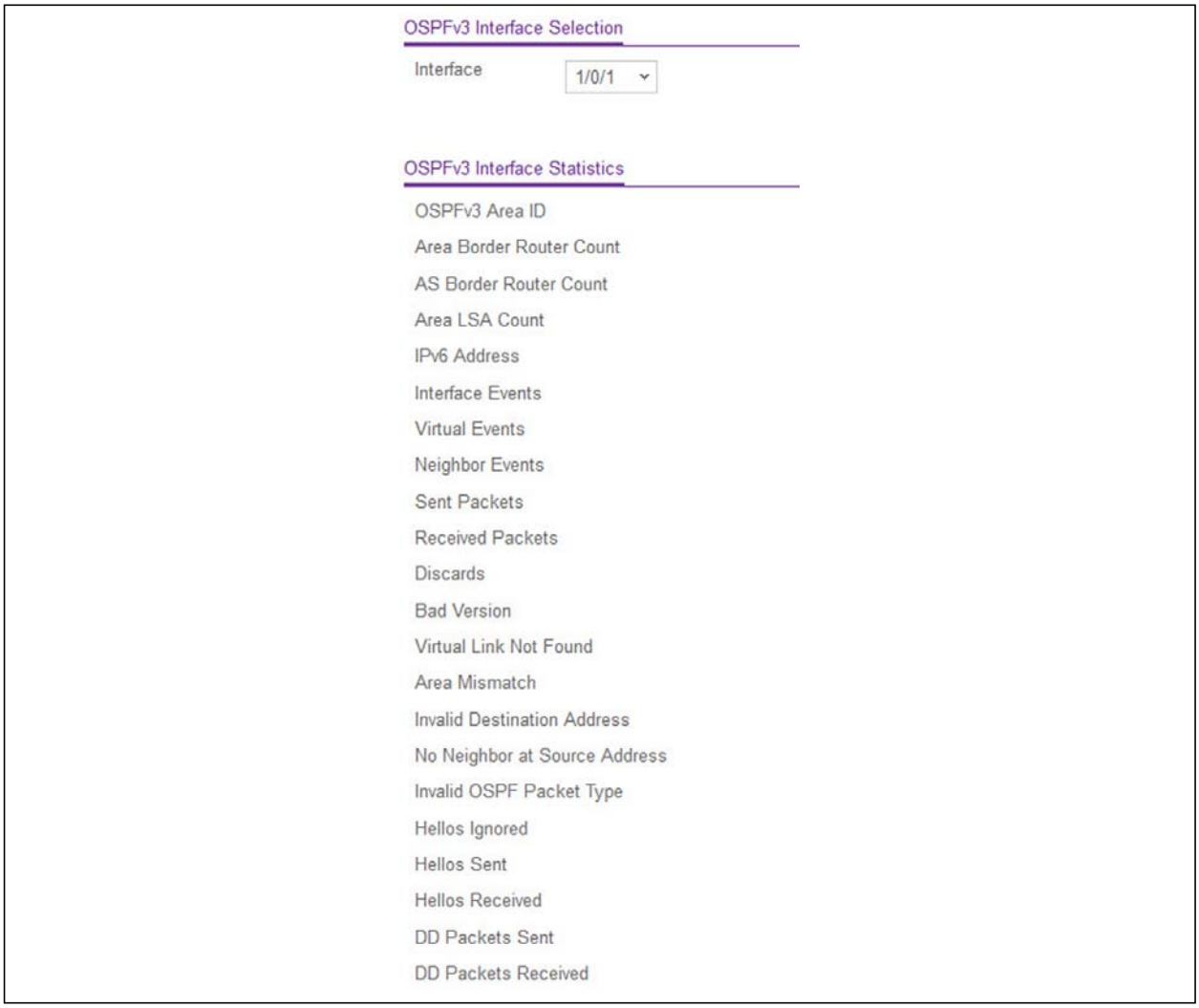
Field	Description
IPv6 Address	The IPv6 address of the interface.
LSA Ack Interval (secs)	The number of seconds between LSA Acknowledgment packet transmissions, which must be less than the Retransmit Interval.
State	The current state of the selected router interface.State is one of the following: • **Down**—This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface. • **Loopback**—In this state, the router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. However, it may still be desirable to gain information on the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets may still be addressed to an interface in Loopback state. To facilitate this, such interfaces are advertised in router-LSAs as single host routes, whose destination is the IP interface address. • **Waiting**—The router is trying to determine the identity of the (Backup) Designated Router for the network by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router. • **Designated Router**—This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network-LSA will contain links to all routers (including the Designated Router itself) attached to the network.

Field	Description
State (cont.)	• **Backup Designated Router**—This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the LSA flooding Procedure, as compared to the Designated Router. • **Other Designated Router**—The interface is connected to a broadcast or NBMA network on which other routers have been selected to be either the Designated Router and Backup Designated Router. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router. **Note:** The State is only displayed if the OSPFv3 Admin Mode is enabled.
Designated Router	The identity of the Designated Router for this network, in the view of the advertising router. The Designated Router is identified here by its router ID. The value 0.0.0.0 means that there is no Designated Router. **Note:** This field is only displayed if the OSPFv3 Admin mode is enabled.
Backup Designated Router	The identity of the Backup Designated Router for this network, in the view of the advertising router. The Backup Designated Router is identified here by its router ID. Set to 0.0.0.0 if there is no Backup Designated Router. **Note:** This field is only displayed if the OSPFv3 Admin mode is enabled.
Number of Link Events	This is the number of times the specified OSPF interface has changed its state. **Note:** This field is only displayed if the OSPFv3 Admin mode is enabled.

OSPFv3 Interface Statistics

This screen displays statistics for the selected interface. The information will be displayed only if OSPFv3 is enabled.

- To display the OSPFv3 Interface Statistics page, click **Routing > OSPFv3 > Advanced > Interface Statistics**. The following page is displayed.



1. In the OSPFv3 Interface Selection area of the screen, from the list in the **Interface** field, select the interface for which data is to be displayed.
2. Click **Clear** to clear all the statistics of the OSPFv3 interface.
3. Click **Update** to update the page with the latest information on the switch.

Table 116, Advanced OSPFv3 Interface Statistics describes the non-configurable OSPF Interface Statistics data that is displayed.

Table 116. Advanced OSPFv3 Interface Statistics

Field	Description
OSPFv3 Area ID	The OSPFv3 area to which the selected router interface belongs. An OSPFv3 Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which the interface connects.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass
AS Border Router Count	The total number of Autonomous System border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IPv6 Address	The IPv6 address of the interface.
Interface Events	The number of times the specified OSPFv3 interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that have occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Sent Packets	The number of OSPFv3 packets transmitted on the interface.
Received Packets	The number of valid OSPFv3 packets received on the interface.
Discards	The number of received OSPFv3 packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPFv3 packets whose version field in the OSPFv3 header does not match the version of the OSPFv3 process handling the packet.
Virtual Link Not Found	The number of received OSPFv3 packets discarded where the ingress interface is in a non-backbone area and the OSPFv3 header identifies the packet as belonging to the backbone, but OSPFv3 does not have a virtual link to the packet's sender.
Area Mismatch	The number of OSPFv3 packets discarded because the area ID in the OSPFv3 header is not the area ID configured on the ingress interface.

Field	Description
Invalid Destination Address	The number of OSPFv3 packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrRouters or AllSpfRouters multicast addresses.
No Neighbor at Source Address	The number of OSPFv3 packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
Invalid OSPF Packet Type	The number of OSPFv3 packets discarded because the packet type field in the OSPFv3 header is not a known type.
Hellos Ignored	The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.
Hellos Sent	The number of Hello packets sent on this interface by this router.
Hellos Received	The number of Hello packets received on this interface by this router.
DD Packets Sent	The number of Database Description packets sent on this interface by this router.
DD Packets Received	The number of Database Description packets received on this interface by this router.
LS Requests Sent	The number of LS Requests sent on this interface by this router.
LS Requests Received	The number of LS Requests received on this interface by this router.
LS Updates Sent	The number of LS updates sent on this interface by this router.
LS Updates Received	The number of LS updates received on this interface by this router.
LS Acknowledgements Sent	The number of LS acknowledgements sent on this interface by this router.
LS Acknowledgements Received	The number of LS acknowledgements received on this interface by this router.

OSPFv3 Neighbor Table

This screen displays the OSPFv3 neighbor table list. This information is displayed only if OSPFv3 is enabled, and there exists at least one OSPFv3-enabled interface having a valid neighbor.

- To display the OSPFv3 Neighbor Table page, click **Routing > OSPFv3 > Advanced > Neighbor Table**. The following page is displayed.

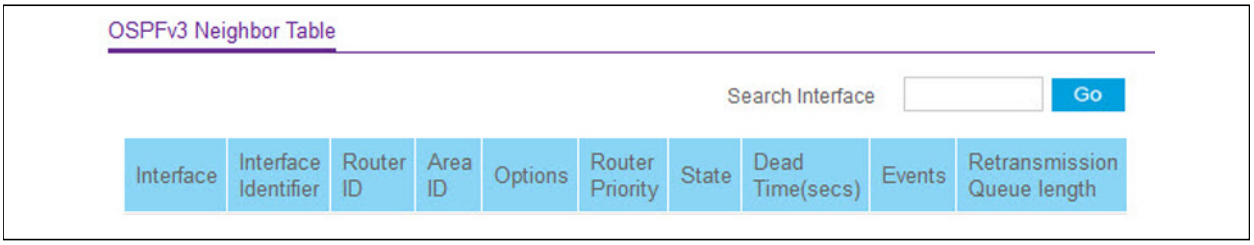


Table 117, Advanced OSPFv3 Neighbor Table on page 311 describes the non-configurable data that is displayed.

Table 117. Advanced OSPFv3 Neighbor Table

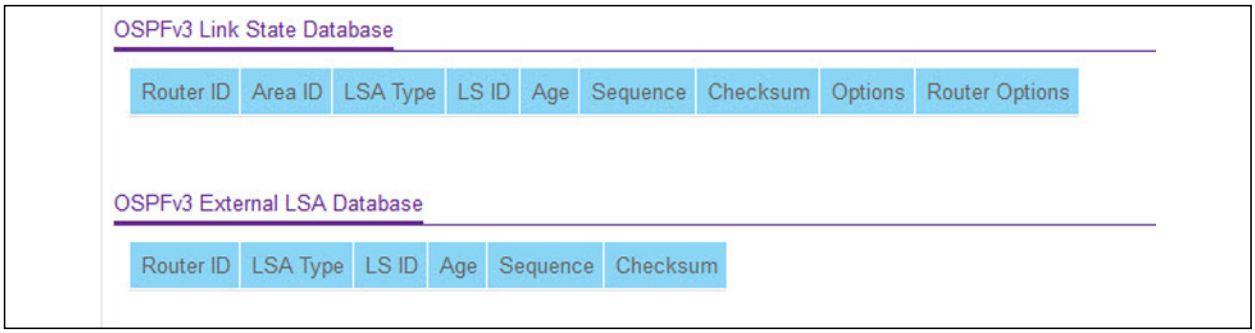
Field	Description
Interface	Displays the interface for which data is to be displayed or configured. Slot 0 is the base unit.
Interface Identifier	The interface ID that the neighbor advertises in its Hello packets on this link.
Router ID	A 32-bit integer in dotted decimal format representing the Router ID of the neighbor on the selected Interface.
Area ID	A 32-bit integer in dotted decimal format representing the area common to the neighbor selected.
Options	A Bit Mask corresponding to the neighbor's options field.
Router Priority	The priority of this neighbor in the designated router election algorithm. A value of 0 signifies that the neighbor is not eligible to become the designated router on this particular network.
State	The state of the relationship with this neighbor.
Dead Time	The amount of time, in seconds, since the last Hello was received from Adjacent Neighbors. Set to 0 for neighbors in a state less than or equal to Init.
Events	The number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	An integer representing the current length of the selected neighbor's retransmit queue.

- Click **Clear** to clear all the neighbors in the table.
- Click **Update** to update the page with the latest information on the switch.

OSPFv3 Link State Database

This screen displays the OSPFv3 Link State Database information.

- To display the OSPF Link State Database page, click **Routing > OSPFv3 > Advanced > Link State Database**. The following page is displayed.



OSPFv3 Link State Database

Table 118, Advanced OSPFv3 Link State Database on page 312 describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 118. Advanced OSPFv3 Link State Database

Field	Description
Router ID	The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the OSPFv3 Configuration page. If you want to change the Router ID you must first disable OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
Area ID	The ID of an OSPFv3 area to which one of the router interfaces is connected. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which an interface is connected.

Field	Description
LSA Type	The format and function of the link state advertisement. LSA Type is one of the following: • Router LSA—A router may originate one or more router-lsas for a given area. Each router-lsa originated in an area describes the collected states of all the router's interfaces to the area. • Network LSA—A network lsa is originated for every link having two or more attached routers, by the designated router. It lists all the routers attached to the link. • Inter-Area Router LSA—This type describes a prefix external to the area, yet internal to the autonomous system. It is originated by an Area Border Router. • AS-External LSA—This LSA type describes a path to a prefix external to the autonomous system and is originated by an Autonomous System Border Router. • Link LSA—A router originates a separate Link-lsa for each attached link. It provides router's link local address to routers attached to the link and also inform them of a list of IPv6 prefixes to associate with the link. • Intra-Area-Prefix LSA—A link's designated router originates one or more intra-area prefix lsas to advertise the link's prefixes throughout the area. A router may originate multiple intra-area-prefix lsas for a given area to advertise its own prefixes and those of its attached stub links.
LS ID	The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

Field	Description
Options	The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. The options are: • Q—This enables support for QoS Traffic Engineering. • E—This describes the way AS-external-LSAs are flooded. • MC—This describes the way IP multicast datagrams are forwarded according to the standard specifications. • O—This describes whether Opaque-LSAs are supported. • V—This describes whether OSPF++ extensions for VPN/COS are supported.
Router Options	The router-specific options.

OSPFv3 External LSA Database

Table 119, Advanced OSPFv3 External Link State Database Table describes the non-configurable data that is displayed in the External Link State Database (LSDB) table.

Click **Update** to update the page with the latest information on the switch.

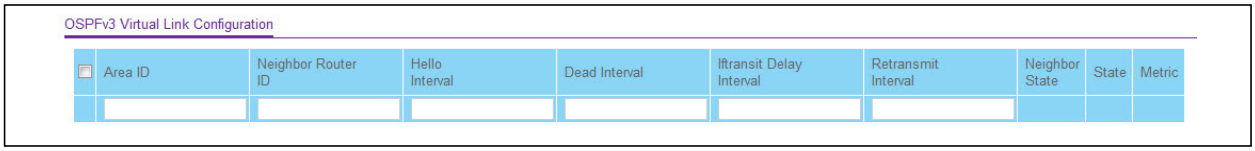
Table 119. Advanced OSPFv3 External Link State Database Table

Field	Description
Router ID	The 32-bit integer in dotted decimal format that uniquely identifies the router within the autonomous system (AS). The Router ID is set on the OSPFv3 Configuration page. If you want to change the Router ID you must first disable OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.
LSA Type	The format and function of the link state advertisement. LSA Type is one of the following: • Router LSA—A router may originate one or more router-lsas for a given area. Each router-lsa originated in an area describes the collected states of all the router's interfaces to the area. • Network LSA—A network lsa is originated for every link having two or more attached routers, by the designated router. It lists all the routers attached to the link. • Inter-Area Router LSA—This type describes a prefix external to the area, yet internal to the autonomous system. It is originated by an Area Border Router. • AS-External LSA—This LSA type describes a path to a prefix external to the autonomous system and is originated by an Autonomous System Border Router. • Link LSA—A router originates a separate Link-lsa for each attached link. It provides router's link local address to routers attached to the link and also inform them of a list of IPv6 prefixes to associate with the link. • Intra-Area-Prefix LSA—A link's designated router originates one or more intra-area prefix lsas to advertise the link's prefixes throughout the area. A router may originate multiple intra-area-prefix lsas for a given area to advertise its own prefixes and those of its attached stub links.
LS ID	The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.

Field	Description
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

OSPFv3 Virtual Link Configuration

- To display the OSPF Virtual Link Configuration page, click **Routing > OSPFv3 > Advanced > Virtual Link Configuration**. The following page is displayed.



- Configure the OSPFv3 Virtual Link.

1. Enter the **Area ID** of the OSPF area. An Area ID is a 32-bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.
2. Configure the **Neighbor Router ID** by entering the neighbor portion of a Virtual Link specification. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.
3. In the **Hello Interval** field, enter the OSPFv3 hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. Valid values range from 1 to 65,535. The default is 10 seconds.
4. In the **Dead Interval** field, enter the OSPFv3 dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value should a multiple of the Hello Interval (for example, 4). Valid values range from 1 to 65,535. The default is 40.
5. In the **Iftransit Delay Interval** field, enter the OSPFv3 Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. Valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.
6. In the **Retransmit Interval** field, enter the OSPFv3 retransmit interval for the specified interface. This is the number of seconds between link-state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link-state request packets. Valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.

7. Click **Add** to add a new virtual link to the switch.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. Click **Delete** to remove the specified virtual link from the switch configuration.

Table 120, Advanced OSPFv3 Virtual Link Configuration on page 318 describes the non-configurable data that is displayed.

Table 120. Advanced OSPFv3 Virtual Link Configuration

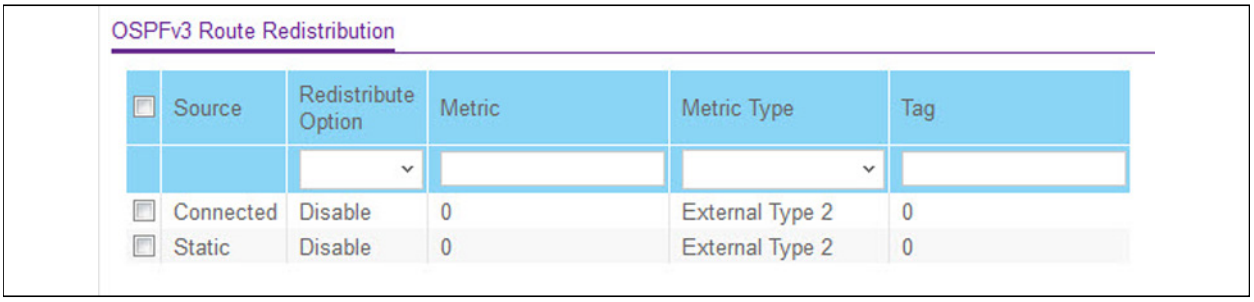
Field	Description
Neighbor State	The state of the Virtual Neighbor Relationship. The OSPFv3 interface state, it can be these values: • **Down**—This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface. • **Waiting**—The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router. • **Point-to-Point**—The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every Hello Interval seconds. • **Designated Router**—This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network. • **Backup Designated Router**—This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router. • **Other Designated Router**—The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.
State	Displays the State of the interface. It takes one the following values: • **Down**—This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable. In this state, interface parameters will be set to their initial values. All interface timers will be disabled, and there will be no adjacencies associated with the interface. • **Waiting**—The router is trying to determine the identity of the (Backup) Designated Router by monitoring received Hello Packets. The router is not allowed to elect a Backup Designated Router or a Designated Router until it transitions out of Waiting state. This prevents unnecessary changes of (Backup) Designated Router. • **Point-to-Point**—The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. Hello Packets are sent to the neighbor every HelloInterval seconds.

Field	Description
State (continued)	• **Designated Router**—This router is itself the Designated Router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA will contain links to all routers (including the Designated Router itself) attached to the network. • **Backup Designated Router**—This router is itself the Backup Designated Router on the attached network. It will be promoted to Designated Router if the present Designated Router fails. The router establishes adjacencies to all other routers attached to the network. The Backup Designated Router performs slightly different functions during the Flooding Procedure, as compared to the Designated Router. • **Other Designated Router**—The interface is connected to a broadcast or NBMA network on which other routers have been selected to be the Designated Router and Backup Designated Router either. The router attempts to form adjacencies to both the Designated Router and the Backup Designated Router.
Metric	The metric value used by the Virtual Link.

OSPFv3 Route Redistribution

Use this screen to configure the OSPFv3 Route Redistribution parameters. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

➢ To display the OSPFv3 Route Redistribution page, click **Routing > OSPFv3 > Advanced > Route Redistribution**. The following page is displayed.



➢ **Configure the OSPFv3 Route Redistribution.**

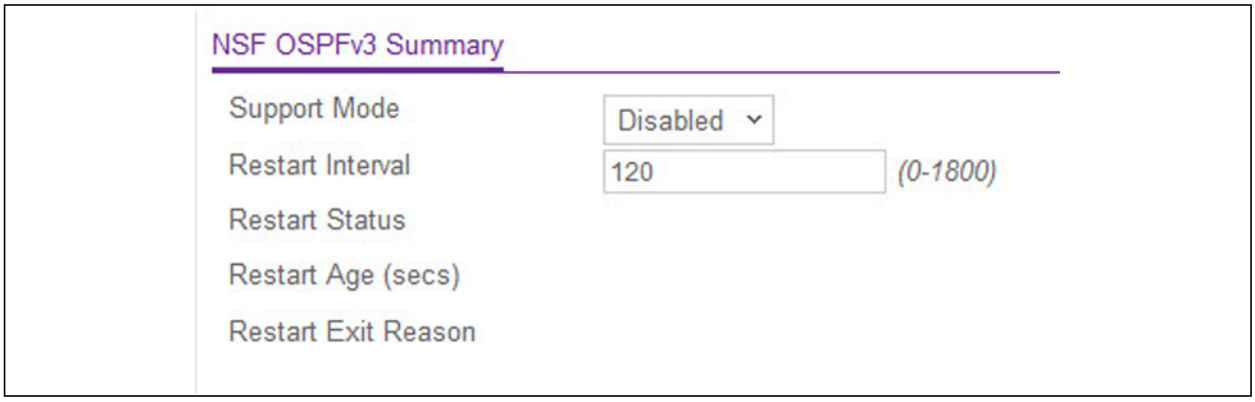
1. From the **Source** menu, select from the list of available source routes that have not previously been configured for redistribution by OSPFv3. The valid values are:
   - Connected
   - Static
2. In the **Redistribute Option** list, select to **Enable** or **Disable** the redistribution for the selected source protocol.
3. Set the **Metric** value to be used as the metric of redistributed routes. This fields displays the metric if the source was preconfigured, otherwise the tag is 0 and can be modified. Valid values are 0 to 16777214.

4. From the **Metric Type** list, select the OSPFv3 metric type of redistributed routes
5. Set the **Tag** field in routes redistributed. This field displays the tag if the source was preconfigured, otherwise the tag is 0 and can be modified. Valid values are 0 to 4294967295.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
8. Click **Update** to update the page with the latest information on the switch.

NSF OSPFv3 Summary

Use this screen to see the NSF OSPFv3 Summary. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

- To display the NSF OSPF Summary page, click **Routing > OSPFv3 > Advanced > NSF OSPFv3 Summary**. The following page is displayed.



- **Configure the NSF OSPFv3 Summary.**

1. From the **Support Mode** list, configure how the unit performs graceful restarts by selecting from the following possible values:
   - **Always**—Indicates that OSPF should perform a graceful restart for all planned and unplanned warm restart events.
   - **Disabled**—Disables OSPF from performing graceful restarts.
   - **Planned**—Indicates that OSPF should only perform a graceful restart when a restart is planned (for example, due to an **initiate failover** command).

   The default is **Disabled**.
2. Configure the **Restart Interval**. Valid values are 0 to 1800 in seconds. The default is 120 seconds.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Update** to update the page with the latest information on the switch.

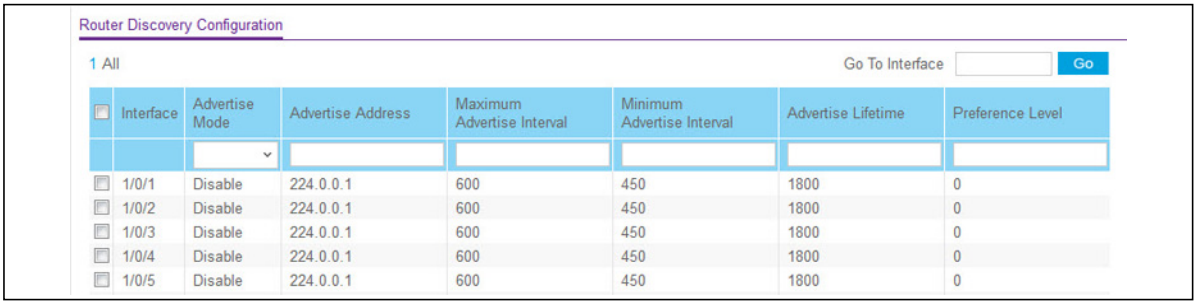
Table 121, Advanced NSF OSPFv3 Summary describes the non-configurable data that is displayed.

Table 121. Advanced NSF OSPFv3 Summary

Field	Description
Restart Status	Displays the restart status of OSPF Helper feature. The possible values are: • Not Restarting • Planned Restart • Unplanned Restart
Restart Age (seconds)	Displays the amount of time since the last restart occurred.
Restart Exit Reason	Displays how the master unit on the chassis last started up. The possible values are: • Not Attempted—Graceful restart has not been attempted. • In Progress—Restart is in progress. • Completed—The previous graceful restart completed successfully. • Timed Out—The previous graceful restart timed out. • Topology Changed—The previous graceful restart terminated prematurely because of a topology change.

Router Discovery

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



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 menu. If you select enable, Router Advertisements will be transmitted from the selected interface.
3. Use **Advertise Address** to select enable or disable from the menu. If you select enable, Router Advertisements will be transmitted from the selected interface.

4. Use **Maximum Advertise Interval** to enter the maximum time (in seconds) allowed between router advertisements sent from the interface.
5. Use **Minimum Advertise Interval** to enter the minimum time (in seconds) allowed between router advertisements sent from the interface. The value must be in the range of (3 to 1800). Default value is 450.000000.
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.

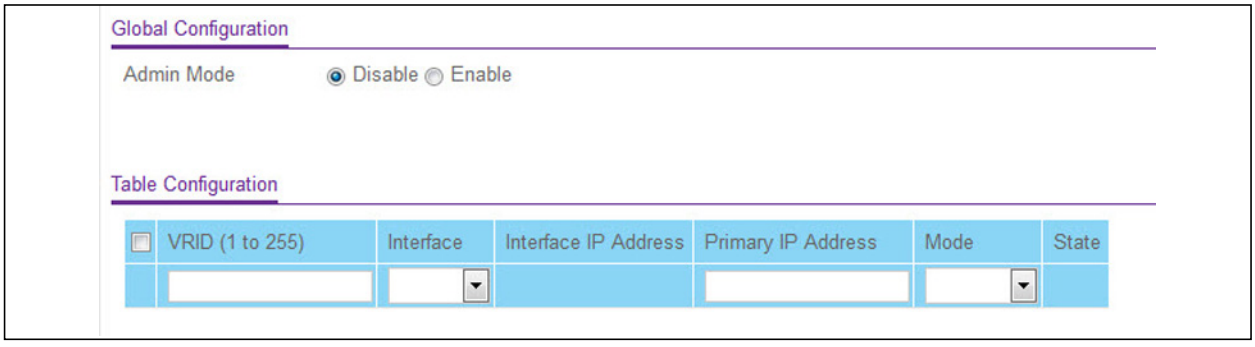
Virtual Router Redundancy Protocol

The **Routing > VRRP** tab contains links to the following web pages that you use to configure and display Virtual Router Redundancy Protocol (VRRP) data:

- *Basic VRRP Configuration* on page 322
- *Advanced VRRP Configuration* on page 323

Basic VRRP Configuration

➢ To display the Basic VRRP Configuration page, click **Routing > VRRP > Basic > VRRP Configuration**. The following page is displayed.



➢ Configure the global VRRP settings.

1. In the Global Configuration **Admin Mode** field, set the administrative status of VRRP in the router to either **Enable** or **Disable** option. By default, VRRP is disabled.
2. The **VRID** field is only configurable if you are creating a new virtual router. Enter the VRID. Valid values are 1 to 255.

3. Select the unit/slot/port for the new virtual router from the **Interface** list.
4. Enter the **Primary IP Address** of the Virtual Router.
5. From the **Mode** list, select **Active** or **Inactive** mode for the new virtual router.
6. Click **Add** to add a new virtual router to the switch configuration.
7. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
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 **Delete** to delete the selected virtual router.

Note: The router cannot be deleted if there are secondary addresses configured.

Table 122, VRRP Global Configuration describes the non-configurable data that is displayed.

Table 122. VRRP Global Configuration

Field	Description
Interface IP Address	Indicates the IP Address associated with the selected interface.
State	The current state of the Virtual Router. Possible values are: • Initialize • Master • Backup

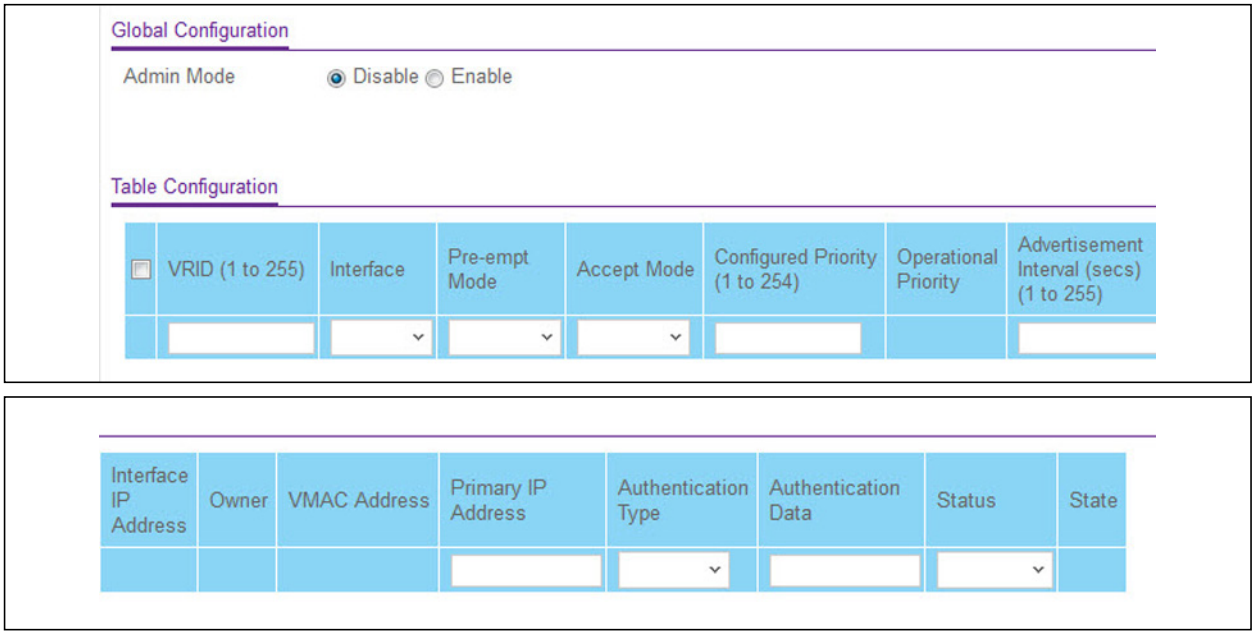
Advanced VRRP Configuration

.From the **Routing > VRRP > Advanced** link, you can access the following pages:

- *Advanced VRRP Configuration*
- *Advanced VRRP Secondary IP Address Configuration* on page 326
- *Advanced VRRP Tracking Interface Configuration* on page 327
- *Advanced VRRP Statistics* on page 329

Advanced VRRP Configuration

➢ To display the Advanced VRRP Configuration page, click **Routing > VRRP > Advanced > VRRP Configuration**. The following page is displayed.



➢ **Configure the Advanced VRRP Global Configuration settings.**

1. In the Global Configuration **Admin Mode** field, set the administrative status of VRRP in the router to either **Enable** or **Disable** option. By default, VRRP is disabled.
2. The **VRID** field is only configurable if you are creating a new virtual router. Enter the VRID. Valid values are 1 to 255.
3. Select the unit/slot/port for the new virtual router from the **Interface** list.
4. In the **Preempt Mode** field, select the **Enable** or **Disable** option. If you select enable, a backup router will preempt the master router if it has a priority greater than the master virtual router's priority, provided the master is not the owner of the virtual router IP address. The default is enable.
5. In the **Accept Mode** field, select the **Enable** or **Disable** option. If you select enable, the VRRP master will accept all types of data packets addressed to IP address(es) associated with the virtual router, and on selecting disable, the VRRP master will discard all types of data packets addressed to IP address(es) associated with the virtual router, if it is not the IP address owner. The default is disable.
6. Enter the **Configured Priority value** to be used by the VRRP router in the election for the master virtual router. Valid values are 1 to 254. If the Virtual IP Address is the same as the interface IP Address, the priority gets set to 254, no matter what the user enters.
7. In the **Advertisement Interval** field, enter the time, in seconds, between the transmission of advertisement packets by this virtual router. Enter a number from 1 to 255. The default value is 1 second.

8. Enter the **Primary IP Address**, the IP Address associated with the Virtual Router. The default is 0.0.0.0.
9. From the **Authentication Type** list, select the type of Authentication for the Virtual Router. The options are:
   - 0-None—No authentication will be performed. The default is None.
   - 1-Simple—Authentication will be performed using a text password.
10. If you selected simple authentication, enter the password in the **Authentication Data** field.
11. In the **Status** field, select the **Active** or **Inactive** option to start or stop the operation of the virtual router. The default is inactive.
12. Click **Add** to add a new virtual router to the switch configuration.
13. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
14. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
15. Click **Delete** to delete the selected virtual router.

Note: The router cannot be deleted if there are secondary addresses configured.

Table 123, Advanced VRRP Global Configuration describes the non-configurable data that is displayed.

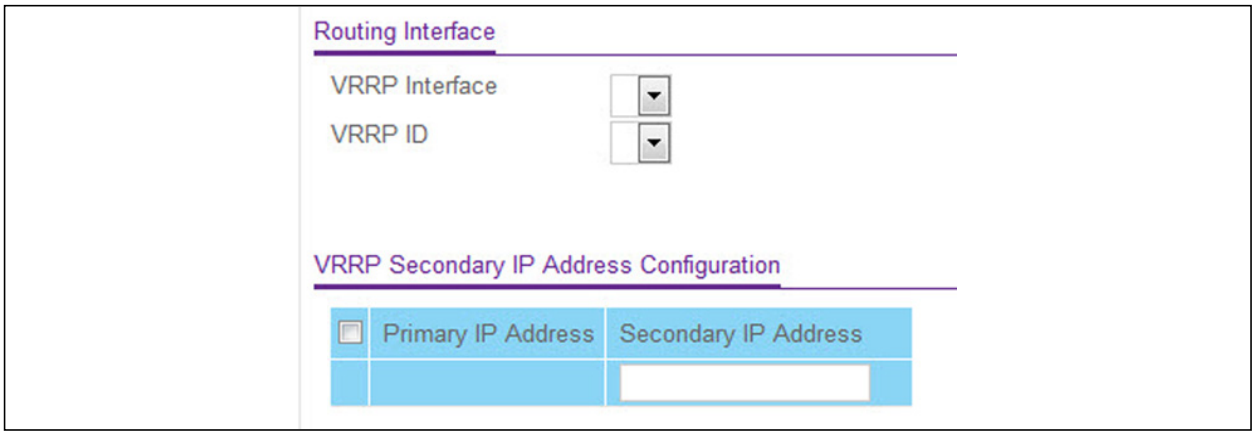
Table 123. Advanced VRRP Global Configuration

Field	Description
Operational Priority	Indicates the priority to be used for the virtual router master election process. Higher values imply higher priority. • A priority of 0 is sent by the master router to indicate that this router has ceased to participate in VRRP and a backup virtual router should transition to become a new master. • A priority of 255 is used for the router that owns the associated IP address(es).
Interface IP Address	Indicates the IP Address associated with the selected interface.
Owner	Set to **True** if the Virtual IP Address and the Interface IP Address are the same, otherwise set to **False**. If this parameter is set to True, the Virtual Router is the owner of the Virtual IP Address, and will always win an election for master router when it is active.

Field	Description
VMAC Address	The virtual MAC Address associated with the Virtual Router, composed of a 24-bit organizationally unique identifier, the 16-bit constant identifying the VRRP address block and the 8-bit VRID.
State	The current state of the Virtual Router. Possible values are: • Initialize • Master • Backup

Advanced VRRP Secondary IP Address Configuration

➢ To display the Advanced VRRP Secondary IP Address Configuration page, click **Routing > VRRP > Advanced > VRRP Secondary IP Address Configuration**. The following page is displayed.



➢ Configure the Advanced VRRP Secondary IP Address Configuration settings.

1. In the **VRRP Interface - VRRP ID** field, select one of the existing Virtual Routers, listed by interface number and VRRP ID.
2. In the **Secondary IP Address** field, enter the IP address for the interface. This address must be a member of one of the subnets currently configured on the interface. This value is read-only once configured.
3. Click **Add** to add a new secondary IP address to the selected VRRP interface.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Delete** to delete the selected secondary IP address interface.

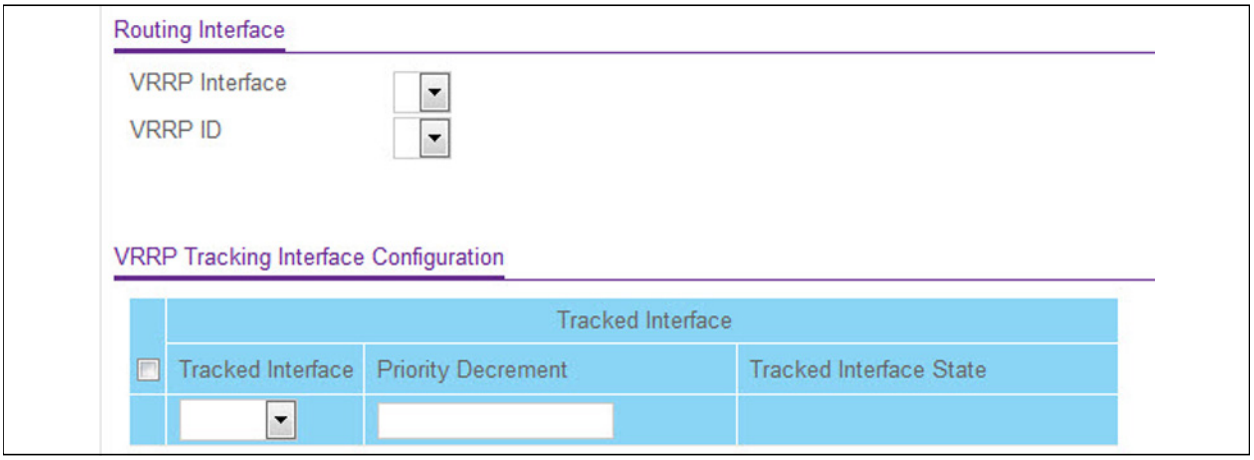
Table 124, Advanced VRRP Secondary IP Address Configuration describes the non-configurable data that is displayed.

Table 124. Advanced VRRP Secondary IP Address Configuration

Field	Description
Primary IP Address	The Primary IP Address of the Virtual Router.

Advanced VRRP Tracking Interface Configuration

- To display the Advanced VRRP Tracking Interface Configuration page, click **Routing > VRRP > Advanced > VRRP Tracking Configuration**. The following page is displayed.



- Configure the Advanced VRRP Tracking Interface Configuration settings.

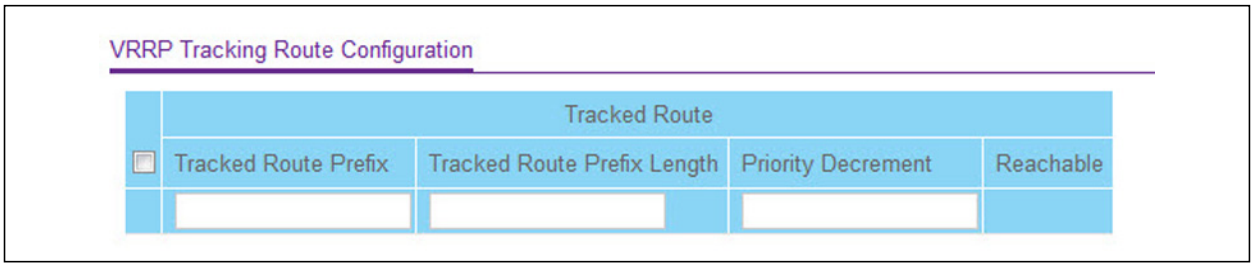
Routing Interface

1. In the **VRRP Interface - VRRP ID** field, select one of the existing Virtual Routers, listed by interface number and VRRP ID.

VRRP Tracking Interface Configuration

2. Select a routing interface from the **Tracked Interface** field, which lists all routing interfaces that are not yet tracked for this VRRP ID and interface configuration. The exceptions to this list are loopback and tunnels that could not be tracked.
3. Enter the **Priority Decrement** for the tracked interface. The valid range is 1 to 254. The default value is 10.
4. The non-configurable field, **Tracked Interface State**, displays the state of the tracked interface.

VRRP Tracking Route Configuration



5. In the **Tracked Route Prefix** field, enter the prefix of the route.
6. In the **Tracked Route Prefix Length** field, enter the prefix length of the route.
7. Enter the **Priority Decrement** for the route. The valid range is 1 to 254. The default value is 10.
8. The non-configurable **Reachable** field displays the reachability of the tracked route.
9. Click **Add** to add a new traced interface or tracked route to the VRRP.
10. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
11. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
12. Click **Delete** to delete the selected tracked interface or tracked route.

Table 125, Advanced VRRP Tracking Configuration describes the non-configurable data that is displayed.

Table 125. Advanced VRRP Tracking Configuration

Field	Description
Tracked Interface State	The state of the tracked interface.
Reachable	The reachability of the tracked route.

Advanced VRRP Statistics

➢ To display the Advanced VRRP Statistics page, click **Routing > VRRP > Advanced > VRRP Statistics**. The following page is displayed.

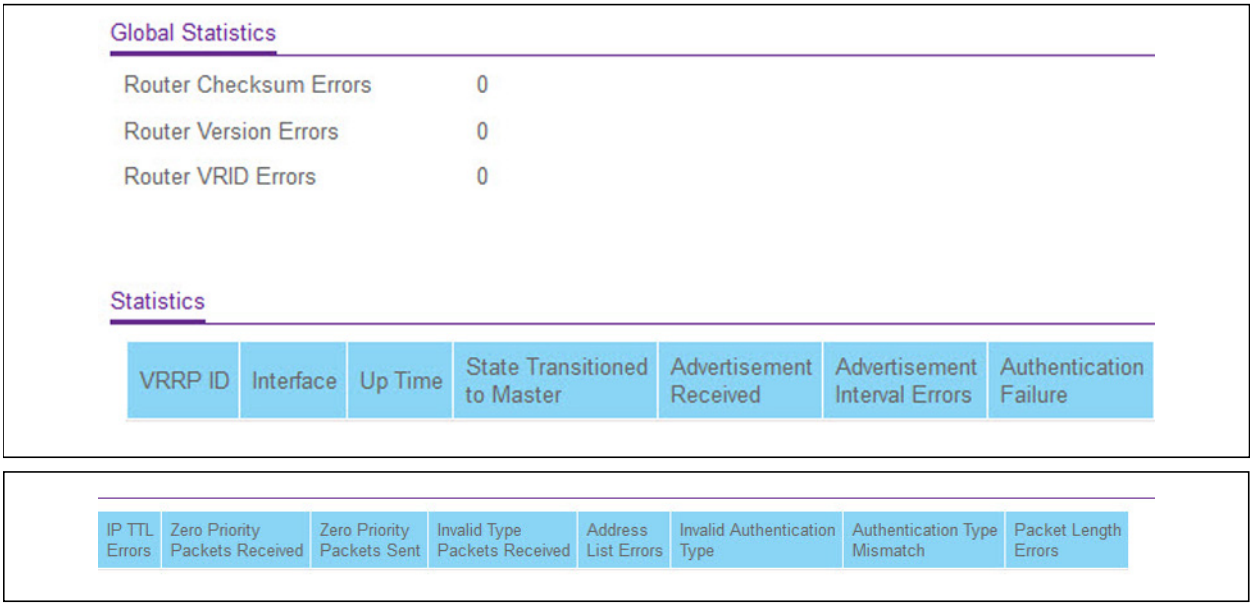


Table 126, Advanced VRRP Statistics describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 126. Advanced VRRP Statistics

Field	Description
Global Statistics	
Router Checksum Errors	The total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	The total number of VRRP packets received with an unknown or unsupported version number.
Router VRID Errors	The total number of VRRP packets received with an invalid VRID for this virtual router.
Statistics	
VRRP ID	The VRID for the selected Virtual Router.
Interface	The Unit/Slot/Port for the selected Virtual Router.
Up Time	The time, in days, hours, minutes and seconds, that has elapsed since the virtual router transitioned to the initialized state.

Field	Description
State Transitioned to Master	The total number of times that this virtual router's state has transitioned to Master.
Advertisement Received	The total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	The total number of VRRP advertisement packets received for which the advertisement interval was different than the one configured for the local virtual router.
Authentication Failure	The total number of VRRP packets received that did not pass the authentication check.
IP TTL Errors	The total number of VRRP packets received by the virtual router with IP Time-To-Live (TTL) not equal to 255.
Zero Priority Packets Received	The total number of VRRP packets received by the virtual router with a priority of 0.
Zero Priority Packets Sent	The total number of VRRP packets sent by the virtual router with a priority of 0.
Invalid Type Packets Received	The number of VRRP packets received by the virtual router with an invalid value in the Type field.
Address List Errors	The total number of packets received for which the address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	The total number of packets received with an unknown authentication type.
Authentication Type Mismatch	The total number of packets received with an authentication type different to the locally configured authentication method.
Packet Length Errors	The total number of packets received with a packet length less than the length of the VRRP header.

Multicast

The NETGEAR ProSafe Managed Multicast component is best suited for video and audio traffic requiring multicast packet control for optimal operation. The Multicast component includes support for IGMPv2 and IGMPv3. Communication from point to multipoint is called Multicasting. The source host (point) transmits a message to a group of zero or more hosts (multipoint) that are identified by a single IP destination address. Although the task may be accomplished by sending unicast (point-to-point) messages to each of the destination hosts, multicasting is the more desirable method for this type of transmission. A multicast message is delivered to all members of its destination host group with the same best-efforts reliability as regular unicast IP messages. The message is not guaranteed to arrive intact at all members of the destination group or in the same order relative to other messages.

The **Routing > Multicast** folder contains links to the following web pages that you use to configure and display Multicast data:

- *Multicast Mroute Table* on page 331

Multicast Mroute Table

➢ To display the Mroute Table page, click **Routing > Multicast > Mroute Table**. The following page is displayed.

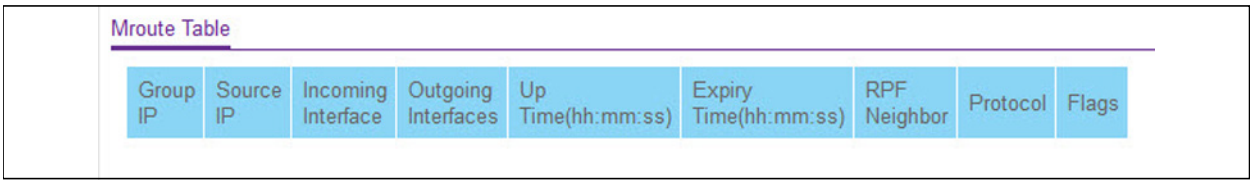


Table 127, Multicast Mroute Table describes the non-configurable data that is displayed. Click **Update** to update the page with the latest information on the switch.

Table 127. Multicast Mroute Table

Field	Description
Group IP	The destination group IP address.
Source IP	The IP address of the multicast packet source to be combined with the Group IP to fully identify a single route whose Mroute table entry.
Incoming Interface	The incoming interface on which multicast packets for this source/group arrive.
Outgoing Interfaces	The list of outgoing interfaces on which multicast packets for this source/group are forwarded.
Up Time (hh:mm:ss)	The time in seconds since the entry was created.
Expiry Time (hh:mm:ss)	The time in seconds before this entry will age out and be removed from the table.
RPF Neighbor	The IP address of the Reverse Path Forwarding (RPF) neighbor.

Field	Description
Protocol	The multicast routing protocol which created this entry. The possible values are: • **PIM-DM** • **PIM-SM** • **DVMRP**
Flags	The value displayed in this field is valid if the multicast routing protocol running is PIM-SM. The possible values are **RPT** or **SPT**. For other protocols a "------" is displayed.

Multicast Global Configuration

➢ To display the Multicast Global Configuration page, click **Routing > Multicast > Global Configuration**. The following page is displayed.

➢ **Configure Multicast Forwarding Globally**

1. In the **Admin Mode** field, select the **Enable** or **Disable** option to set the administrative status of Multicast Forwarding in the router. The default is **Disable**.
2. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 128, Multicast Global Configuration on page 332 describes the non-configurable data that is displayed.

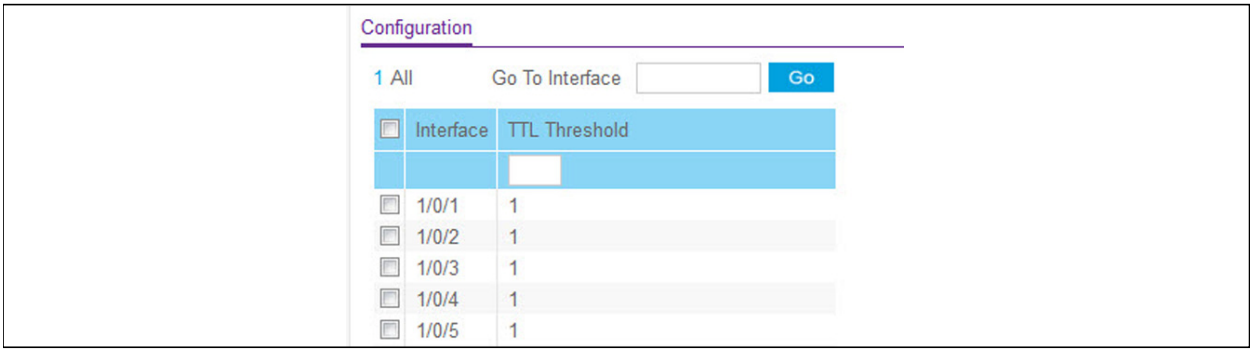
Table 128. Multicast Global Configuration

Field	Description
Protocol State	The operational state of the multicast forwarding module.
Table Maximum Entry Count	The maximum number of entries in the IP Multicast routing table.

Field	Description
Protocol	The multicast routing protocol presently activated on the router, if any.
Table Entry Count	The number of multicast route entries currently present in the Multicast route table.

Multicast Interface Configuration

- To display the Multicast Interface Configuration page, click **Routing > Multicast > Interface Configuration**. The following page is displayed.



- **Configure Multicast Interface**

1. In the **Go To Interface** field, enter the interface in unit/slot/port format and click on the **Go** button. The entry corresponding to the specified interface is selected.
2. Select the check box next to the routing interface for which data is to be displayed or configured.
3. Enter the **TTL Threshold** below which a multicast data packet will not be forwarded from the selected interface. Enter a number between 0 and 255. The default is **1**. If you enter **0**, all multicast packets for the selected interface will be forwarded. You must configure at least one router interface before you see this field.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Multicast DVMRP

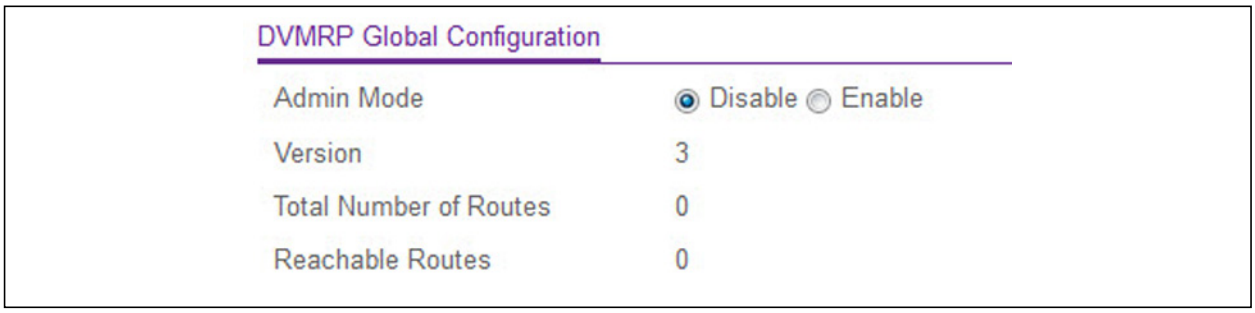
From the **Routing > Multicast > DVMRP** link, you can access the following pages:

- *DVMRP Global Configuration* on page 334
- *DVMRP Interface Configuration* on page 334
- *DVMRP Neighbor* on page 336
- *DVMRP Next Hop* on page 337
- *DVMRP Prune* on page 337

- *DVMRP Route* on page 338

DVMRP Global Configuration

To display the Multicast DVMRP Global Configuration page, click **Routing** > **Multicast**> **DVMRP** > **Global Configuration**. The following page is displayed.



➢ **DVMRP Global Configuration**

1. In the **Admin Mode** field, select the **Enable** or **Disable** option. This sets the administrative status of DVMRP to active or inactive. The default is disable.
2. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

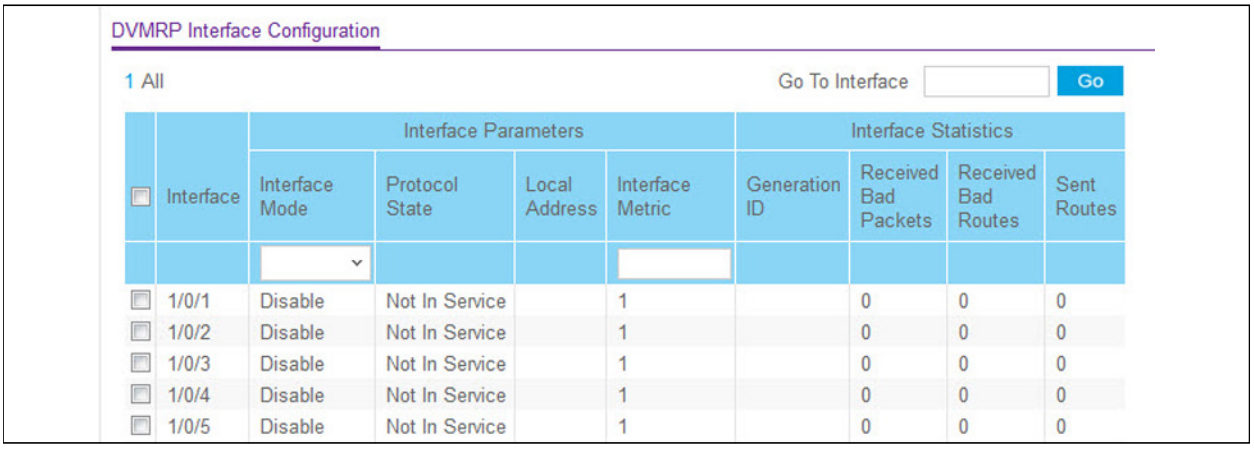
Table 129, DVMRP Global Configuration describes the non-configurable data that is displayed.

Table 129. DVMRP Global Configuration

Field	Description
Version	The current value of the DVMRP version string.
Total Number of Routes	The number of routes in the DVMRP routing table.
Reachable Routes	The number of routes in the DVMRP routing table that have a non-infinite metric.

DVMRP Interface Configuration

To display the Multicast DVMRP Interface Configuration page, click **Routing** > **Multicast**> **DVMRP** > **Interface Configuration**. The following page is displayed.



DVMRP Interface Configuration

1. In the **Go To Interface** field, enter the interface in unit/slot/port format and click **Go**. The entry corresponding to the specified interface is selected.
2. Select the check box next to the **Interface** for which data is to be displayed or configured.
3. In the **Interface Mode** field, select the **Enable** or **Disable** option to set the administrative mode of the selected DVMRP routing interface. The default is disable.
4. In the **Interface Metric** field, enter the DVMRP metric for the selected interface. This value is sent in DVMRP messages as the cost to reach this network. Valid values are 1 to 31. The default value is 1.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. Click **Update** to update the page with the latest information on the switch.

Table 130, DVMRP Interface Configuration describes the non-configurable data that is displayed.

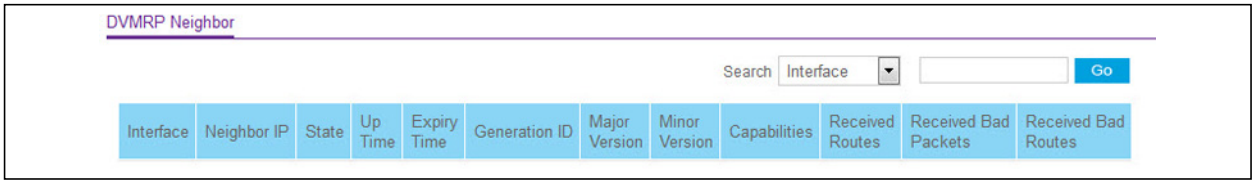
Table 130. DVMRP Interface Configuration

Field	Description
Protocol State	The operational state of the DVMRP protocol on the selected interface, either operational or non-operational.
Local Address	The IP address used as a source address in packets sent from the selected interface.
Generation ID	The DVMRP generation ID used by the router for the selected interface. This value is reset every time an interface is (re)started and is placed in prune messages. A change in generation ID informs the neighbor routers that any previous information about this router should be discarded.
Received Bad Packets	The number of invalid packets received on the selected interface.

Field	Description
Received Bad Routes	The number of invalid routes received on the selected interface.
Sent Routes	The number of routes sent on the selected interface.

DVMRP Neighbor

To display the Multicast DVMRP Neighbor page, click **Routing** > **Multicast**> **DVMRP** > **DVMRP Neighbor**. The following page is displayed.



DVMRP Neighbor Search

1. Use the **Search** menu to search for neighbor entries by MAC **Interface** or **Neighbor IP**.
   - Select **Search > Interface** from the list, enter the Interface in unit/slot/port format, for example 1/0/13, then click **Go**. If the neighbor entry exists, the entry is displayed as the first entry, followed by the remaining entries.
   - Select **Search** > **Neighbor IP** from the list, enter the neighbor IP, then click **Go**. If the entry with the matching Neighbor IP exists, that entry is displayed as the first entry, followed by the remaining entries. An exact match is required.
   - Click **Update** to update the page with the latest information on the switch.

Table 131, DVMRP Neighbor describes the non-configurable data that is displayed.

Table 131. DVMRP Neighbor

Field	Description
Interface	Select the interface for which data is to be displayed, or all the interface will be displayed.
Neighbor IP	The IP address of the neighbor whose information is displayed
State	The state of the specified neighbor router on the selected interface, either active or down.
Up Time	The DVMRP uptime for the specified neighbor on the selected interface. This is the time since the neighbor entry was learned.
Expiry Time	The DVMRP expiry time for the specified neighbor on the selected interface. This is the time left before this neighbor entry will age out, and is not applicable if the neighbor router's state is down.
Generation ID	The DVMRP generation ID for the specified neighbor on the selected interface.

Field	Description
Major Version	The DVMRP Major Version for the specified neighbor on the selected interface.
Minor Version	The DVMRP Minor Version for the specified neighbor on the selected interface.
Capabilities	The DVMRP capabilities of the specified neighbor on the selected interface.
Received Routes	The number of routes received for the specified neighbor on the selected interface.
Received Bad Packets	The number of invalid packets received for the specified neighbor on the selected interface.
Received Bad Routes	The number of invalid routes received for the specified neighbor on the selected interface.

DVMRP Next Hop

To display the Multicast DVMRP Next Hop page, click **Routing** > **Multicast** > **DVMRP** > **DVMRP Next Hop**. The following page is displayed.

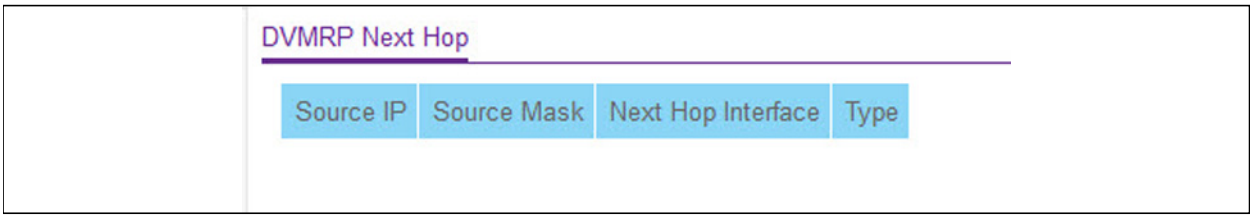


Table 132, DVMRP Next Hop on page 337 describes the non-configurable data that is displayed. Click **Update** to update the page with the latest information on the switch.

Table 132. DVMRP Next Hop

Field	Description
Source IP	The IP address used with the source mask to identify the source network for this table entry.
Source Mask	The network mask used with the source IP address.
Next Hop Interface	The outgoing interface for this next hop.
Type	The next hop type. **Leaf** means that no downstream dependent neighbors exist on the outgoing interface. Otherwise, the type is **branch**.

DVMRP Prune

To display the Multicast DVMRP Prune page, click **Routing** > **Multicast**> **DVMRP** > **DVMRP Prune**. The following page is displayed.

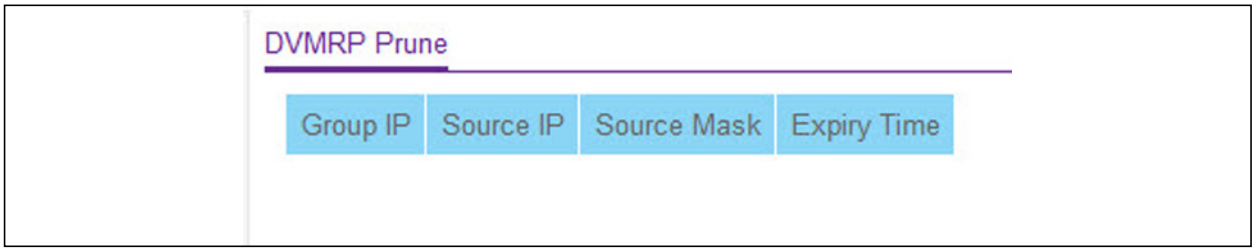


Table 133, DVMRP Prune describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 133. DVMRP Prune

Field	Description
Group IP	The group address which has been pruned.
Source IP	The IP address used with the source mask to identify the source network for this table entry.
Source Mask	The network mask used with the source IP address.
Expiry Time	The amount of time remaining before this prune should expire at the upstream neighbor. If no prune messages have been received from downstream neighbors, this is set to value of the default prune lifetime timer, otherwise it is set to the smallest received value or the default timer, whichever is less.

DVMRP Route

To display the Multicast DVMRP Route page, click **Routing** > **Multicast**> **DVMRP** > **DVMRP Route**. The following page is displayed.

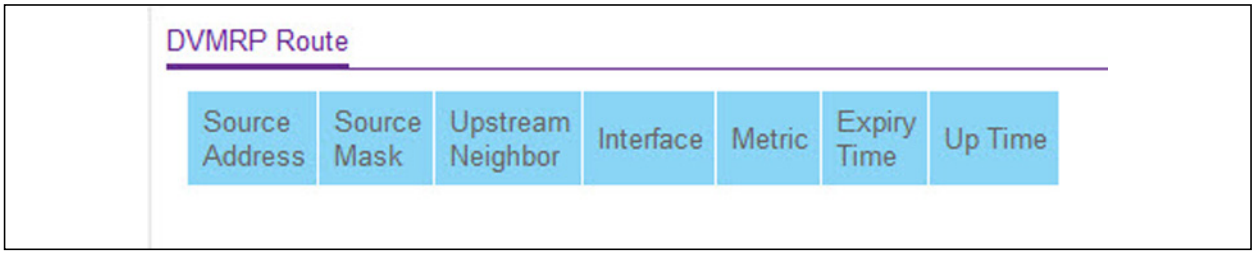


Table 134, DVMRP Route describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 134. DVMRP Route

Field	Description
Source Address	The network address that is combined with the source mask to identify the sources for this entry.
Source Mask	The network subnet mask used with the source IP address to identify the sources for this entry.
Upstream Neighbor	The address of the upstream neighbor (for example, RPF neighbor) from which IP datagrams from these sources are received.
Interface	The interface on which IP datagrams sent by these sources are received. A value of 0 typically means the route is an aggregate for which no next-hop interface exists.
Metric	The distance in hops to the source subnet.
Expiry Time	The amount of time remaining before this prune should expire at the upstream neighbor. If no prune messages have been received from downstream neighbors, this is set to value of the default prune lifetime timer, otherwise it is set to the smallest received value or the default timer, whichever is less.
Up Time	The time since the route represented by this entry was learned by the router.

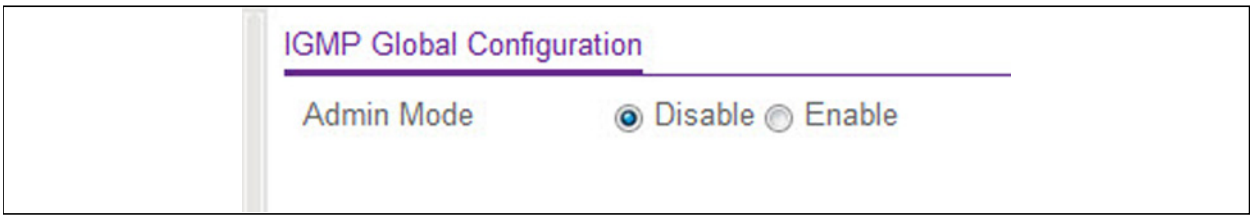
Multicast IGMP

From the **Routing > Multicast > IGMP** link, you can access the following pages:

- *IGMP Global Configuration*
- *IGMP Routing Interface Configuration* on page 340
- *IGMP Routing Interface Statistics* on page 341
- *IGMP Groups* on page 342
- *IGMP Membership* on page 343
- *IGMP Proxy Interface Configuration* on page 344
- *IGMP Proxy Interface Statistics* on page 345
- *IGMP Proxy Membership* on page 346

IGMP Global Configuration

To display the Multicast IGMP Global Configuration page, click **Routing** > **Multicast** > **IGMP** > **Global Configuration**. The following page is displayed.

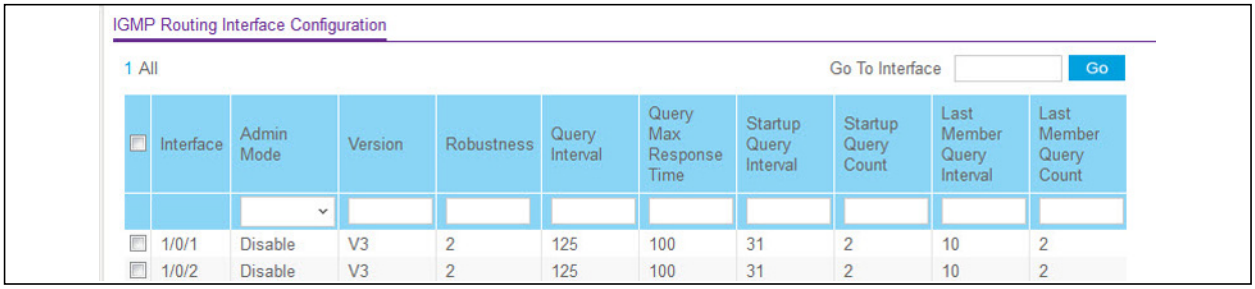


IGMP Global Configuration

1. In the **Admin Mode** field, select the **Enable** or **Disable** option. This sets the administrative status of IGMP in the router to active or inactive. The default is disable.
2. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IGMP Routing Interface Configuration

To display the Multicast IGMP Routing Interface Configuration page, click **Routing** > **Multicast** > **IGMP** > **Routing Interface Configuration**. The following page is displayed.



IGMP Routing Interface Configuration

1. In the **Go To Interface** field, enter the interface in unit/slot/port format and click **Go**. The entry corresponding to the specified interface is selected.
2. Select the check box beside the interface for which data is to be displayed or configured.
3. In the **Admin Mode** field, select the **Enable** or **Disable** option to set the administrative status of IGMP on the selected routing interface. The default is disable.
4. In the **Version** field, enter the version of IGMP you want to configure for the selected interface. Valid values are 1 to 3. The default value is 3. This field is configurable only when IGMP Interface mode is enabled.
5. In the **Robustness** field, enter the robustness value. This variable allows tuning for the expected packet loss on a subnet. If you expect the subnet to be lossy, you should enter a higher number for this parameter. IGMP is robust to (robustness variable-1) packet losses. Valid values are 1 to 255. The default value is 2.
6. In the **Query Interval** field, enter the frequency in seconds at which IGMP host-query packets are to be transmitted on this interface. Valid values are 1 to 3600. The default value is 125.
7. In the **Query Max Response Time** field, enter the maximum query response time, in tenths of a second, to be advertised in IGMPv2 queries on this interface. The default value is 100. Valid values are 0 to 255.
8. In the **Startup Query Interval** field, enter the number of seconds between the transmission of startup queries on the selected interface. Valid values are 1 to 300. The default value is 31.

9. In the **Startup Query Count** field, enter the number of queries to be sent on startup. The valid values are 1 to 20. The default value is 2.
10. In the **Last Member Query Interval** field, enter the last member query interval in tenths of a second. This is the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 255. The default value is 10. This value is not used for IGMP version 1.
11. In the **Last Member Query Count** field, enter the number of queries to be sent on receiving a leave group report. Valid values are from 1 to 20. The default value is 2.
12. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
13. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IGMP Routing Interface Statistics

To display the Multicast IGMP Routing Interface Statistics page, click **Routing** > **Multicast** > **IGMP** > **Routing Interface Statistics**. The following page is displayed.

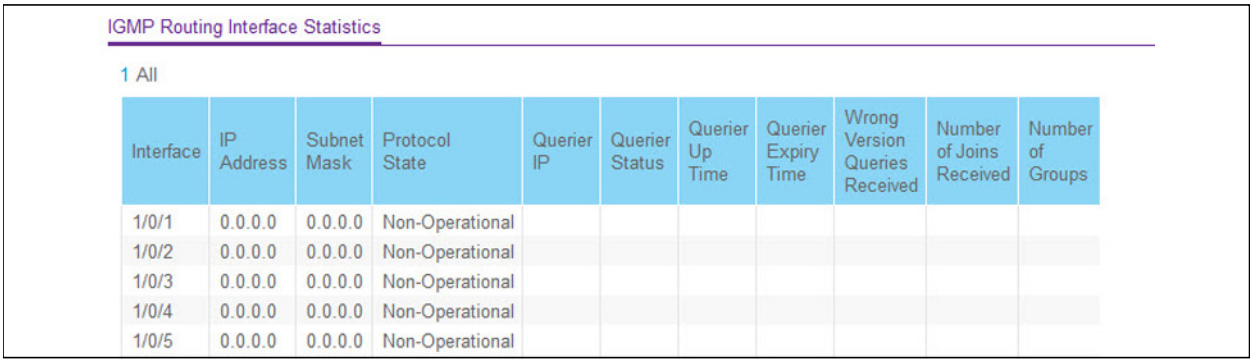


Table 135, Multicast IGMP Routing Interface Statistics describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

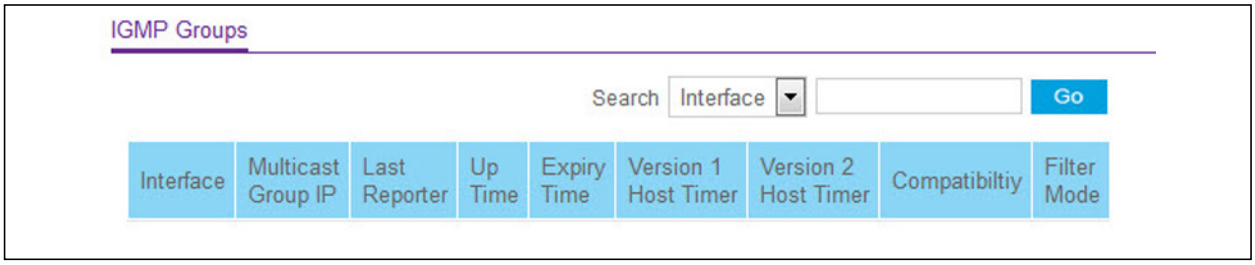
Table 135. Multicast IGMP Routing Interface Statistics

Field	Description
Interface	The interface on which the IGMP is enabled.
IP Address	The IP address of the selected interface.
Subnet Mask	The subnet mask for the IP address of the selected interface.
Protocol State	The operational state of IGMP on the selected interface, either operational or non-operational.
Querier IP	The address of the IGMP Querier on the IP subnet to which the selected interface is attached.

Field	Description
Querier Status	Indicates whether the selected interface is in Querier or non-querier mode.
Querier Up Time	The time in seconds since the IGMP interface Querier was last changed
Querier Expiry Time	The time in seconds remaining before the other Querier present timer expires. If the local system is the Querier, this will be zero.
Wrong Version Queries Received	The number of queries that have been received on the selected interface with an IGMP version that does not match the IGMP version configured for the interface, over the lifetime of the entry. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Therefore, a configuration error is indicated if any queries are received with the wrong version number.
Number of Joins Received	The number of times a group membership has been added on the selected interface; that is, the number of times an entry for this interface has been added to the cache table. This gives an indication of the amount of IGMP activity on the interface.
Number of Groups	The current number of entries for the selected interface in the cache table.

IGMP Groups

To display the Multicast IGMP Groups page, click **Routing** > **Multicast** > **IGMP** > **IGMP Groups**. The following page is displayed.



1. Use the **Search** menu to search for multicast entries by **Interface** or **Group**.
   - Select **Interface** from the **Search** list, enter the Interface in unit/slot/port format, for example 1/0/13, then click **Go**. If the entry exists, the entry is displayed as the first entry, followed by the remaining entries.
   - Select **Group** from the **Search** list, enter the Multicast Group IP, then click **Go**. If the entry exists, that entry with the matching Group is displayed as the first entry, followed by the remaining entries. An exact match is required.

Table 136, Multicast IGMP Groups on page 343 describes the non-configurable data that is displayed.

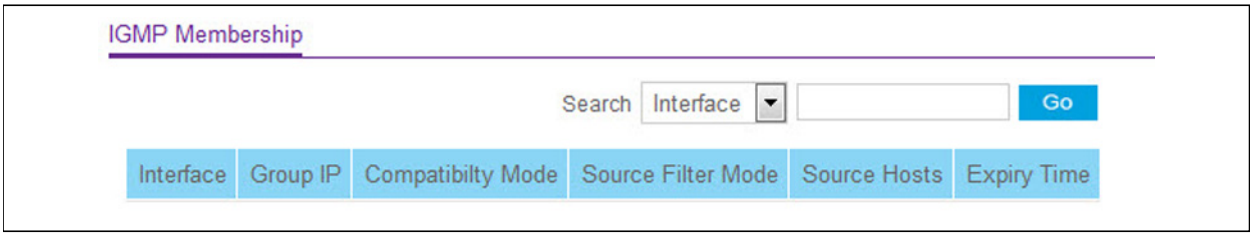
Click **Update** to update the page with the latest information on the switch.

Table 136. Multicast IGMP Groups

Field	Description
Interface	The interface for which data is to be displayed.
Multicast Group IP	The IP multicast group address for which data is to be displayed.
Last Reporter	The IP address of the source of the last membership report received for the IP Multicast group address on the selected interface.
Up Time	The time elapsed since this entry was created.
Expiry Time	The minimum amount of time remaining before this entry will be aged out.
Version 1 Host Timer	The time remaining until the local router will assume that there are no longer any IGMP version 1 members on the IP subnet attached to this interface. When an IGMPv1 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv2 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 1.
Version 2 Host Timer	The time remaining until the local router will assume that there are no longer any IGMP version 2 members on the IP subnet attached to this interface. When an IGMPv2 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv1 and IGMPv3 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 2.
Compatibility	This parameter shows group compatibility mode (v1, v2 and v3) for this group on the specified interface.
Filter Mode	The source filter mode (**Include**, **Exclude**, or **NA**) for the specified group on this interface. When NA mode is active, the field is blank

IGMP Membership

To display the Multicast IGMP Membership page, click **Routing** > **Multicast** > **IGMP** > **IGMP Membership**. The following page is displayed.



1. Use the **Search By** menu to search for multicast entries by **Interface** or **Group IP**.
   - Select **Interface** from the **Search** list, enter the Interface in unit/slot/port format, for example 1/0/13, then click **Go**. If the entry exists, the entry is displayed as the first entry, followed by the remaining entries.

- Select **Group IP** from the **Search** list, enter the Multicast Group IP, then click **Go**. If the entry exists, that entry with the matching Group IP is displayed as the first entry, followed by the remaining entries. An exact match is required.

Table 137, Multicast IGMP Membership describes the non-configurable data that is displayed.

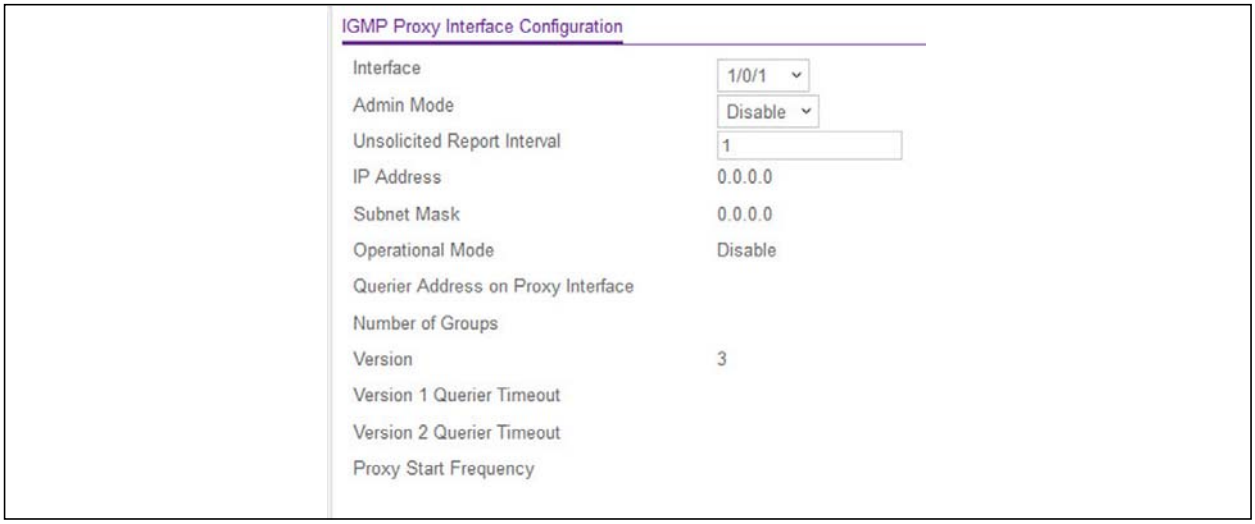
Click **Update** to update the page with the latest information on the switch.

Table 137. Multicast IGMP Membership

Field	Description
Interface	The interface on which multicast packets are forwarded.
Group IP	The IP multicast group address for which data is to be displayed.
Compatibility Mode	This parameter shows group compatibility mode (v1, v2 and v3) for this group on the specified interface.
Source Filter Mode	The source filter mode (**Include**, **Exclude**, or **NA**) for the specified group on this interface. When NA mode is active, the field is blank.
Source Hosts	This parameter shows source addresses which are members of this multicast address.
Expiry Time	This parameter shows expiry time interval against each source address which are members of this multicast group. This is the amount of time after which the specified source entry is aged out.

IGMP Proxy Interface Configuration

To display the Multicast IGMP Proxy Interface Configuration page, click **Routing** > **Multicast** > **IGMP** > **Proxy Interface Configuration**. The following page is displayed.



➢ **To configure the IGMP Proxy Interface**

1. Use the **Interface** list to select the port for which data is to be configured. You must have configured at least one router interface before configuring or displaying data for an IGMP Proxy interface, and it should not be an IGMP routing interface.
2. Select **Enable** or **Disable** from the Admin Mode list to set the administrative status of IGMP Proxy on the selected interface. The default is disable. Routing, IGMP and Multicast global admin modes should be enabled to enable IGMP Proxy interface mode.
3. In the **Unsolicited Report Interval** field, enter the unsolicited time interval value in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Valid values are from 1 to 260. The default value is 1.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 138, Multicast IGMP Proxy Interface Configuration describes the non-configurable data that is displayed.

Table 138. Multicast IGMP Proxy Interface Configuration

Field	Description
IP Address	The IP address of the IGMP Proxy interface.
Subnet Mask	The subnet mask for the IP address of the IGMP Proxy interface.
Operational Mode	The operational state of IGMP Proxy interface.
Querier Address on Proxy Interface	Specifies the Querier address on the proxy interface.
Number of Groups	The current number of multicast group entries for the IGMP Proxy interface in the cache table.
Version	Enter the version of IGMP you want to configure on the selected interface. Valid values are 1 to 3; the default value is 3. This field is configurable only when IGMP Proxy Interface mode is enabled.
Version 1 Querier Timeout	The older IGMP version 1 Querier timeout value in seconds. The Older Version Querier Interval is the time-out for transitioning a host back to IGMPv3 mode, once an older version query is heard. When an older version query is received, hosts set their Older Version Querier Present Timer to Older Version Querier Interval.
Version 2 Querier Timeout	The older IGMP version 2 Querier timeout value in seconds.
Proxy Start Frequency	The number of times the proxy was brought up.

IGMP Proxy Interface Statistics

To display the Multicast IGMP Proxy Interface Statistics page, click **Routing** > **Multicast** > **IGMP** > **Proxy Interface Statistics**. The following page is displayed.

Table 139, Multicast IGMP Proxy Interface Statistics describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 139. Multicast IGMP Proxy Interface Statistics

Field	Description
Proxy Interface	Displays the interface on which IGMP packets are received.
Version	The version of IGMP packets received.
Queries Received	The number of IGMP queries received.
Report Received	The number of IGMP reports received.
Reports Sent	The number of IGMP reports sent.
Leaves Received	The number of IGMP leaves received.
Leaves Sent	The number of IGMP leaves sent.

IGMP Proxy Membership

To display the Multicast IGMP Proxy Membership page, click **Routing** > **Multicast** > **IGMP** > **Proxy Membership**. The following page is displayed.

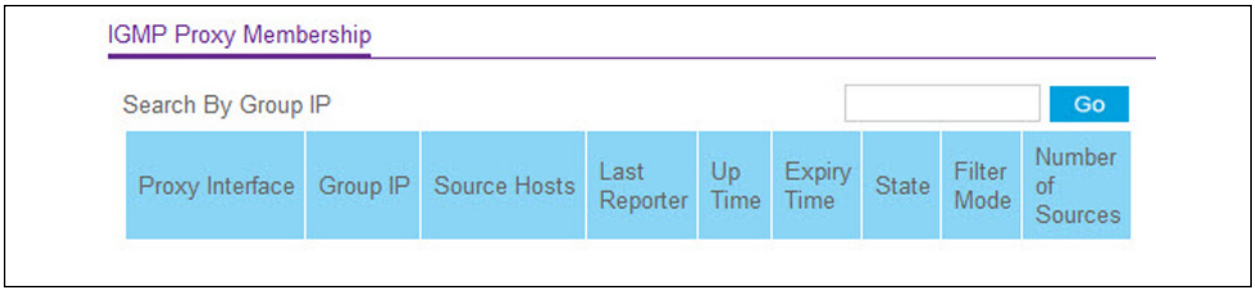


Table 140, Multicast IGMP Proxy Membership describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 140. Multicast IGMP Proxy Membership

Field	Description
Proxy Interface	Displays the interface on which IGMP proxy is enabled.
Group IP	Displays the IP multicast group address.
Source Hosts	This parameter shows source addresses which are members of this multicast address.
Last Reporter	The IP address of the source of the last membership report received for the IP Multicast group address on the IGMP Proxy interface.
Up Time	The time elapsed since this entry was created.
Expiry Time	This parameter shows expiry time interval against each source address which is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.
State	The state of the host entry. A Host can be in one of the state. Non-member state - does not belong to the group on the interface. Delaying member state - host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. Idle member state - host belongs to the group on the interface and no report timer running.
Filter Mode	The group filter mode (Include/Exclude/None) for the specified group on the IGMP Proxy interface.
Number of Sources	The number of source hosts present in the selected multicast group.

Multicast PIM

Protocol-Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable interdomain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol.

From the **Routing > Multicast > PIM** link, you can access the following pages:

- *PIM Global Configuration* on page 347
- *PIM SSM Configuration* on page 348
- *PIM Interface Configuration* on page 349
- *PIM Neighbor* on page 350
- *PIM Candidate Rendezvous Point Configuration* on page 350
- *PIM Bootstrap Router Candidate Configuration* on page 351
- *PIM Static Rendezvous Point Configuration* on page 352

PIM Global Configuration

To display the Multicast PIM Global Configuration page, click **Routing** > **Multicast** > **PIM** > **Global Configuration**. The following page is displayed.

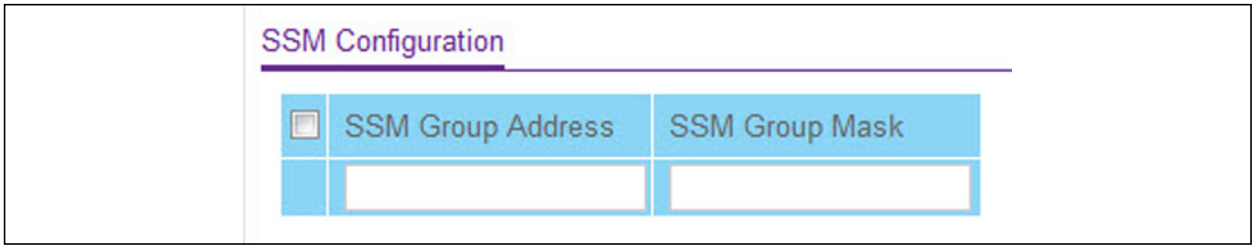
- **PIM Global Configuration**

1. In the **Admin Mode** field, select the protocol of PIM in the router. Possible values are **Disable**, **PIM-SM**, or **PIM-DM**. The default is **Disable**.
2. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

PIM SSM Configuration

While PIM employs a specially-configured Rendezvous Point (RP) router that serves as a meeting junction for multicast senders and listeners, Protocol-Independent Multicast Single-Source Multicast (PIM-SSM) does not use an RP. It supports only source route delivery trees. It is used between routers so that they can track which multicast packets to forward to each other and to their directly-connected LANs. The SSM service model can be implemented with a strict subset of the PIM protocol mechanisms. Both regular IP Multicast and SSM semantics can coexist on a single router, and both can be implemented using the PIM protocol. A range of multicast addresses, currently 232.0.0.0/8 in IPv4 and FF3x::/32 in IPv6, is reserved for SSM.

To display the Multicast PIM SSM Configuration page, click **Routing** > **Multicast** > **PIM** > **SSM Configuration**. The following page is displayed.

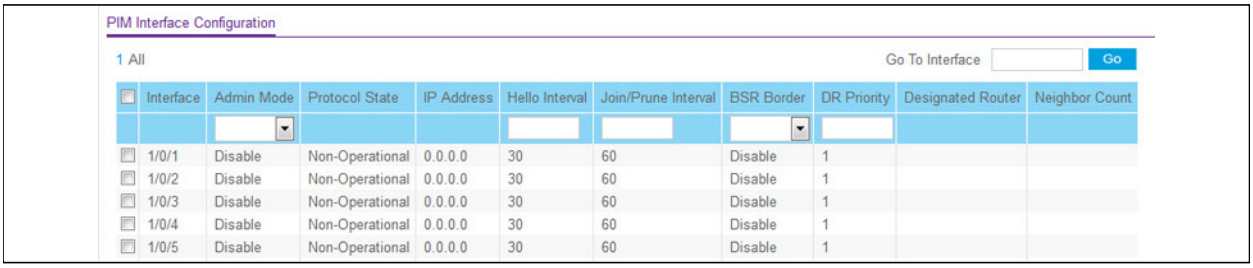


- **PIM SSM Configuration**

1. In the **SSM Group Address** field, enter the source-specific multicast group ip-address.
2. In the **SSM Group Mask** field, enter the source-specific multicast group ip-address mask.
3. Click **Add** to add a new source-specific 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.
5. Click **Delete** to delete an existing source-specific group.

PIM Interface Configuration

To display the Multicast PIM Interface Configuration page, click **Routing** > **Multicast** > **PIM** > **Interface Configuration**. The following page is displayed.



PIM Interface Configuration

1. Select the check box beside the interface for which data is to be configured or displayed.
2. In the **Admin Mode** field, select the **Enable** or **Disable** option to set the administrative status of PIM in the router. The default is disable.
3. In the **Hello Interval** field, enter the time in seconds between the transmission of PIM Hello messages on this interface. The valid values are from 0 to 18000. The default value is 30.
4. In the **Join/Prune Interval**, enter the time in seconds at which PIM Join/Prune messages are transmitted on this PIM interface. The valid values are from 0 to 18000. The default value is 60.
5. In the **BSR Border** field, select the **Enable** or **Disable** option to set the Bootstrap Router (BSR) border status on the selected interface.
6. Enter the **DR Priority** for the selected interface. The valid values are from 0 to 2147483647. The default value is 1.
7. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
8. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 141, Multicast PIM Interface Configuration on page 349 describes the non-configurable data that is displayed.

Table 141. Multicast PIM Interface Configuration

Field	Description
Protocol State	The state of PIM in the router—either operational or non-operational.
IP Address	The IP address of the selected PIM interface. If you enter an IPv6 address, the format is Prefix/Prefix Length.
Designated Router	The Designated Router on the selected PIM interface.
Neighbor Count	The number of PIM neighbors on the selected interface.

PIM Neighbor

To display the Multicast PIM Neighbor page, click **Routing** > **Multicast** > **PIM** > **PIM Neighbor**. The following page is displayed.

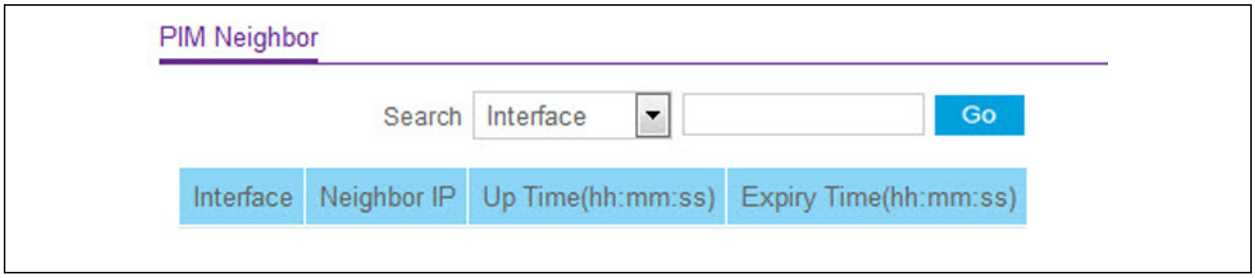


Table 142, Multicast PIM Neighbor describes the non-configurable data that is displayed.

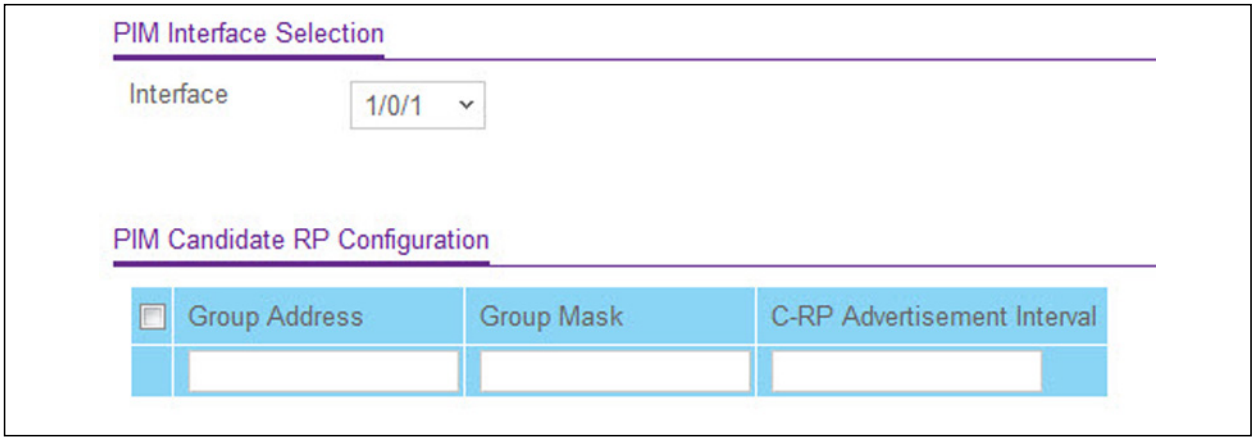
Click **Update** to update the page with the latest information on the switch.

Table 142. Multicast PIM Neighbor

Field	Description
Interface	The interface on which neighbor is displayed.
Neighbor IP	The IP address of the PIM neighbor for this entry.
Up Time (hh:mm:ss)	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time (hh:mm:ss)	The minimum time remaining before this PIM neighbor will be aged out.

PIM Candidate Rendezvous Point Configuration

To display the Multicast PIM Candidate Rendezvous Point (RP) Configuration page, click **Routing** > **Multicast** > **PIM** > **Candidate RP Configuration**. The following page is displayed.

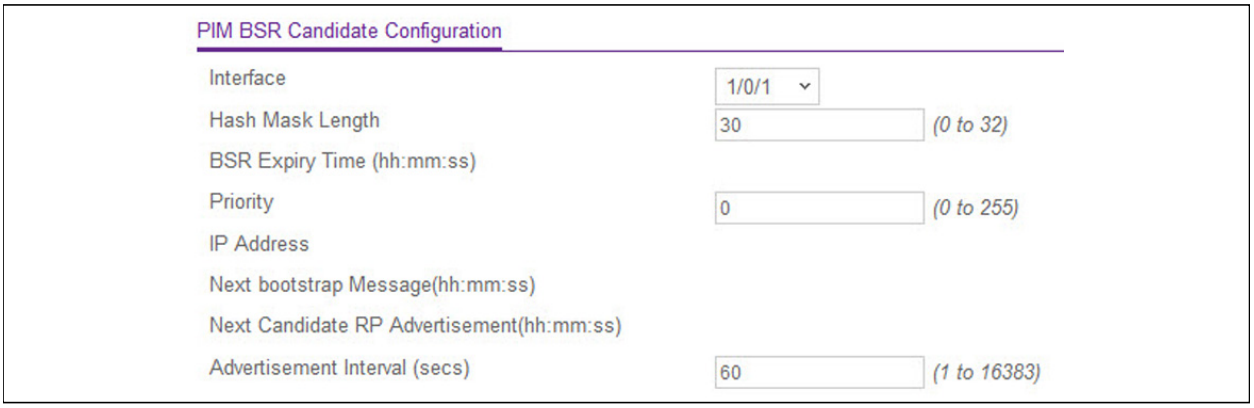


PIM Candidate RP Configuration

1. From the list of interfaces, select the **Interface** for which data is to be configured or displayed.
2. Enter the **Group Address** transmitted in Candidate-RP-Advertisements. If you enter an IPv6 address, the format is Prefix/Prefix Length.
3. In the **Group Mask** field, enter the group address mask transmitted in Candidate-RP-Advertisements
4. In the **C-RP Advertisement Interval**, specify the duration in seconds at which the C-RP messages are unicast to the Bootstrap Router (BSR). The range is from 1 to 16383 seconds. The default value is 60 seconds. If this field is submitted without any value, the default value is used.
5. Click **Add** to add a new Candidate-RP Address for the PIM router.
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 **Delete** to delete an existing Candidate-RP Address for the PIM router.

PIM Bootstrap Router Candidate Configuration

To display the Multicast PIM Bootstrap Router (BSR) Candidate Configuration page, click **Routing** > **Multicast** > **PIM** > **BSR Candidate Configuration**. The following page is displayed.



PIM BSR Candidate Configuration

1. From the list of interfaces, select the **Interface** for which data is to be configured or displayed.
2. Enter the C-BSR **Hash Mask Length** to be advertised in bootstrap messages. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid values are from 0 to 32. Default value is 30.
3. In the **Priority** field, enter the priority of C-BSR.
4. Enter the **Advertisement Interval** value of the C-BSR in seconds. The default value is 60.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Delete** to remove the configured Hash Mask Length, and Priority values and restore them to the default values.

7. Click **Update** to update the page with the latest information on the switch.

Table 143, Multicast BSR Candidate Configuration describes the non-configurable data that is displayed.

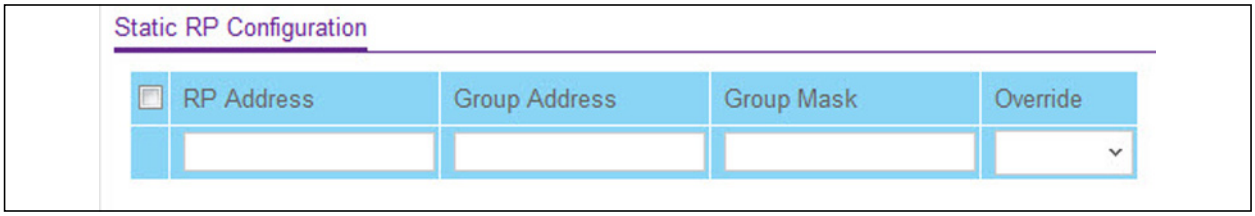
Table 143. Multicast BSR Candidate Configuration

Field	Description
BSR Expiry Time (hh:mm:ss)	Time (in hours, minutes and seconds) in which the learned elected bootstrap router (BSR) expires.
IP Address	Displays the IP address of the Elected BSR.
Next bootstrap Message (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP Advertisement (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

PIM Static Rendezvous Point Configuration

Use this page to statically configure the Rendezvous Point (RP) address for one or more multicast groups.

To display the Multicast PIM Static RP Configuration page, click **Routing** > **Multicast** > **PIM** > **Static RP Configuration**. The following page is displayed.

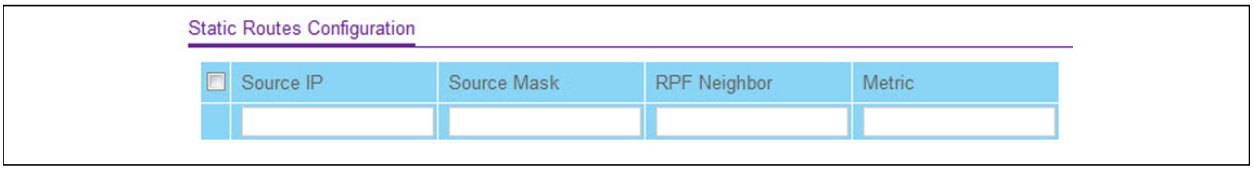


➢ **PIM Static RP Configuration**

1. In the **RP Address** field, enter the IP address for one or more multicast groups.
2. Enter the **Group Address** of the RP to be created or deleted.
3. Enter the **Group Mask** of the RP to be created or deleted.
4. In the **Override** field, select the **Enable** or **Disable** option. **Enable** indicates that, if there is a conflict, the RP configured with this option prevails over the RP learned by BSR.
5. Click **Add** to add a new static RP address for one or more multicast groups.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
8. Click **Delete** to remove the selected RP address.

Multicast Static Routes Configuration

To display the Multicast Static Routes Configuration page, click **Routing** > **Multicast** > **Static Routes Configuration**. The following page is displayed.



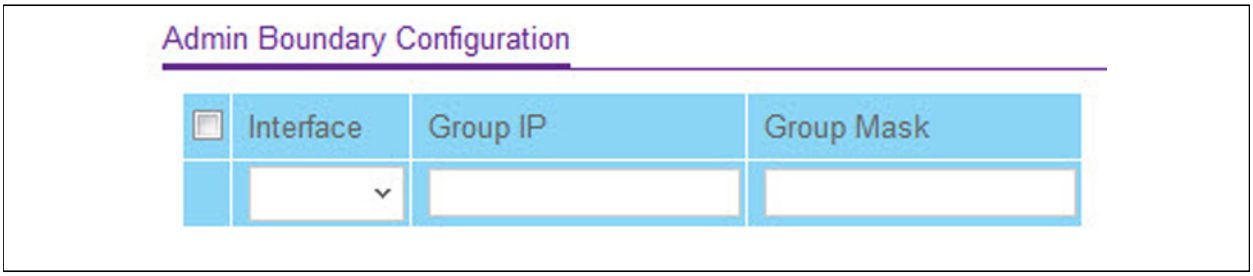
- **Static Routes Configuration**

1. In the **Source IP** field, enter the IP address that identifies the multicast packet source for the entry you are creating.
2. In the **Source Mask** field, enter the subnet mask to be applied to the Source IP address.
3. In **RPF Neighbor** field, enter the IP address of the neighbor router on the path to the source.
4. In the **Metric** field, enter the link state cost of the path to the multicast source. The range is 0 to 255, the default is 1. You can change the metric for a configured route by selecting the static route and editing this field.
5. Click **Add** to add a new static route to the switch.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
8. Click **Delete** to delete the selected multicast static route.

Multicast Admin Boundary Configuration

The definition of an administratively-scoped boundary is a mechanism to stop the ingress and egress of multicast traffic for a given range of multicast addresses on a given routing interface.

To display the Multicast Admin Boundary Configuration page, click **Routing** > **Multicast** > **Admin Boundary Configuration**. The following page is displayed.



➢ **Admin Boundary Configuration**

1. In the **Interface** list, select the router interface for which the administratively-scoped boundary is to be configured.
2. In the **Group IP** field, enter the multicast group address for the start of the range of addresses to be excluded. The address must be in the range of 239.0.0.0 through 239.255.255.255.
3. In the **Group Mask** field, enter the mask to be applied to the multicast group address. The combination of the mask and the Group IP gives the range of administratively-scoped addresses for the selected interface.
4. Click **Add** to add a new administratively-scoped boundary.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Delete** to delete the selected administratively-scoped boundary.

IPv6 Multicast

The **Routing > IPv6 Multicast** folder contains links to the following web pages that you use to configure and display IPv6 Multicast data:

- *IPv6 Multicast Mroute Table* on page 354
- *IPv6 Multicast PIM* on page 355
- *IPv6 Multicast MLD* on page 361
- *IPv6 Multicast Static Routes Configuration* on page 369

IPv6 Multicast Mroute Table

This screen displays the contents of the Mroute Table in tabular format.

➢ To display the Mroute Table page, click **Routing > IPv6 Multicast > Mroute Table**. The following page is displayed.

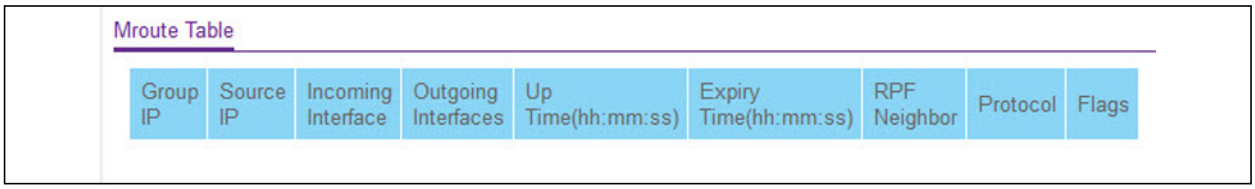


Table 127, Multicast Mroute Table describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 144. Multicast Mroute Table

Field	Description
Group IP	The destination group IP address.
Source IP	The IP address of the multicast packet source to be combined with the Group IP to fully identify a single route whose Mroute table entry.
Incoming Interface	The incoming interface on which multicast packets for this source/group arrive.
Outgoing Interfaces	The list of outgoing interfaces on which multicast packets for this source/group are forwarded.
Up Time (hh:mm:ss)	The time in seconds since the entry was created.
Expiry Time (hh:mm:ss)	The time in seconds before this entry will age out and be removed from the table.
RPF Neighbor	The IP address of the Reverse Path Forwarding (RPF) neighbor.
Protocol	The multicast routing protocol which created this entry. The possible values are: • **PIM-DM** • **PIM-SM**
Flags	The value displayed in this field is valid if the multicast routing protocol running is PIM-SM. The possible values are **RPT** or **SPT**. For other protocols a – (dash) is displayed.

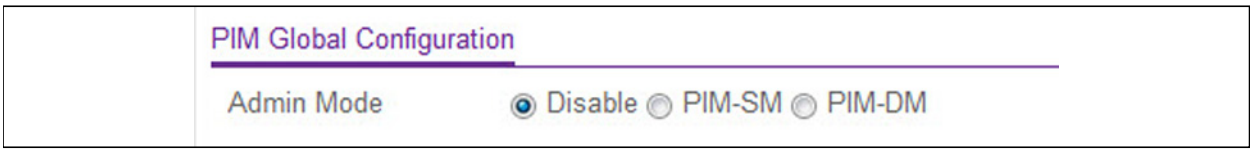
IPv6 Multicast PIM

From the **IPv6 Multicast > IPv6 PIM** link, you can access the following pages:

- *IPv6 PIM Global Configuration*
- *IPv6 PIM SSM Configuration* on page 356
- *IPv6 PIM Interface Configuration* on page 356
- *IPv6 PIM Neighbor* on page 358
- *IPv6 PIM Candidate Rendezvous Point Configuration* on page 358
- *IPv6 PIM Bootstrap Router Candidate Configuration* on page 359
- *IPv6 PIM Static Rendezvous Point Configuration* on page 360

IPv6 PIM Global Configuration

To display the IPv6 PIM Global Configuration page, click **Routing** > **IPv6 Multicast** > **IPv6 PIM** > **Global Configuration**. The following page is displayed.



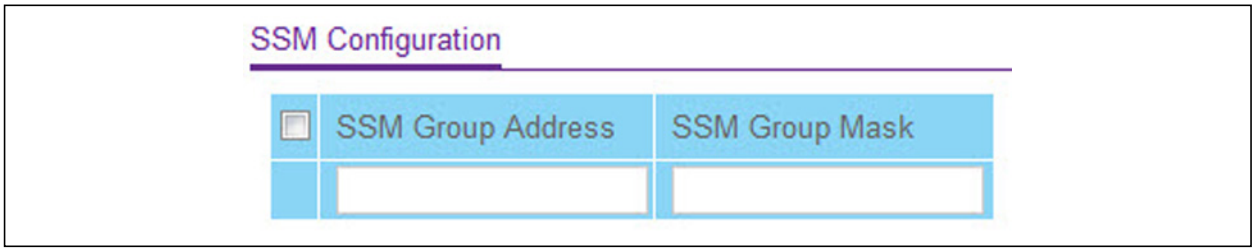
- **IPv6 PIM Global Configuration**

1. In the **Admin Mode** field, select the **Disable** option, or the protocol variant of PIM option, either Dense Mode (**PIM-DM**) or Sparse Mode (**PIM-SM**), to be enabled. By default, PIM Global Configuration Admin Mode is disabled. The **Disable** option sets the administrative status of PM in the router to active or inactive.
2. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IPv6 PIM SSM Configuration

While PIM employs a specially-configured Rendezvous Point (RP) router that serves as a meeting junction for multicast senders and listeners, Protocol-Independent Multicast Single-Source Multicast (PIM-SSM) does not use an RP. It supports only source route delivery trees. It is used between routers so that they can track which multicast packets to forward to each other and to their directly-connected LANs. The SSM service model can be implemented with a strict subset of the PIM protocol mechanisms. Both regular IP Multicast and SSM semantics can coexist on a single router, and both can be implemented using the PIM protocol. A range of multicast addresses, currently 232.0.0.0/8 in IPv4 and FF3x::/32 in IPv6, is reserved for SSM.

To display the IPv6 PIM SSM Configuration page, click **Routing** > **IPv6 Multicast** > **IPv6 PIM** > **SSM Configuration**. The following page is displayed.

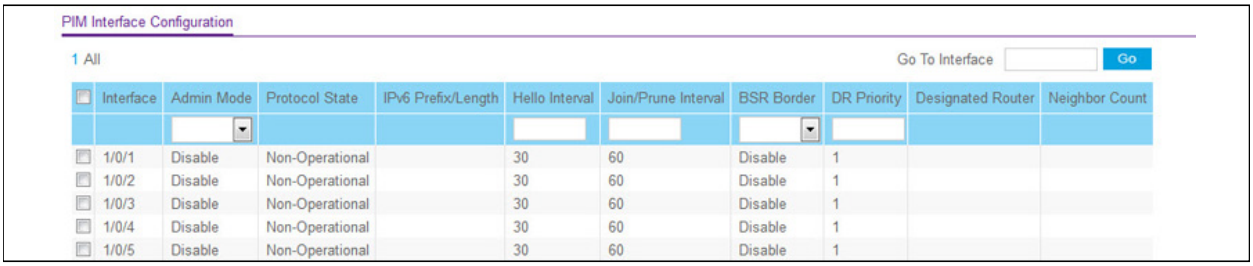


- **IPv6 PIM SSM Configuration**

1. In the **SSM Group Address** field, enter the source-specific multicast group ip-address.
2. In the **SSM Group Mask** field, enter the source-specific multicast group ip-address mask.
3. Click **Add** to add a new source-specific 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.
5. Click **Delete** to delete an existing source-specific group.

IPv6 PIM Interface Configuration

To display the IPv6 PIM Interface Configuration page, click **Routing** > **IPv6 Multicast** > **IPv6 PIM** > **Interface Configuration**. The following page is displayed.



IPv6 PIM Interface Configuration

1. In the **Go To Interface** field, enter the interface in unit/slot/port format and click on the **Go** button. The entry corresponding to the specified interface will be selected.
2. Select the check box beside the **Interface** for which data is to be configured or displayed.
3. In the **Admin Mode** field, select the **Enable** or **Disable** option to set the administrative status of PIM-SM in the router. The default is Disable.
4. In the **Hello Interval** field, enter the time in seconds between the transmission of PIM Hello messages on this interface. The valid values are from 0 to 18000. The default value is 30.
5. In the **Join/Prune Interval**, enter the frequency at which PIM Join/Prune messages are transmitted on this PIM interface. The valid values are from 0 to 18000. The default value is 60.
6. In the **BSR Border** field, select the **Enable** or **Disable** option to set the Bootstrap Router (BSR) border status on the selected interface.
7. Enter the **DR Priority** for the selected interface. The valid values are from 0 to 2147483647. The default value is 1.
8. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 145, IPv6 PIM Interface Configuration describes the non-configurable data that is displayed.

Table 145. IPv6 PIM Interface Configuration

Field	Description
Protocol State	The state of PIM in the router—either operational or non-operational.
IPv6 Prefix/Length	The IPv6 Address Prefix and the Length of the selected interface.
Designated Router	The Designated Router on the selected PIM interface.
Neighbor Count	The number of PIM neighbors on the selected interface.

IPv6 PIM Neighbor

To display the IPv6 PIM Neighbor page, click **Routing** > **IPv6 Multicast** > **IPv6 PIM** > **PIM Neighbor**. The following page is displayed.

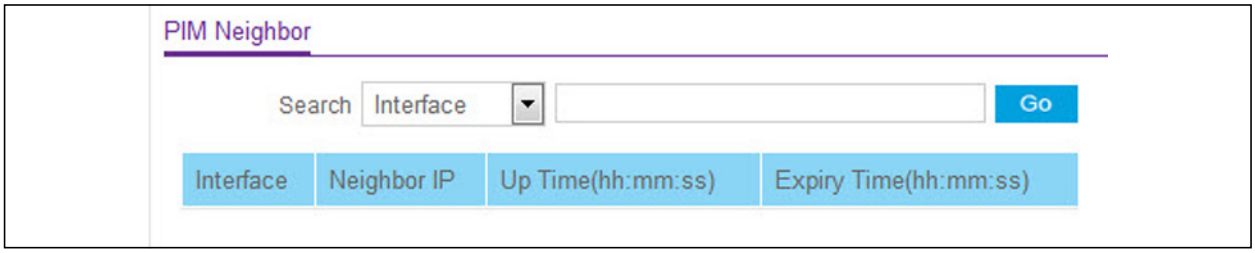


Table 146, IPv6 PIM Neighbor describes the non-configurable data that is displayed.

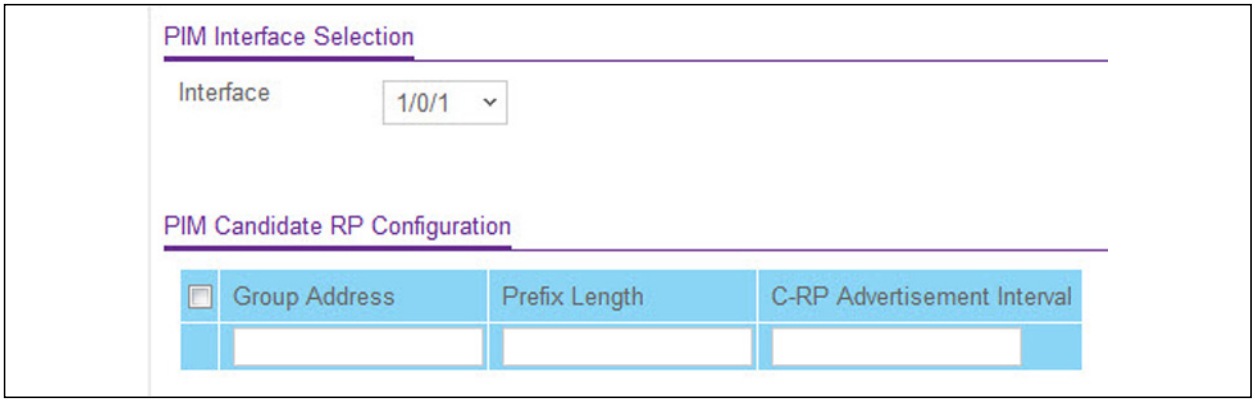
Click **Update** to update the page with the latest information on the switch.

Table 146. IPv6 PIM Neighbor

Field	Description
Interface	The interface on which neighbor is displayed.
Neighbor IP	The IP address of the PIM neighbor for this entry.
Up Time (hh:mm:ss)	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time (hh:mm:ss)	The minimum time remaining before this PIM neighbor will be aged out.

IPv6 PIM Candidate Rendezvous Point Configuration

To display the IPv6 PIM Candidate Rendezvous Point (RP) Configuration page, click **Routing** > **IPv6 Multicast** > **IPv6 PIM** > **Candidate RP Configuration**. The following page is displayed.



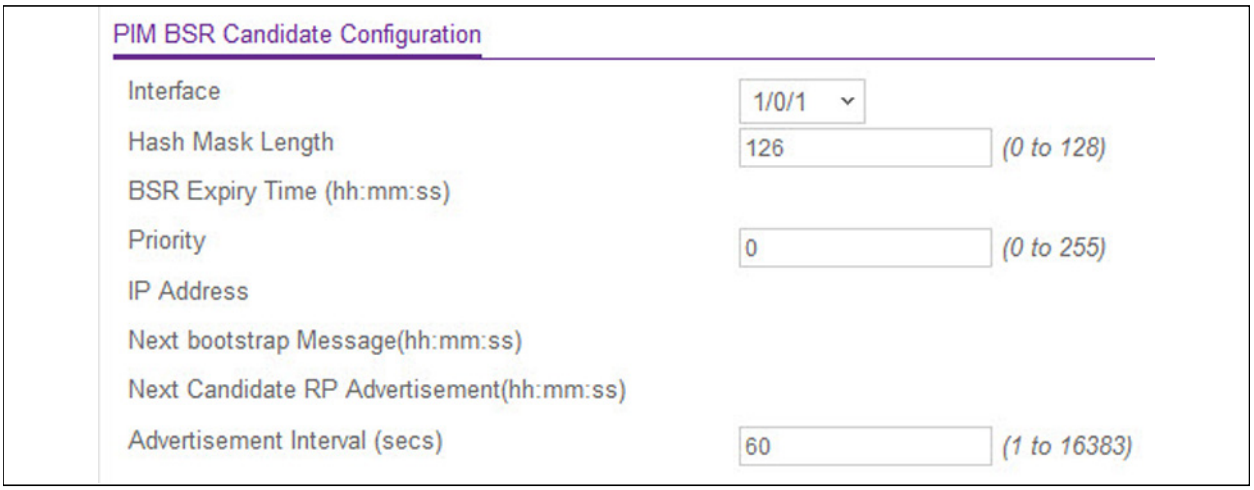
➢ **IPv6 PIM Candidate RP Configuration**

1. From the list of interfaces, select the **Interface** for which data is to be configured or displayed.

2. In the **Group Address** field, enter the group IPv6 address prefix transmitted in Candidate-RP-Advertisements.
3. In the **Prefix Length** field, enter the group IPv6 Prefix Length transmitted in Candidate-RP-Advertisements
4. In the **C-RP Advertisement Interval**, specify the duration in seconds at which the C-RP messages are unicast to the Bootstrap Router (BSR). The range is from 1 to 16383 seconds. The default value is 60 seconds. If this field is submitted without any value, the default value is used.
5. Click **Add** to add a new Candidate-RP Address for the PIM router.
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 **Delete** to delete an existing Candidate-RP Address for the PIM router.

IPv6 PIM Bootstrap Router Candidate Configuration

To display the IPv6 PIM Bootstrap Router (BSR) Candidate Configuration page, click **Routing** > **IPv6 Multicast** > **IPv6 PIM** > **BSR Candidate Configuration**. The following page is displayed.



- **IPv6 PIM BSR Candidate Configuration**

1. From the list of interfaces, select the **Interface** for which data is to be configured or displayed.
2. Enter the C-BSR **Hash Mask Length** to be advertised in bootstrap messages. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid values are from 0 to 128. Default value is 126.
3. In the **Priority** field, enter the priority of C-BSR.
4. Enter the **Advertisement Interval** value of the C-BSR in seconds. The default value is 60.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Delete** to remove the configured Hash Mask Length, and Priority values and restore them to the default values.

7. Click **Update** to update the page with the latest information on the switch.

Table 147, IPv6 PIM BSR Candidate Configuration describes the non-configurable data that is displayed.

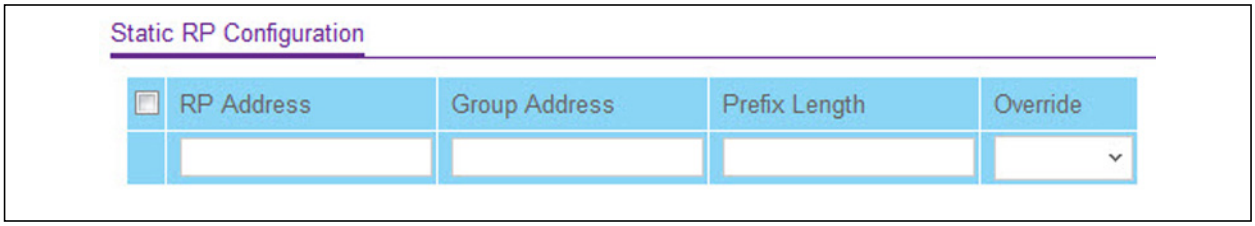
Table 147. IPv6 PIM BSR Candidate Configuration

Field	Description
BSR Expiry Time (hh:mm:ss)	Time (in hours, minutes and seconds) in which the learned elected bootstrap router (BSR) expires.
IP Address	Displays the IP address of the Elected BSR.
Next bootstrap Message (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP Advertisement (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

IPv6 PIM Static Rendezvous Point Configuration

Use this page to statically configure the Rendezvous Point (RP) address for one or more multicast groups.

To display the IPv6 PIM Static RP Configuration page, click **Routing** > **IPv6 Multicast** > **IPv6 PIM** > **Static RP Configuration**. The following page is displayed.



- **IPv6 PIM Static RP Configuration**

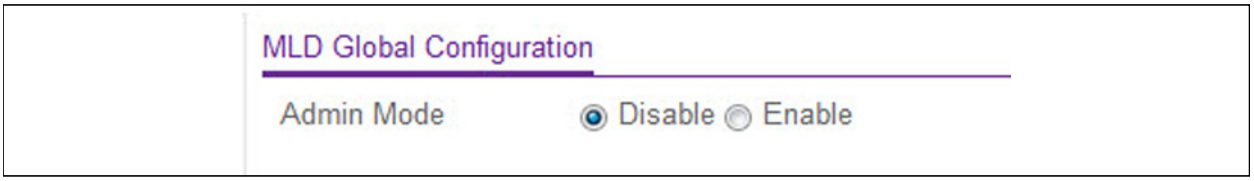
1. In the **RP Address** field, enter the IP address of the RP to be created or deleted.
2. Enter the **Group Address** of the RP to be created or deleted.
3. Enter the **Group Mask** of the RP to be created or deleted.
4. In the **Override** field, select the **Enable** or **Disable** option. **Enable** indicates that, if there is a conflict, the RP configured with this option prevails over the RP learned by BSR.
5. Click **Add** to add a new static RP address for one or more multicast groups.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
8. Click **Delete** to remove the selected RP address.

IPv6 Multicast MLD

From the **Routing > IPv6 Multicast > MLD** link, you can access the following pages:

IPv6 MLD Global Configuration

To display the IPv6 PIM Global Configuration page, click **Routing** > **IPv6 Multicast** > **MLD** > **Global Configuration**. The following page is displayed.

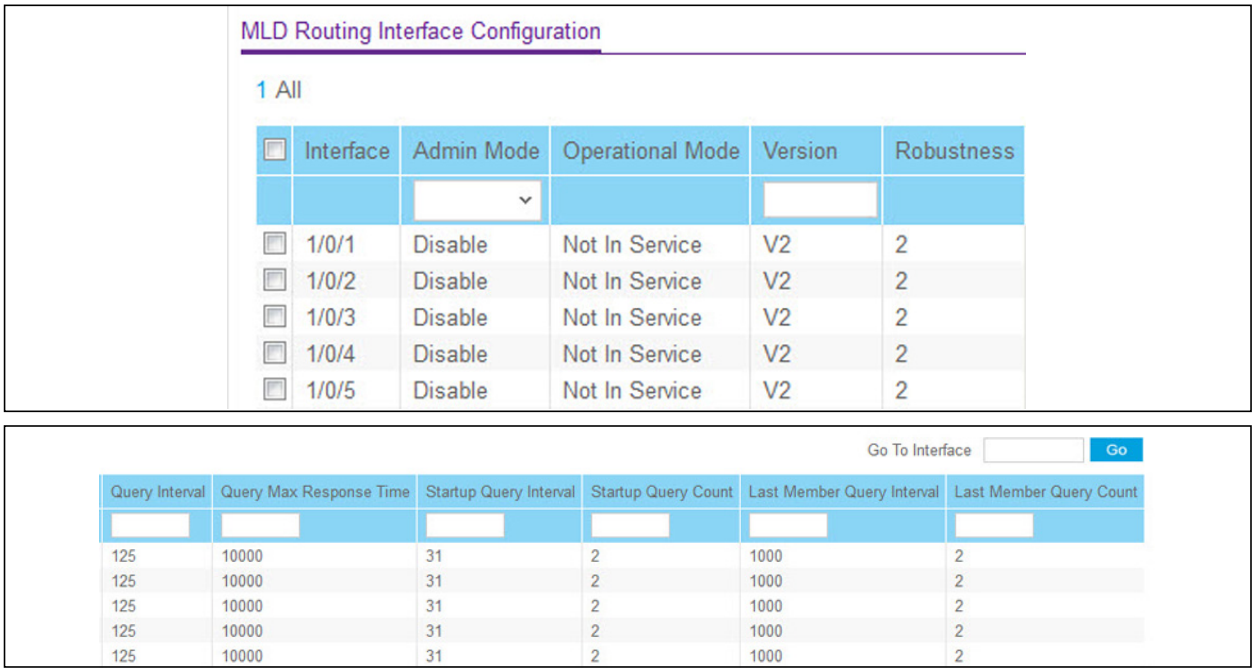


➢ **IPv6 MLD Global Configuration**

1. In the **Admin Mode** field, select the **Enable** or **Disable** option. This sets the administrative status of MLD in the router to active or inactive. The default is disable.
2. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IPv6 MLD Routing Interface Configuration

To display the IPv6 Multicast MLD Routing Interface Configuration page, click **Routing** > **IPv6 Multicast** > **MLD** > **Routing Interface Configuration**. The following page is displayed.



IPv6 MLD Routing Interface Configuration

1. In the **Go To Interface** field, enter the interface in unit/slot/port format and click **Go**. The entry corresponding to the specified interface is selected.
2. Select the check box beside the **Interface** for which data is to be displayed or configured.
3. In the **Admin Mode** field, select the **Enable** or **Disable** option to set the administrative status of MLD on the selected routing interface. The default is disable.
4. In the **Version** field, enter the version you want to configure for the selected interface. Valid values are 1 to 2. The default value is 2.
5. In the **Query Interval** field, enter the frequency in seconds at which MLD host-query packets are to be transmitted on this interface. Valid values are 1 to 3600. The default value is 125.
6. In the **Query Max Response Time** field, enter the maximum query response time, in milliseconds, to be advertised in MLDv2 queries on this interface. Valid values are 0 to 65535. The default value is 10000 milliseconds.
7. In the **Startup Query Interval** field, enter the configured interval in seconds between general queries sent by a Querier on startup. The default value is 31.
8. Enter the **Startup Query Count** value to indicate the configured number of Queries sent out on startup, separated by the Startup Query Interval. The default value is 2.
9. In the **Last Member Query Interval** field, enter the last member query interval in milliseconds. This is the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 655355. The default value is 1000 milliseconds.
10. In the **Last Member Query Count** field, enter the number of queries to be sent on receiving a leave group report. Valid values are from 1 to 20. The default value is 2.

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

Table 148, IPv6 MLD Routing Interface Configuration describes the non-configurable data that is displayed.

Table 148. IPv6 MLD Routing Interface Configuration

Field	Description
Operational Mode	The operational status of MLD on the Interface.
Robustness	The robustness parameter for the selected interface. This variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness variable may be increased. MLD is robust to (robustness variable-1) packet losses. The default value is 2.

IPv6 MLD Routing Interface Statistics

To display the IPv6 Multicast MLD Routing Interface Statistics page, click **Routing** > **IPv6 Multicast** > **MLD** > **Routing Interface Statistics**. The following page is displayed.

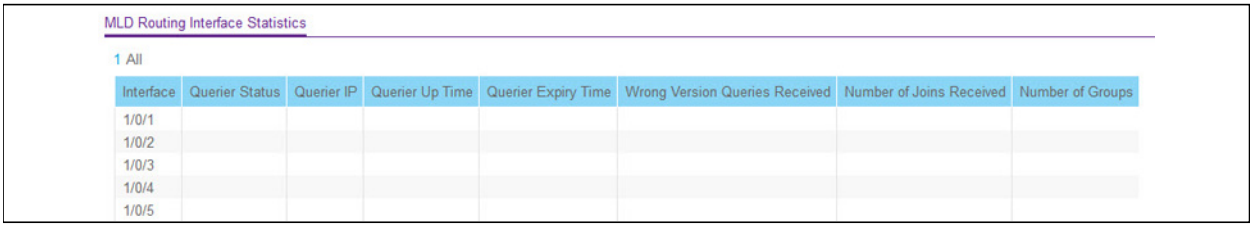


Table 149, IPv6 MLD Routing Interface Statistics describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

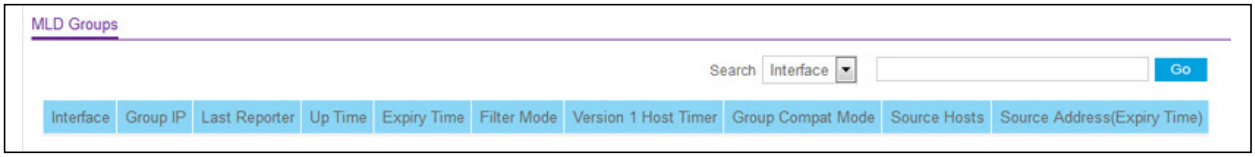
Table 149. IPv6 MLD Routing Interface Statistics

Field	Description
Interface	The interface for which data is to be displayed.
Querier Status	Indicates whether the selected interface is an MLD Querier or non-querier on the subnet it is associated with.
Querier IP	The address of the MLD Querier on the IP subnet to which the selected interface is attached.
Querier Up Time	The time in seconds since the MLD interface Querier was last changed

Field	Description
Querier Expiry Time	The time in seconds remaining before the other Querier present timer expires. If the local system is the Querier, this will be zero.
Wrong Version Queries Received	The number of queries received whose MLD version does not match the MLD version of the interface.
Number of Joins Received	The number of times a group membership has been added on the selected interface.
Number of Groups	The current number of membership entries for the selected interface in the cache table.

IPv6 MLD Groups

To display the IPv6 MLD Groups page, click **Routing** > **IPv6 Multicast** > **MLD** > **MLD Groups**. The following page is displayed.



1. Use the **Search By** menu to search for multicast entries by **Interface** or **Group**.
   - Select **Interface** from the **Search** list, enter the Interface in unit/slot/port format, for example 1/0/13, then click **Go**. If the entry exists, the entry is displayed as the first entry, followed by the remaining entries.
   - Select **Group** from the **Search** list, enter the MLD Group IP, then click **Go**. If the entry exists, that entry with the matching Group is displayed as the first entry, followed by the remaining entries. An exact match is required.

Table 150, IPv6 Multicast MLD Groups describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 150. IPv6 Multicast MLD Groups

Field	Description
Interface	The interface for which data is to be displayed.
Group IP	The address of the MLD members.
Last Reporter	The IP address of the source of the last membership report received for this multicast group address on the selected interface.
Up Time	The time elapsed in seconds since the multicast group has been known.
Expiry Time	Time left in seconds before the entry is removed from the MLD membership table of this interface.

Field	Description
Filter Mode	The filter mode of the multicast group on this interface. Possible values are **Include** and **Exclude**.
Version 1 Host Timer	The time remaining until the router assumes that there are no longer any MLD version 1 Hosts on the specified interface.
Group Compat Mode	The compatibility mode of the multicast group on the interface. The values it can take are MLDv1 and MLDv2.
Source Hosts	This parameter shows source addresses which are members of this multicast address.
Source Address (Expiry Time)	This parameter shows expiry time interval against each source address that is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.

IPv6 MLD Traffic

To display the IPv6 MLD Traffic page, click **Routing** > **IPv6 Multicast** > **MLD** > **MLD Traffic**. The following page is displayed.

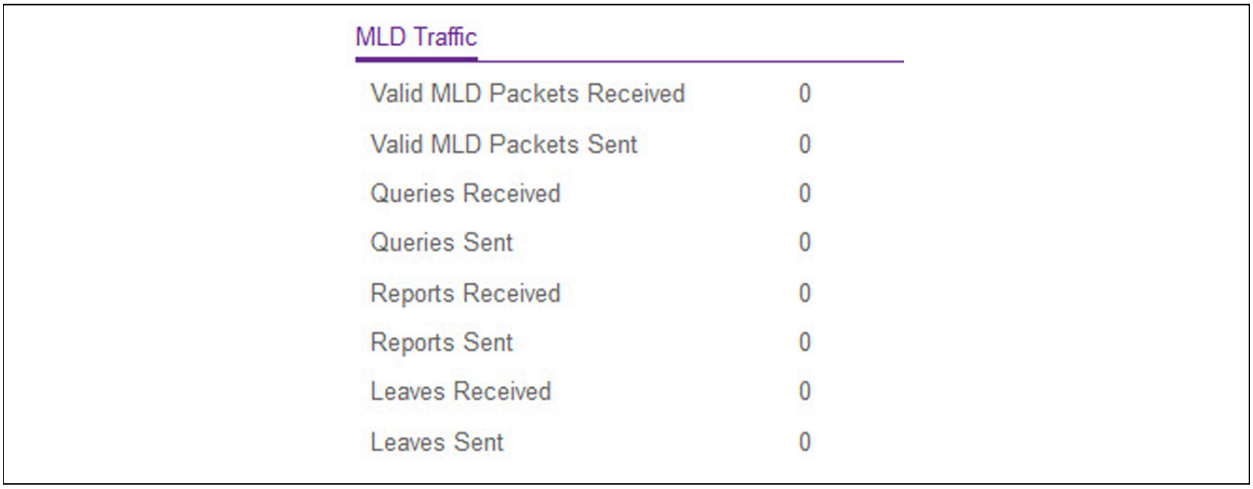


Table 151, IPv6 Multicast MLD Traffic describes the non-configurable data that is displayed.

Table 151. IPv6 Multicast MLD Traffic

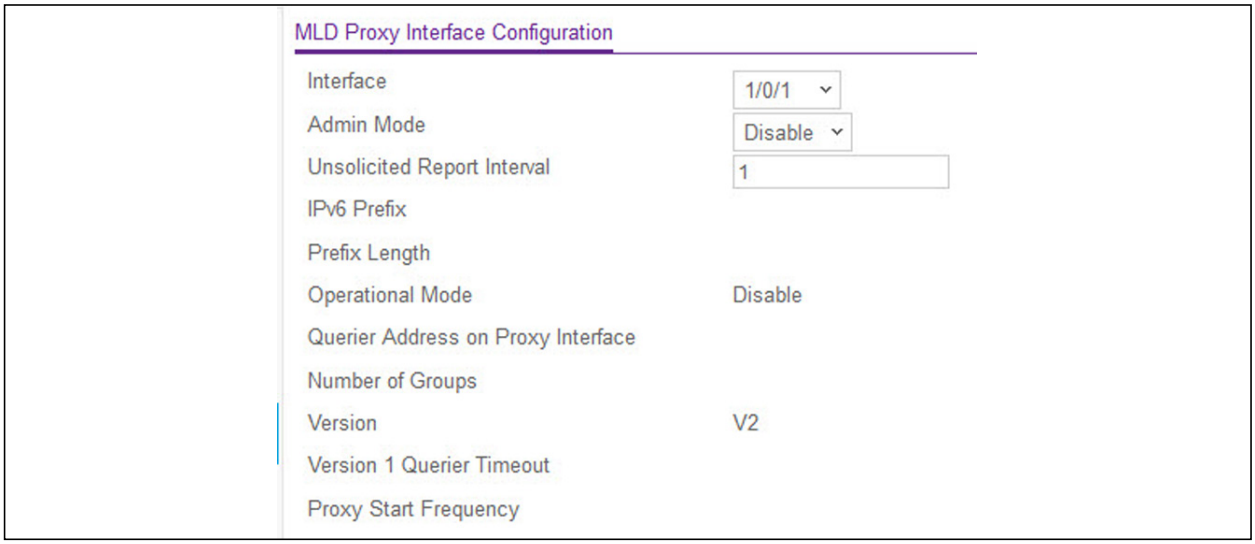
Field	Description
Valid MLD Packets Received	The number of valid MLD packets received by the router.
Valid MLD Packets Sent	The number of valid MLD packets sent by the router.
Queries Received	The number of valid MLD queries received by the router.
Queries Sent	The number of valid MLD queries sent by the router.

Field	Description
Reports Received	The number of valid MLD reports received by the router.
Reports Sent	The number of valid MLD reports sent by the router.
Leaves Received	The number of valid MLD leaves received by the router.
Leaves Sent	The number of valid MLD leaves sent by the router.

- Click **Clear** to clear all the MLD traffic.
- Click **Update** to update the page with the latest information on the switch.

IPv6 MLD Proxy Interface Configuration

To display the IPv6 Multicast MLD Proxy Interface Configuration page, click **Routing** > **IPv6 Multicast** > **MLD** > **Proxy Interface Configuration**. The following page is displayed.



➢ **IPv6 MLD Proxy Interface Configuration**

1. In the **Interface** list, select the interface.
2. In the **Admin Mode** list, select the **Enable** or **Disable** option to set the administrative status of MLD Proxy on the selected interface. The default is disable. Routing, MLD and Multicast global admin modes should be enabled to enable MLD Proxy interface mode.
3. In the **Unsolicited Report Interval** field, enter the unsolicited time interval value in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Valid values are 1 to 260. The default value is 1.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 152, IPv6 Multicast MLD Proxy Interface Configuration describes the non-configurable data that is displayed.

Table 152. IPv6 Multicast MLD Proxy Interface Configuration

Field	Description
IPv6 Prefix	The IPv6 address of the MLD Proxy interface.
Prefix Length	The prefix length for the IPv6 address of the MLD Proxy interface.
Operational Mode	The operational state of MLD Proxy interface.
Querier Address on Proxy Interface	Specifies the Querier address on the proxy interface.
Number of Groups	The current number of multicast group entries for the MLD Proxy interface in the cache table.
Version	This field is configurable only when MLD Proxy interface mode is enabled. Enter the version of MLD to configure on the selected interface. Valid values are 1 to 2. The default version is 3.
Version 1 Querier Timeout	The older MLD version 1 Querier time-out value in seconds. The Older Version Querier Interval is the timeout for transitioning a host back to MLDv2 mode once an older version query is heard. When an older version query is received, hosts set their Older Version Querier Present Timer to Older Version Querier Interval.
Proxy Start Frequency	The number of times the proxy was brought up.

IPv6 MLD Proxy Interface Statistics

To display the IPv6 Multicast MLD Proxy Interface Statistics page, click **Routing** > **IPv6 Multicast** > **MLD** > **Proxy Interface Statistics**.

Table 153, IPv6 Multicast MLD Proxy Interface Statistics describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

Table 153. IPv6 Multicast MLD Proxy Interface Statistics

Field	Description
Proxy Interface	Displays the interface on which MLD Proxy packets received.
Version	The version of MLD Proxy packets received.
Queries Received	The number of MLD Proxy queries received.
Reports Received	The number of MLD Proxy reports received.
Reports Sent	The number of MLD Proxy reports sent.

Field	Description
Leaves Received	The number of MLD Proxy leaves received.
Leaves Sent	The number of MLD Proxy leaves sent.

IPv6 MLD Proxy Membership

To display the IPv6 Multicast MLD Proxy Membership page, click **Routing** > **IPv6 Multicast** > **MLD** > **Proxy Membership**.

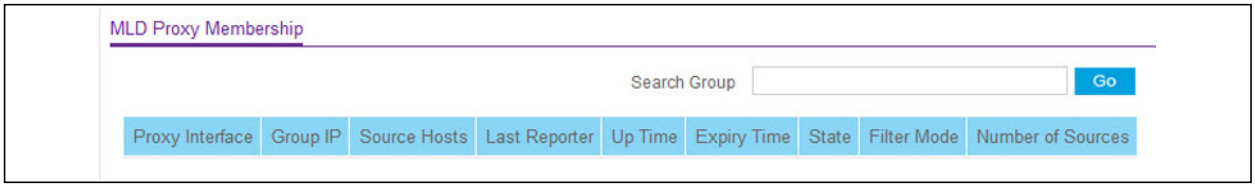


Table 154, IPv6 Multicast MLD Proxy Membership on page 368 describes the non-configurable data that is displayed.

Click **Update** to update the page with the latest information on the switch.

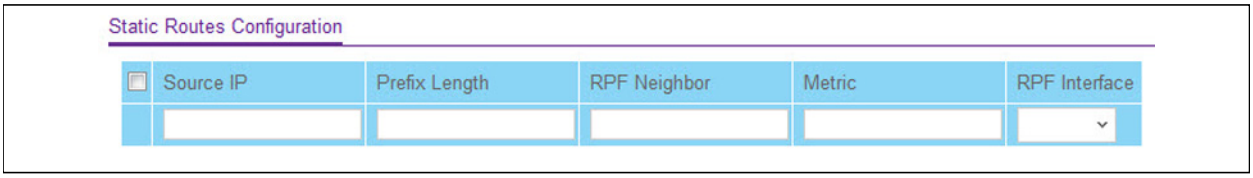
Table 154. IPv6 Multicast MLD Proxy Membership

Field	Description
Proxy Interface	Displays the interface on which MLD Proxy is enabled.
Group IP	The IPv6 multicast group address.
Source Hosts	Source addresses that are members of this multicast address.
Last Reporter	The IPv6 address of the source of the last membership report received for the IPv6 Multicast group address on the MLD Proxy interface.
Up Time	The time elapsed since this entry was created.
Expiry Time	The expiry time interval against each source address that is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.
State	The state of the host entry. A host can be in one of the following states: • Non-member state—Does not belong to the group on the interface. • Delaying member state—Host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. • Idle member state—Host belongs to the group on the interface and no report timer is running.

Field	Description
Filter Mode	The group filter mode (Include/Exclude/None) for the specified group on the MLD Proxy interface. Possible modes are: • Include • Exclude • None
Number of Sources	The number of source hosts present in the selected multicast group.

IPv6 Multicast Static Routes Configuration

To display the IPv6 Multicast Static Routes Configuration page, click **Routing** > **IPv6 Multicast** > **Static Routes Configuration**. The following page is displayed.



➢ **IPv6 Static Routes Configuration**

1. In the **Source IP** field, enter the IP Address that identifies the multicast packet source for the entry you are creating.
2. In the **Prefix Length** field, enter the Prefix Length to be applied to the Source IPv6 address.
3. In the **RPF Neighbor** field, enter the IP address of the neighbor router on the path to the source.
4. In the **Metric** field, enter the link state cost of the path to the multicast source. The range is 0 to 255; the default is 1. You can change the metric for a configured route by selecting the static route and editing this field.
5. Select the interface number from the **RPF Interface** list. This is the interface that connects to the neighbor router for the given source IP address.
6. Click **Add** to add a new static route to the switch.
7. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
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 **Delete** to delete the selected multicast static route.

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 370
- *Differentiated Services* on page 378

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 371

- *Advanced* on page 372

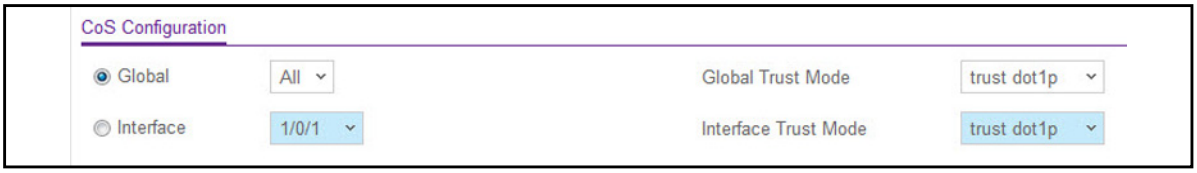
Basic

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

- *CoS Configuration* on page 371

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.

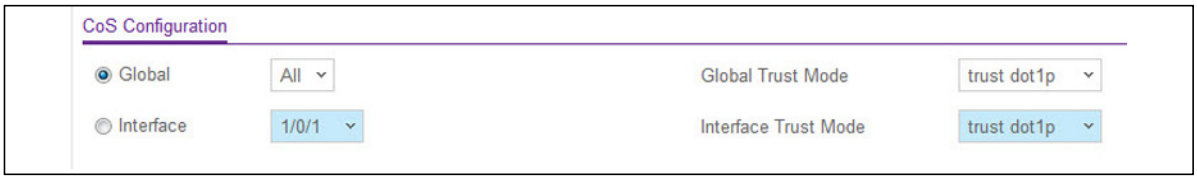
Advanced

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

- *CoS Configuration* on page 372
- *802.1p to Queue Mapping* on page 373 (Advanced)
- *IP DSCP to Queue Mapping* on page 373 (Advanced
- *CoS Interface Configuration* on page 374 (Advanced)
- *Interface Queue Configuration* on page 375 (Advanced)
- *CoS Queue Drop Precedence Configuration* on page 376

CoS Configuration

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

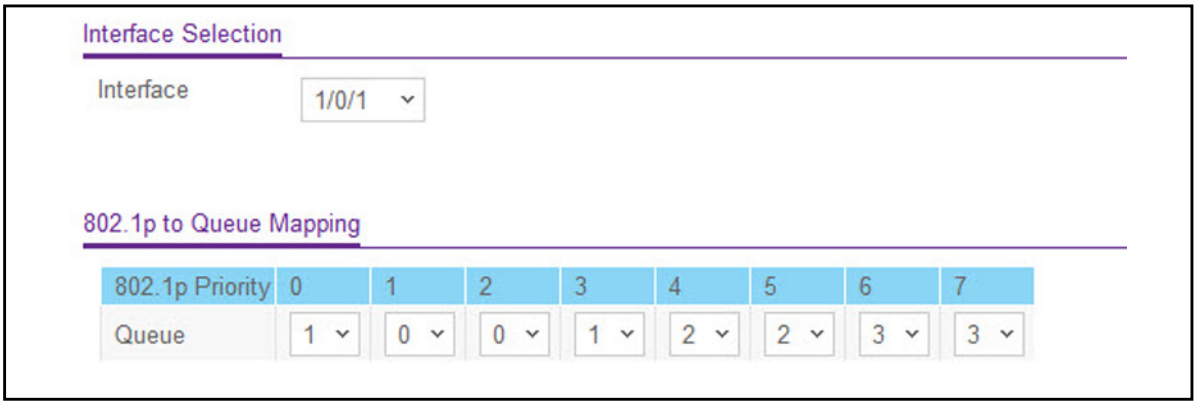


1. Use **Global** to specify all CoS configurable interfaces. The option “Global” represents the most recent global configuration settings.
2. Use **Interface** to specify CoS configuration settings based per-interface.
3. Use **Global Trust Mode** to specify whether to trust a particular packet marking at ingress. Global Trust Mode can only be one of the following. Default value is trust dot1p.
   - untrusted
   - trust dot1p
   - trust ip-dscp
4. Use **Interface Trust Mode** to specify whether to trust a particular packet marking at ingress. Interface Trust Mode can only be one of the following. Default value is untrusted.
   - untrusted
   - trust dot1p
   - trust ip-dscp

802.1p to Queue Mapping

The 802.1p to Queue Mapping page also displays the Current 802.1p Priority Mapping table.

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



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.

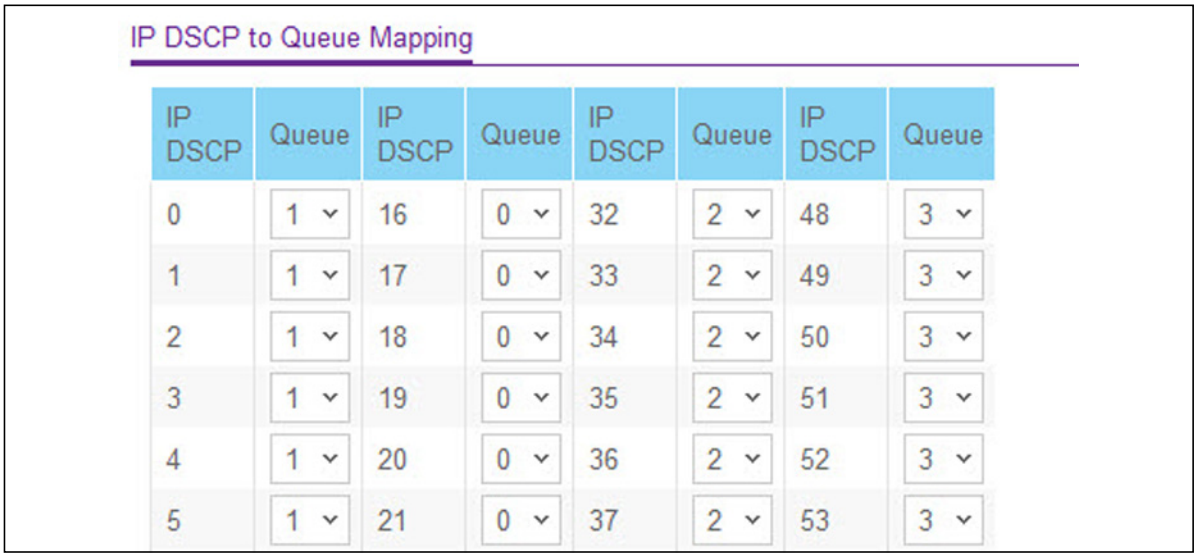
   The 802.1p Priority row contains traffic class selectors for each of the eight 802.1p priorities to be mapped. The priority goes from low (0) to high (3). For example, traffic with a priority of 0 is for most data traffic and is sent using “best effort.” Traffic with a higher priority, such as 3, might be time-sensitive traffic, such as voice or video.

   The values in each 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**.



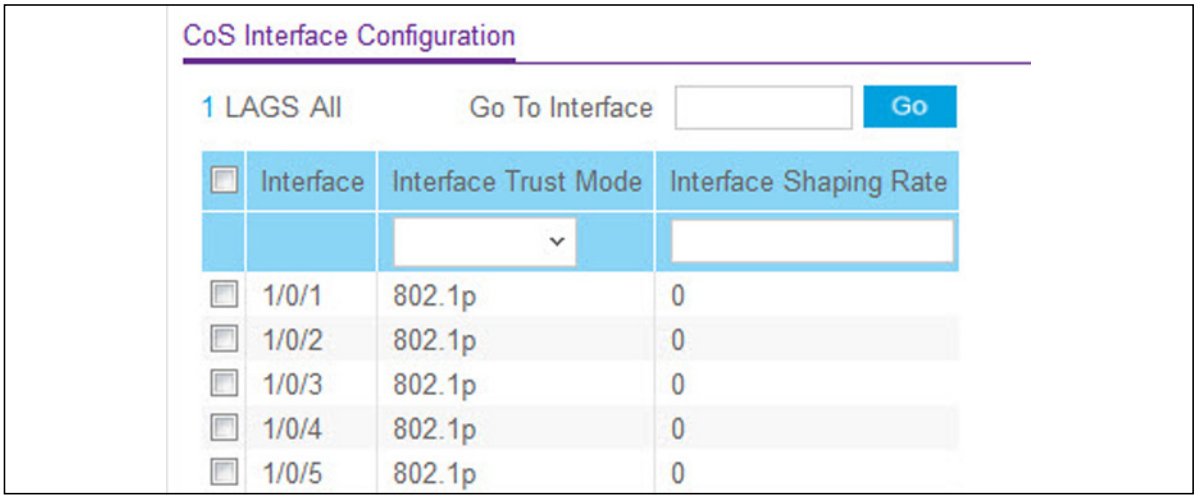
To map DSCP values to queues:

1. The **IP DSCP** field displays an IP DSCP value from 0 to 63.
2. For each DSCP value, specify which internal traffic class to map the corresponding IP DSCP value. The queue number depends on specific hardware.
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.

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.**



To configure CoS settings for an interface:

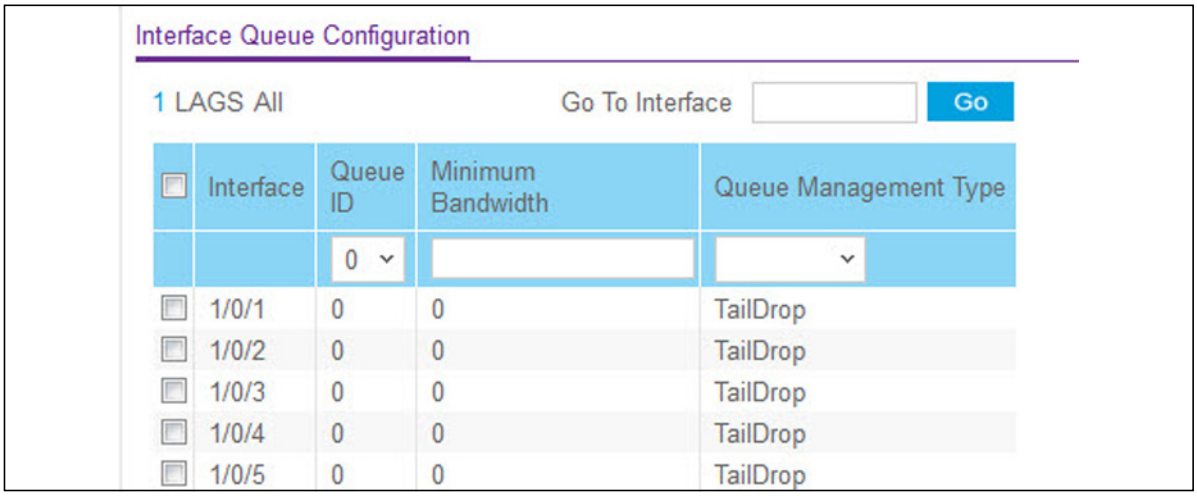
1. Select **LAG** to show the list of all LAG interfaces.
2. Select **All** to show the list of all physical as well as LAG interfaces.
3. Select an interface from the **Interface** list of all CoS configurable interfaces.
4. Use the **Go To Interface** field to enter the interface in unit/slot/port format and click **Go**. The entry corresponding the specified interface is selected.
5. Use **Interface Trust Mode** to specify whether or not to trust a particular packet marking at ingress. Interface Trust Mode can only be one of the following. Default value is 802.1p.
   - Untrusted
   - 802.1p
   - IP DSCP
6. 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.
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.

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**.



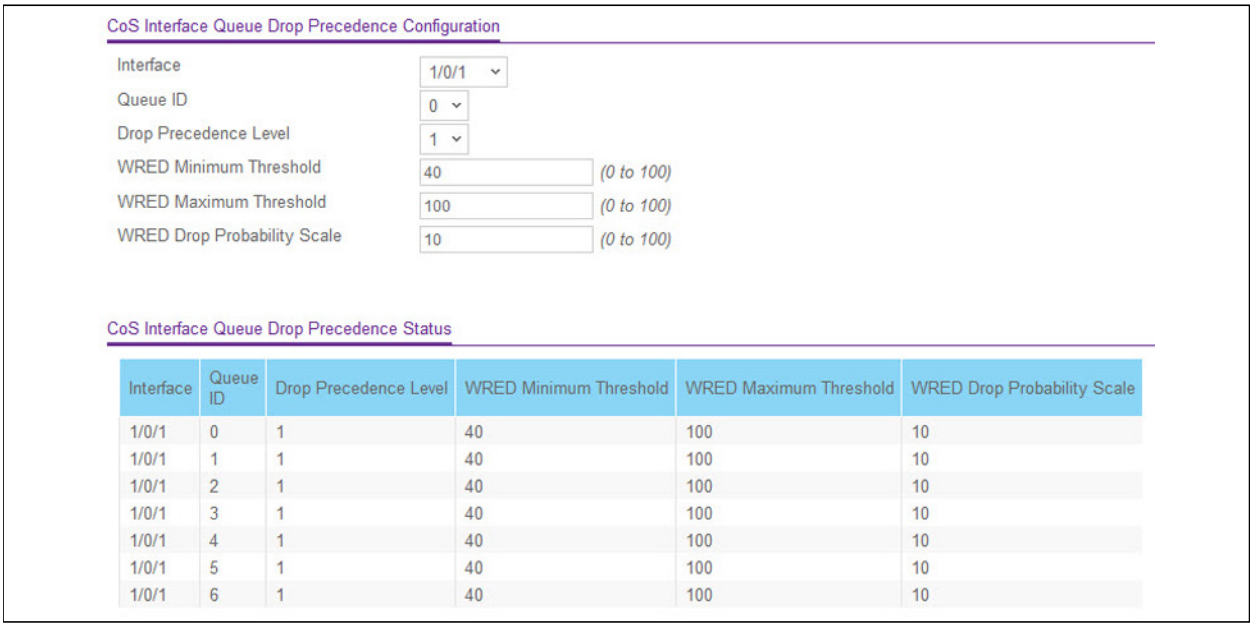
➢ **To configure CoS queue settings for an interface:**

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. Use the **Queue ID** menu to select the queue to be configured (platform based).
3. 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).
4. **Queue Management Type** displays the Queue depth management technique used for queues on this interface. This is only used if the device supports independent settings per-queue. From the Queue Management Type menu, select either **TailDrop** or **WRED**. The default value is **TailDrop**.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. If you make changes to the page, click **Apply** to apply the changes to the system.

CoS Queue Drop Precedence Configuration

Use the CoS Queue Drop Precedence Configuration page to configure CoS Drop Precedence settings.

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



- **Configure CoS Queue Drop Precedence settings**

1. Use **Interface** to specify all CoS configurable interfaces.
2. Use **Queue ID** to specify all the available queues. Valid values are 0 to 6. The default is 0.
3. Use **Drop Precedence Level** to specify all the available drop precedence levels. Valid values are 1 to 4. The default is 1.
4. Use **WRED Minimum Threshold** to specify the weighted RED minimum queue threshold below which no packets are dropped for the current drop precedence level. The range is 0 to 100. The default is 40.
5. Use **WRED Maximum Threshold** to specify the weighted RED maximum queue threshold above which all packets are dropped for the current drop precedence level. The range is 0 to 100. The default is 100.
6. Use **WRED Drop Probability Scale** to determine the packet drop probability for the current drop precedence level. The range is 0 to 100. The default is 10
7. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
8. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

CoS Interface Queue Drop Precedence Status

Table 155, CoS Interface Queue Drop Precedence Status describes the non-configurable data that is displayed.

Table 155. CoS Interface Queue Drop Precedence Status

Field	Description
Interface	Displays the CoS configurable interface.
Queue ID	Displays the Queue ID.
Drop Precedence Level	Displays the drop precedence level.
WRED Minimum Threshold	Displays the weighted RED minimum queue threshold value.
WRED Maximum Threshold	Displays the weighted RED maximum queue threshold value.
WRED Drop Probability Scale	Displays the packet drop probability value.

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.

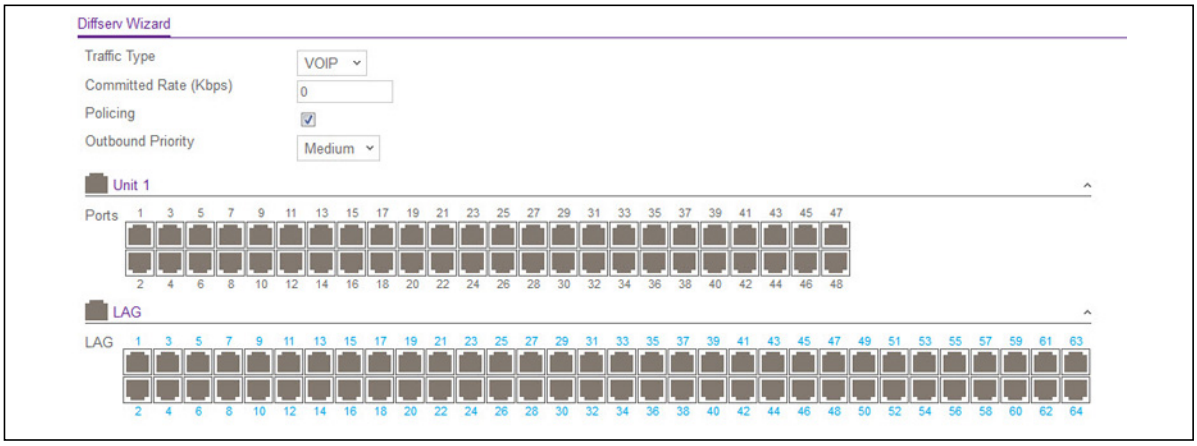
From the DiffServ link under the QoS tab, you can access the following pages:

DiffServ Wizard

The DiffServ Wizard enables DiffServ on the switch by creating a traffic class, adding the traffic class to a policy, and then adding the policy to the ports selected on DiffServ Wizard page. The DiffServ Wizard will:

- Create a **DiffServ Class** and define match criteria used as a filter to determine if incoming traffic meets the requirements to be a member of the class.
- Set the **DiffServ Class** match criteria based on **Traffic Type** selection as below:
  - **VOIP** - sets match criteria to UDP protocol.
  - **HTTP** - sets match criteria to HTTP destination port.
  - **FTP** - sets match criteria to FTP destination port.
  - **Telnet** - sets match criteria to Telnet destination port.
  - **Every** - sets match criteria all traffic.
- Create a **Diffserv Policy** and add it to the **DiffServ Class** created.
- If **Policing** is set to **YES**, then **DiffServ Policy** style is set to **Simple**. Traffic which conforms to the **Class Match** criteria will be processed according to the **Outbound Priority** selection. **Outbound Priority** configures the handling of conforming traffic as below:
  - **High** - sets policing action to markdscp ef.
  - **Med** - sets policing action to markdscp af31.
  - **Low** - sets policing action to send.
- If **Policing** is set to **NO**, then all traffic will be marked as specified below:
  - **High** - sets policy mark ipdscp ef.
  - **Med** - sets policy mark ipdscp af31.
  - **Low** - sets policy mark ipdscp be.
- Each port selected will be added to the policy created.

To display the DiffServ Wizard page, click **QoS** > **DiffServ**> **DiffServ Wizard**.



1. Use **Traffic Type** to define the **DiffServ Class**. Traffic type options: **VOIP**, **HTTP**, **FTP**, **Telnet**, and **Every**.
2. Ports displays the ports which can be configured to support a **DiffServ policy**. The **DiffServ policy** will be added to selected ports.
3. Use **Enable Policing** to add policing to the **DiffServ** Policy. The policing rate will be applied.
4. Committed Rate:
   - When **Policing** is enabled, the committed rate will be applied to the policy and the policing action is set to conform.
   - When **Policing** is disabled, the committed rate is not applied and the policy is set to markdscp.
5. Outbound Priority:
   - When **Policing** is enabled, **Outbound Priority** defines the type of policing conform action where: **High** sets action to markdscp ef, **Med** sets action to markdscp af31, and **Low** sets action to send.
   - When **Policing** is disabled, **Outbound Priority** defines the policy where: **High** sets policy to mark ipdscp ef, **Med** sets policy to mark ipdscp af31, **Low** set policy to mark ipdscp be.

Basic

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

- *DiffServ Configuration* on page 380

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**.

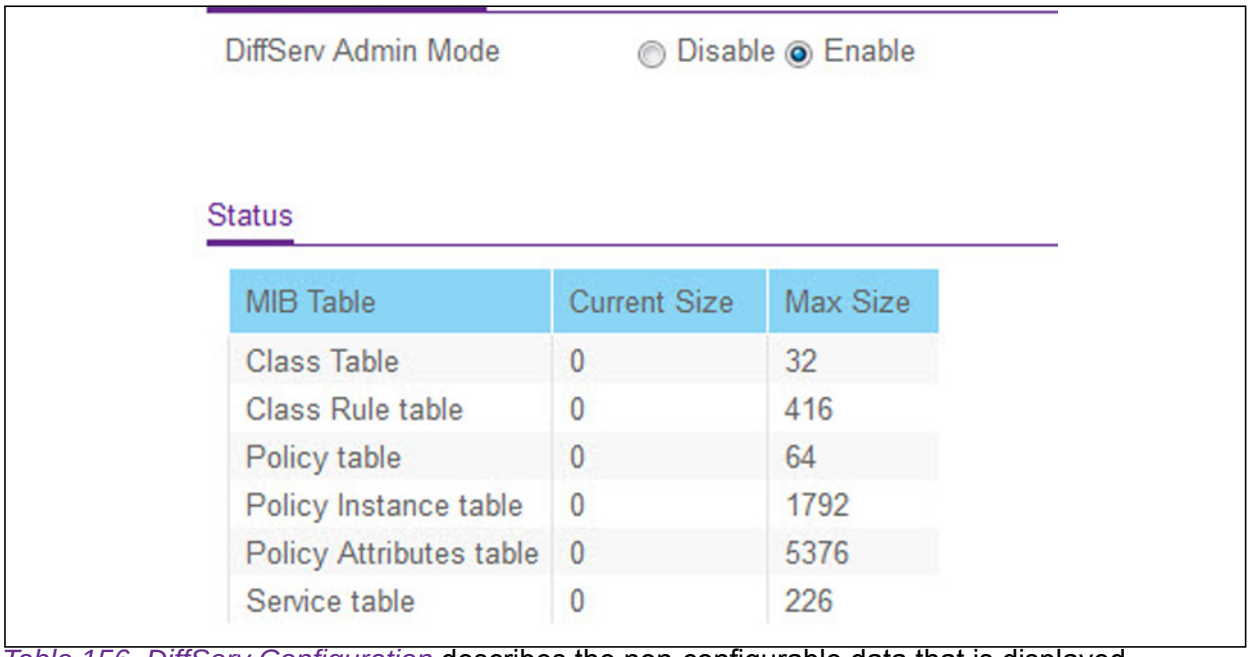


Table 156, DiffServ Configuration describes the non-configurable data that is displayed.

Table 156. DiffServ Configuration

Field	Description
DiffServ Admin Mode	The options mode for DiffServ. The default value is 'enable'. While disabled, the DiffServ configuration is retained when saved and can be changed, but it is not activated. When enabled, Diffserv services are activated.
Class table	Displays the number of configured DiffServ classes out of the total allowed on the switch.
Class Rule table	Displays the number of configured class rules out of the total allowed on the switch.
Policy table	Displays the number of configured policies out of the total allowed on the switch.
Policy Instance table	Displays the number of configured policy class instances out of the total allowed on the switch.

Field	Description
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

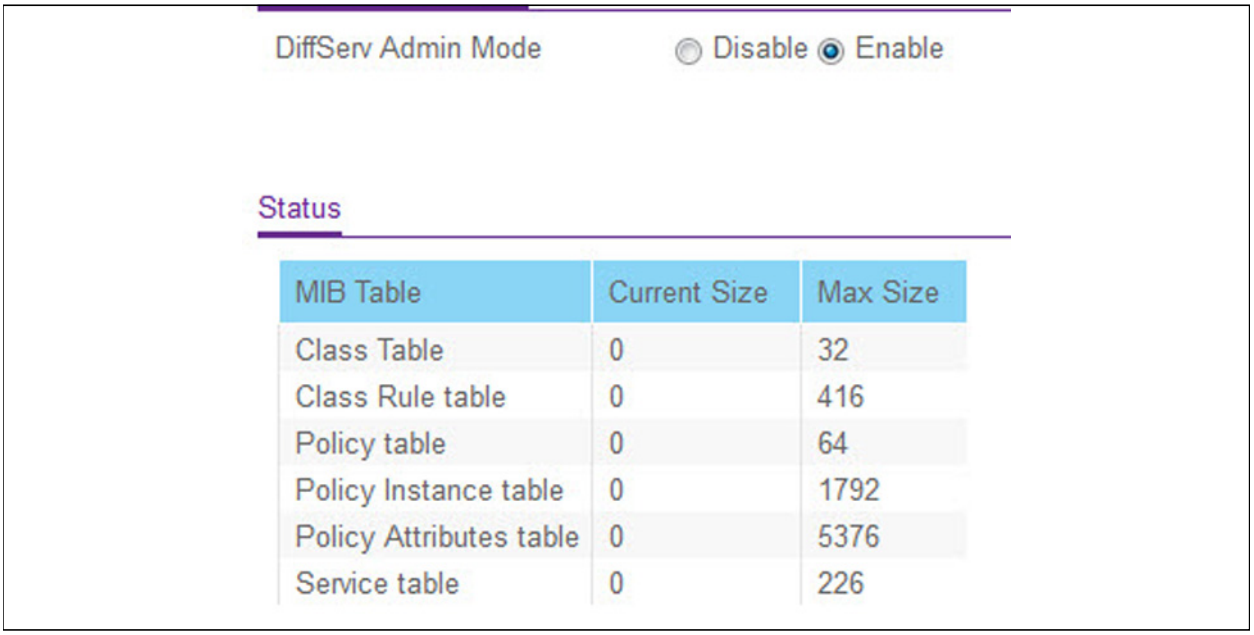
Diffserv Configuration

Packets are filtered and processed based on defined criteria. The filtering criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.

The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.

Packet processing begins by testing the match criteria for a packet. The 'all' class type option defines that each match criteria within a class must evaluate to true for a packet to match that class. The 'any' class type option defines that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

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



To configure the global DiffServ mode:

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

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

Field	Description
Class table	Displays the number of configured DiffServ classes out of the total allowed on the switch.
Class Rule table	Displays the number of configured class rules out of the total allowed on the switch.
Policy table	Displays the number of configured policies out of the total allowed on the switch.
Policy Instance table	Displays the number of configured policy class instances out of the total allowed on the switch.

Field	Description
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.

Class Configuration

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

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

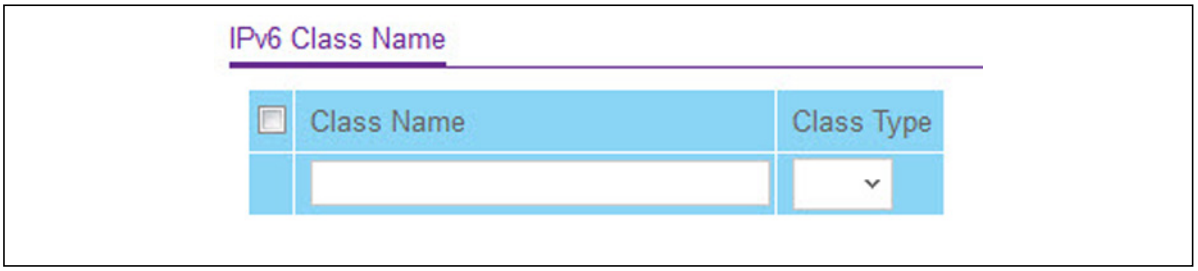
To configure a DiffServ class:

1. To create a new class, enter a **class name**, select the **class type**, and click **Add**. This field also lists all the existing DiffServ class names, from which one can be selected.

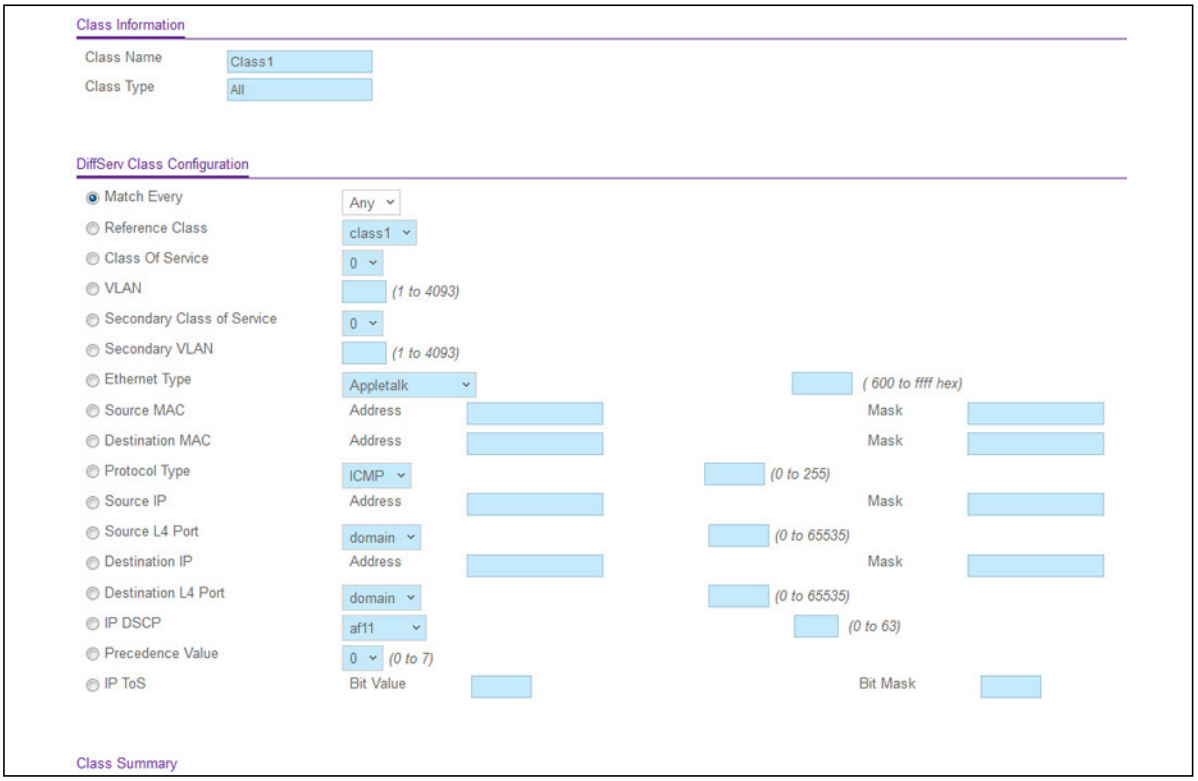
   The switch supports only the **Class Type** value **All**, which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria. Only when a new class is created, this field is a selector field. After class creation this becomes a non-configurable field displaying the configured class type.
2. To rename an existing class, select the check box next to the configured class, update the name, and click **Apply**.
3. To remove a class, click the check box beside the Class Name, then click **Delete**.
4. Click **Update** to update the page with the latest information on the switch.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch. After creating a Class, click the class link to the Class page.

To configure the class match criteria:

1. Click the **class name** for an existing class.



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



2. **Class Name** - Displays the name for the configured DiffServ class.
3. **Class Type** - Displays the DiffServ class type. Options:
   - All

   Only when a new class is created, this field is a selector field. After class creation this becomes a non-configurable field displaying the configured class type.
4. Define the criteria to associate with a DiffServ class:
   - **Match Every** - This adds to the specified class definition a match condition whereby all packets are considered to belong to the class.
   - **Reference Class** - This lists the class(es) that can be assigned as reference class(es) to the current class.
   - **Class of Service** - This lists all the values for the class of service match criterion in the range 0 to 7 from which one can be selected.

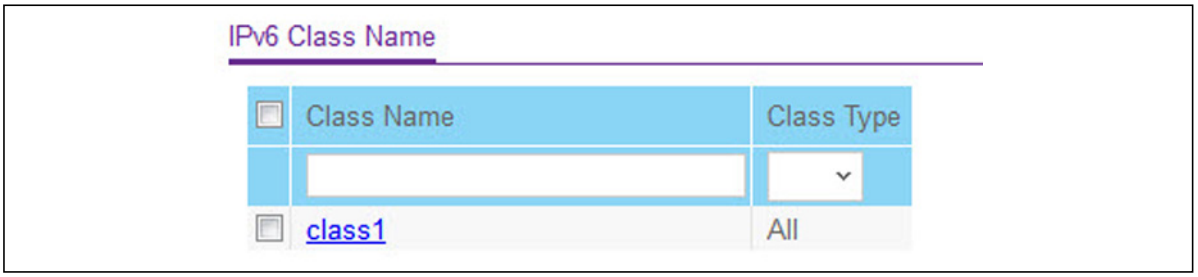
- **VLAN** - This is a value in the range of 0-4093.
- **Ethernet Type** - This lists the keywords for the Ethertype from which one can be selected.
- **Source MAC Address** - This is the source MAC address specified as six, two-digit hexadecimal numbers separated by colons.
- **Source MAC Mask** - This 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**.



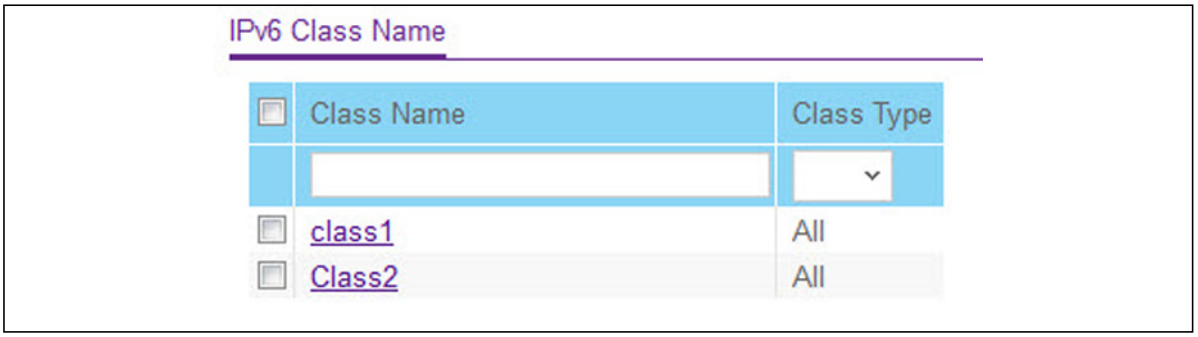
To configure a DiffServ class:

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.

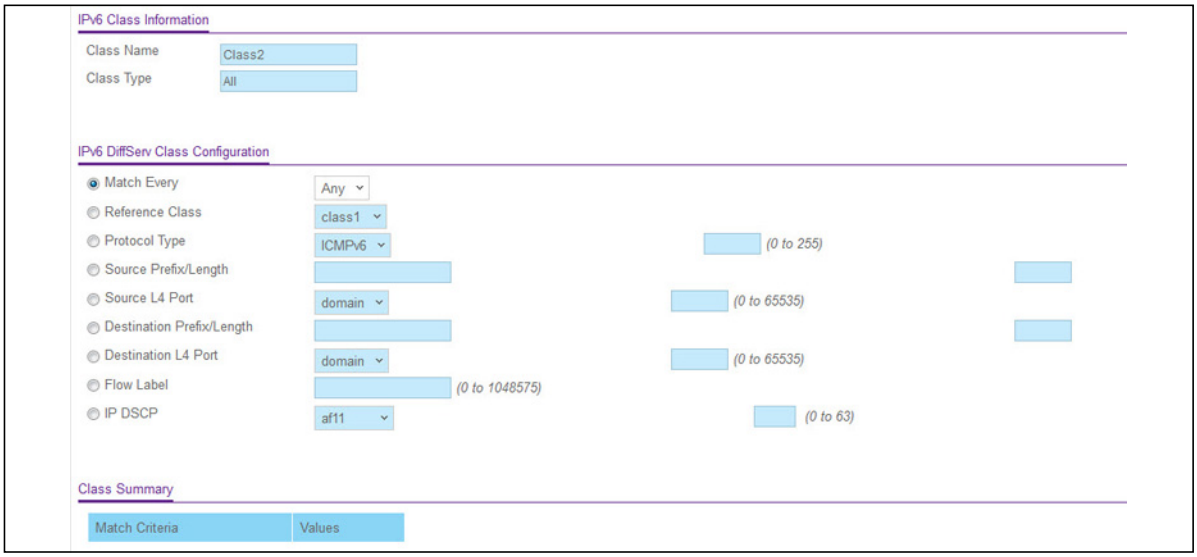
   The switch supports only the **Class Type** value **All**, which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria. Only when a new class is created, this field is a selector field. After class creation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

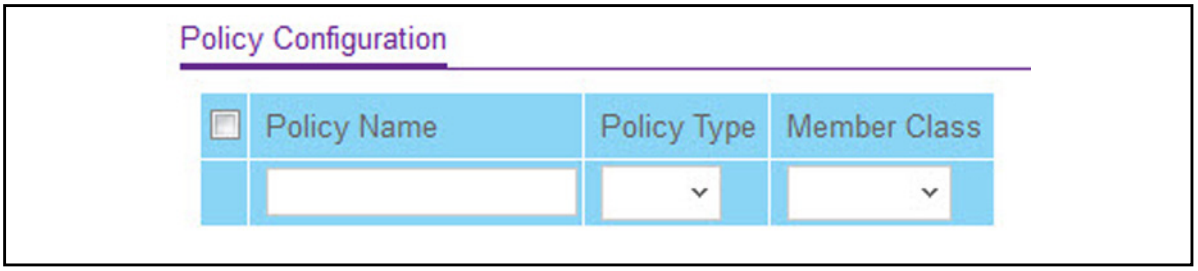
- **Destination L4 Port** - This lists the keywords for the known destination layer 4 ports from which one can be selected. The list includes 'other' as an option for the unnamed ports.
- **Flow Label** - This is a 20-bit number that is unique to an IPv6 Packet, used by end stations to signify Quality 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.

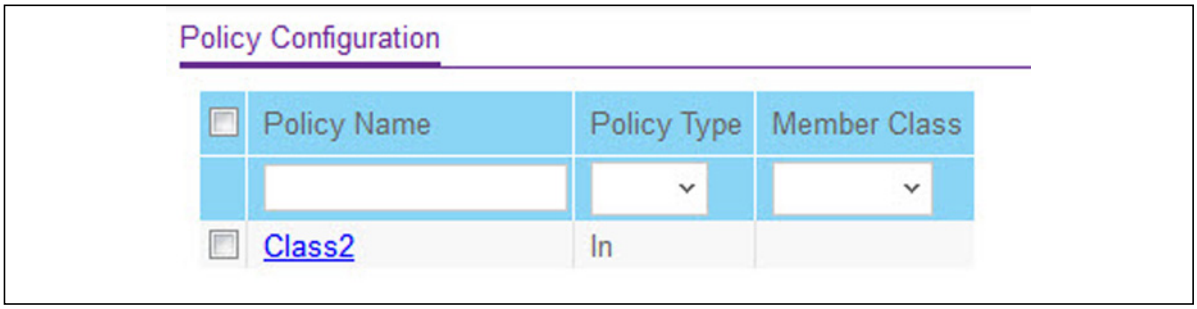
To display the page, click **QoS** > **DiffServ** > **Advanced** > **Policy Configuration**.



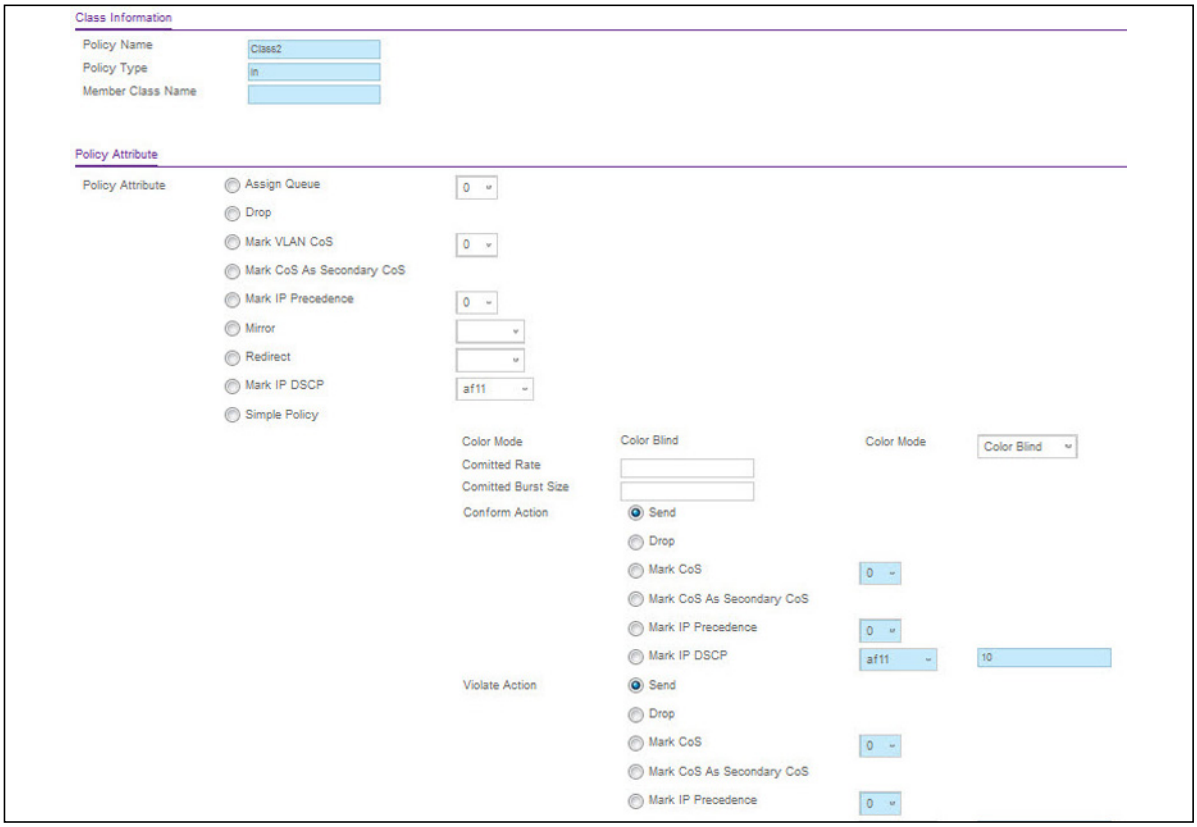
1. Use **Policy Name** to uniquely identify a policy using a case-sensitive alphanumeric string from 1 to 31 characters.
2. **Member Class** - This lists all existing DiffServ classes currently defined as members of the specified Policy, from which one can be selected. This list is automatically updated 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 **Assign Queue** to which packets will of this policy-class will be assigned. This is an integer value in the range 0 to 6.
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 CoS as Secondary Cos** - This option marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

- **Mark IP Precedence** - This is an IP Precedence value in the range from 0 to 7.
- **Two Rate Policy** - With the Two-Rate Policer, you can enforce traffic policing according to two separate rates: Committed Rate and Peak Rate.
- **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.

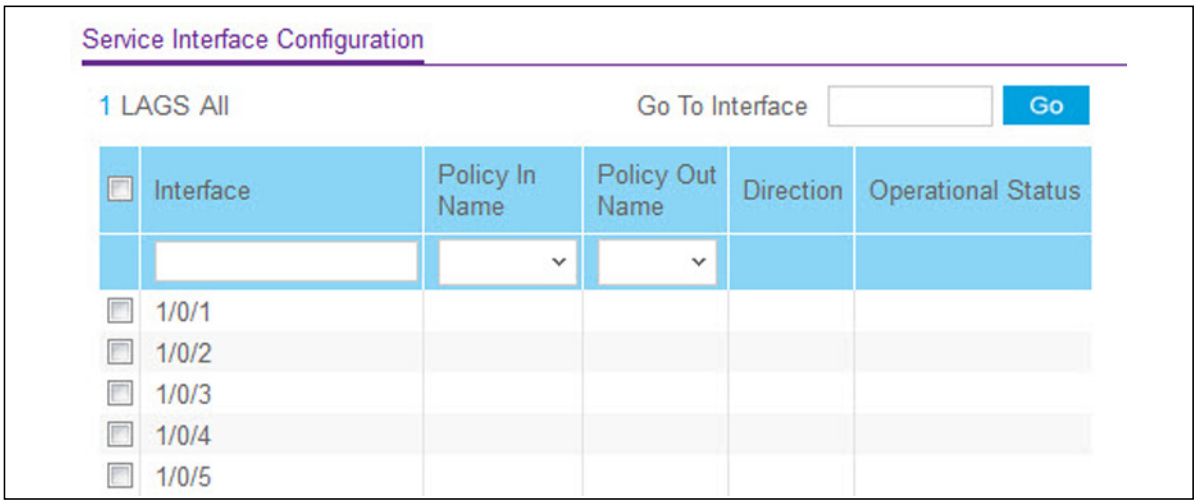
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

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:

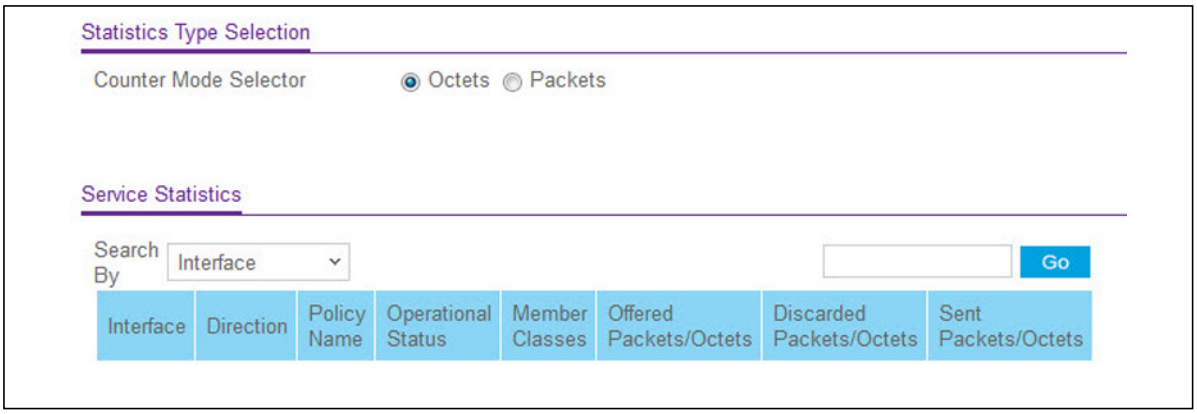
1. Use **Interface** to select the interface on which you will configure the DiffServ service.
2. **Policy Name** - Lists all the policy names from which one can be selected. This field is not shown for Read/Write users where inbound service policy attachment is not supported by the platform.

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.

Field	Description
Offered Packets/Octets	A count of the total number of packets/octets offered to all class instances in this service policy before their defined DiffServ treatment is applied. This is the overall count per-interface, per-direction.
Discarded Packets/Octets	A count of the total number of packets/octets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.
Sent Packets/Octets	A count of the total number of packets/octets forwarded for all class instances in this service policy after their defined DiffServ treatments were applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function of an outbound link transmission element. This is the overall count per-interface, per-direction.

Click **Update** to update the page with the latest information on the switch.

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

From the **Management Security Settings** tab, 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 tab contains links to the following features:

Local User

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

User Management

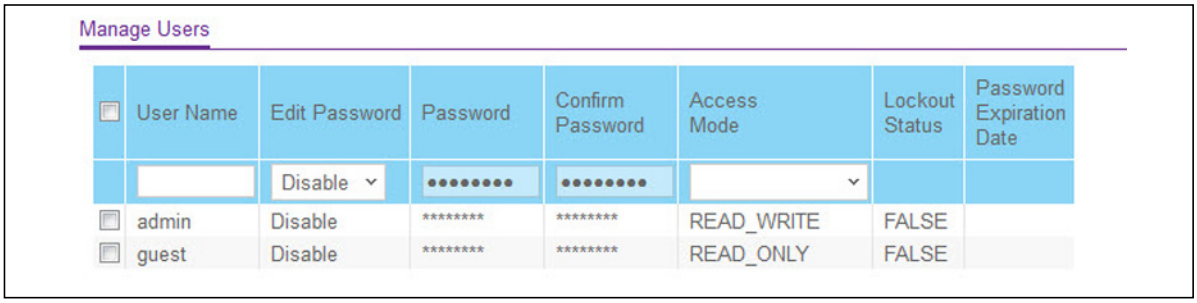
By default, two user accounts exist:

- 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 to a user account with 'Read/Write' privileges (i.e. as admin) you can use the User Management screen to assign passwords and set security parameters for the default accounts, and to add and delete accounts (other than admin) up to a maximum of six. Only a user with 'Read/Write' privileges may modify data on the web interface screens, and only one account may be created with 'Read/Write' privileges.

To display the User Management page, click **Security** > **Management Security** > **Local User** > **User Management**.

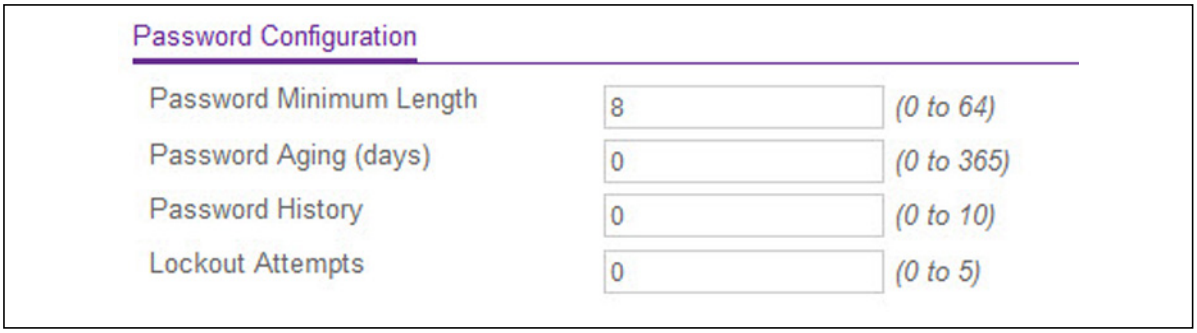


1. Use **User Name** to enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) User names are up to 64 characters in length and are not case sensitive. Valid characters include all the alphanumeric characters as well as the dash ('-') 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 the password as it is typed, 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. The default value is 'Read Only'.
6. Click **Add** to add a user account with 'Read Only' or 'Read/Write' access.
7. Click **Delete** to delete the currently selected user account. You can not delete the admin 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**.

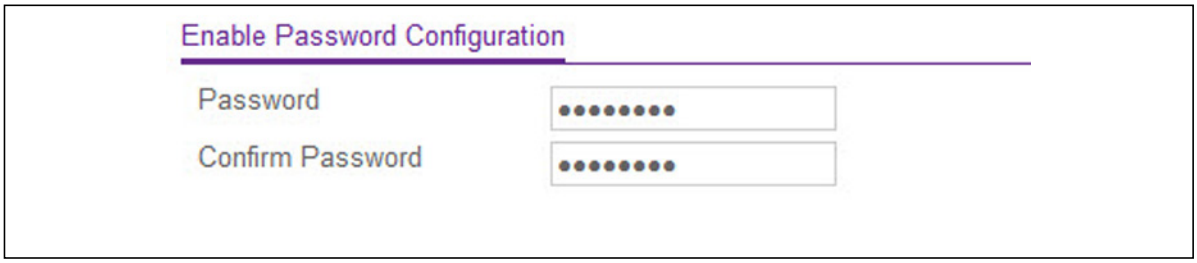


1. Use **Password Minimum Length** to specify the minimum character length of all new local user passwords.
2. Use **Password Aging (days)** to specify the maximum time for which the user passwords are valid, in days, from the time the password is set. Once a password expires, the user will be required 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.

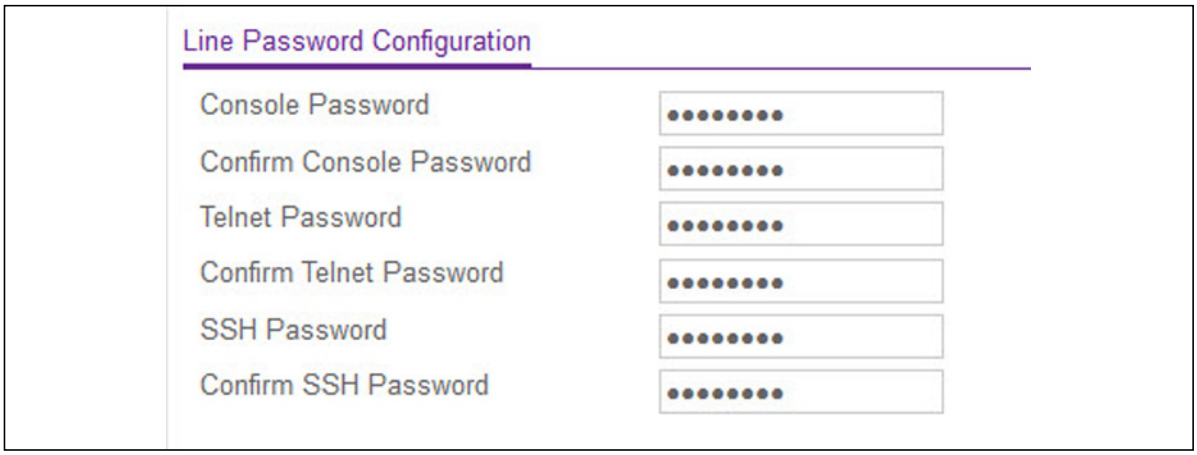
To display the Enable Password Configuration page, click **Security** > **Management Security** > **Enable Password**.



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.
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.

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)

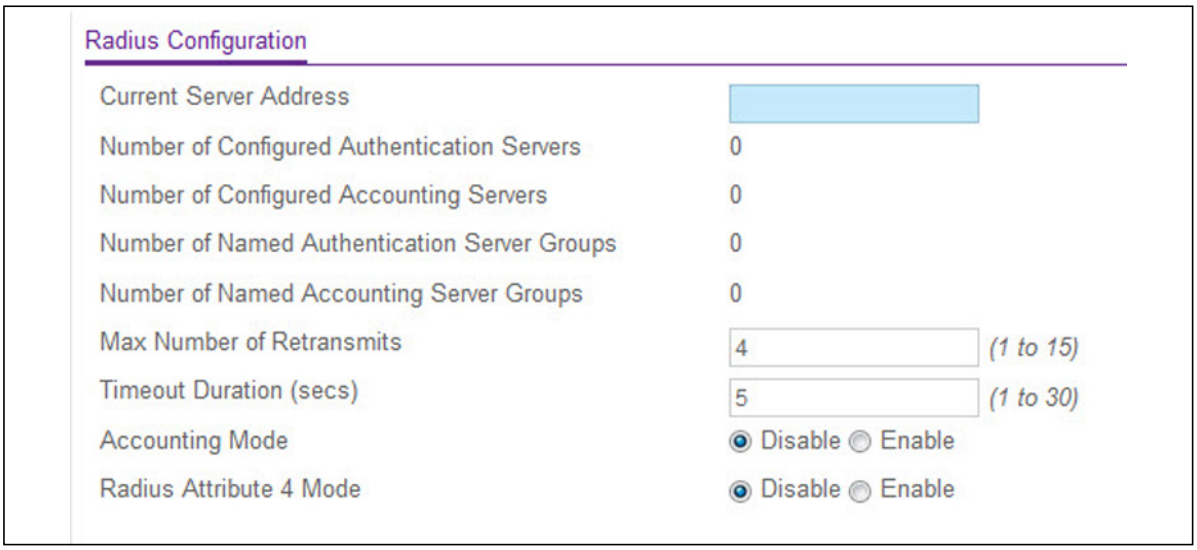
The RADIUS link contains links to the following pages:

- *RADIUS Configuration* on page 399
- *RADIUS Server Configuration* on page 400
- *Accounting Server Configuration* on page 403

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 Current Server IP Address field is blank if no servers are configured (see “RADIUS Server Configuration” on page 6-400). 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 valid range is 1 - 15. The default value is 4.

   Consideration to maximum delay time should be given when configuring RADIUS max retransmit 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. The default value is 5.

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

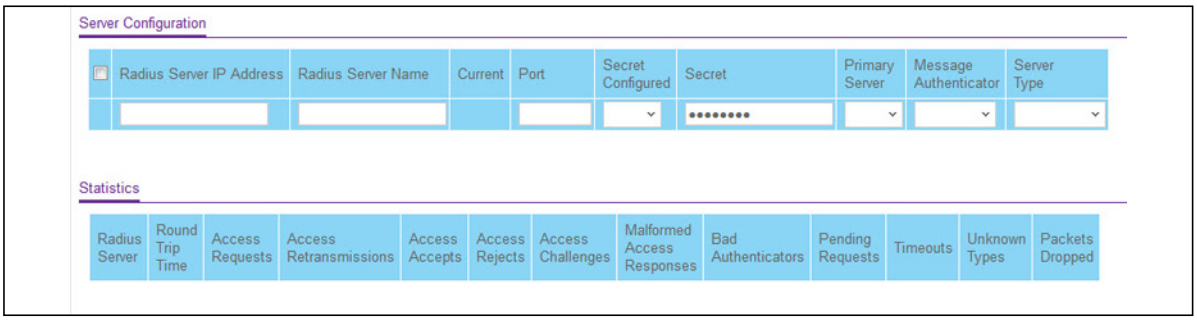
3. From the **Accounting Mode** menu, select whether the RADIUS accounting mode is enabled or disabled on the current server.
4. Use **RADIUS Attribute 4** to enable or disable RADIUS attribute 4. Default value is Disable.
5. The **Radius Attribute 4 Value** is an optional field and can be seen only when Radius attribute 4 Mode is enabled. It takes an 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 Authentication Servers	Displays the number of configured Authentication RADIUS servers. The value can range from 0 to 32.
Number of Configured Accounting Servers	Displays the number of RADIUS Accounting Servers configured. The value can range from 0 to 32.
Number of Named Authentication Server Groups	Displays the number of Named RADIUS server Authentication groups configured.
Number of Named Accounting Server Groups	Displays the number of Named RADIUS server Accounting groups configured.

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 as a 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:

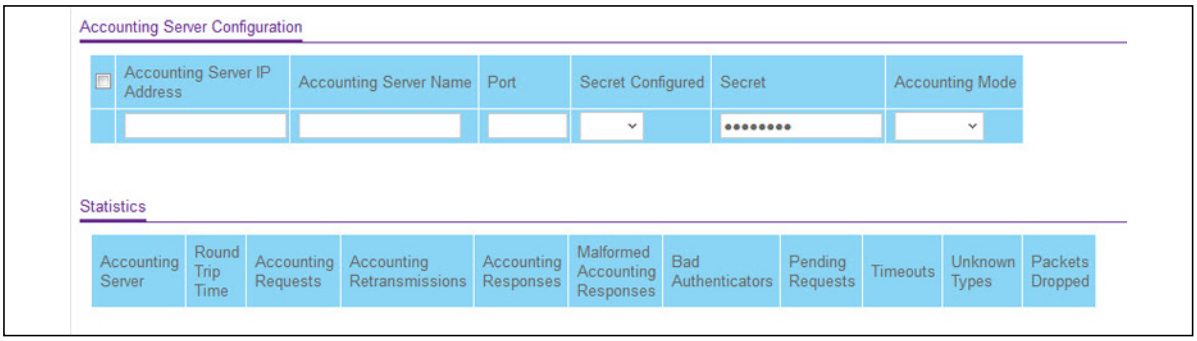
- Click **Clear Counters** to reset the authentication server and RADIUS statistics to their default values.

Field	Description
Radius Server	Displays the address of the RADIUS server or the name of the RADIUS server for which the statistics are displayed.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included in 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. 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** drop-down box, select Yes to add a RADIUS secret in the next field. 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** drop-down box, 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	Displays 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.

Field	Description
Accounting Requests	Displays the number of RADIUS Accounting-Request packets sent not including retransmissions.
Accounting Retransmissions	Displays the number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Accounting Responses	Displays the number of RADIUS packets received on the accounting port from this server.
Malformed Accounting Responses	Displays the number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	Displays the number of RADIUS Accounting-Response packets that contained invalid authenticators received from this accounting server.
Pending Requests	Displays the number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	Displays the number of accounting timeouts to this server.
Unknown Types	Displays the number of RADIUS packets of unknown type that were received from this server on the accounting port.
Packets Dropped	Displays the number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

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.

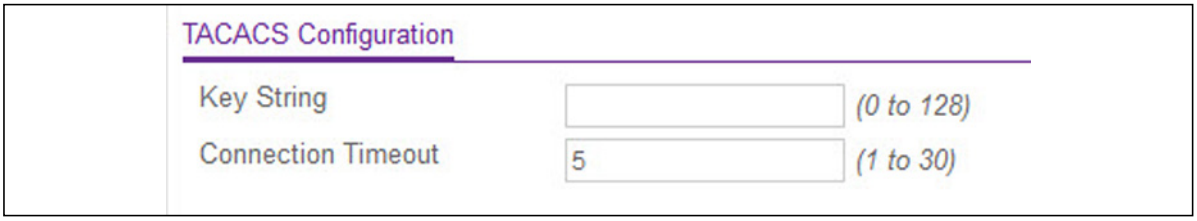
The TACACS protocol ensures network security through encrypted protocol exchanges between the device and TACACS server.

The TACACS link contains links to the following pages:

TACACS Configuration

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

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



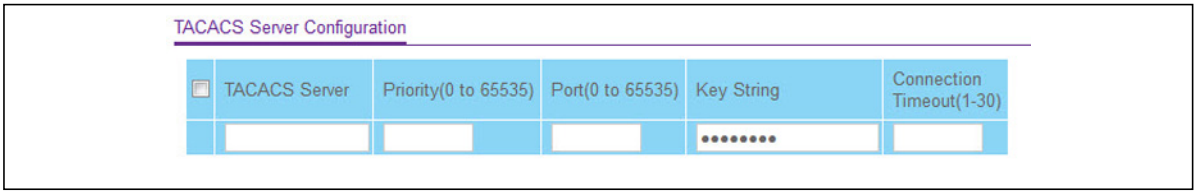
To configure global TACACS settings:

1. In the **Key String** field, specify the authentication and encryption key for TACACS communications between the 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 Product Family 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 configure the TACACS server IP address.
2. Use **Priority** to specify the order in which the TACACS servers should be 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 key 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

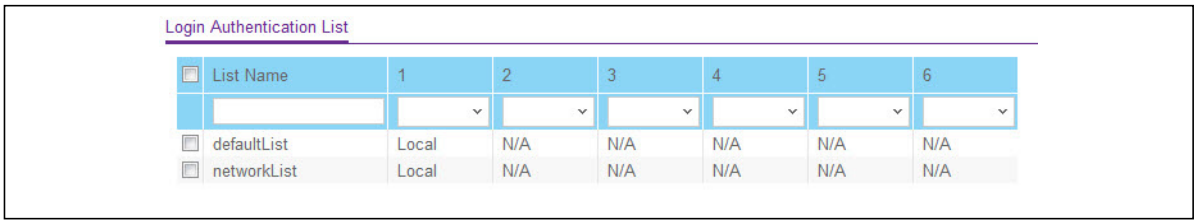
The Authentication List link contains links to the following pages:

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 cannot delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list.

Two default lists are present: DefaultList and networkList.

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



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 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:
   - **Enable**- the privileged EXEC password will be used for authentication.
   - **Line**- the line password will be used for authentication.

- **Local**- the user's locally stored ID and password will be used for authentication
- **None**- the user will not be authenticated.
- **Radius**- the user's ID and password will be authenticated using the RADIUS server instead of local server.
- **Tacacs**- the user's ID and password will be authenticated using the TACACS server.

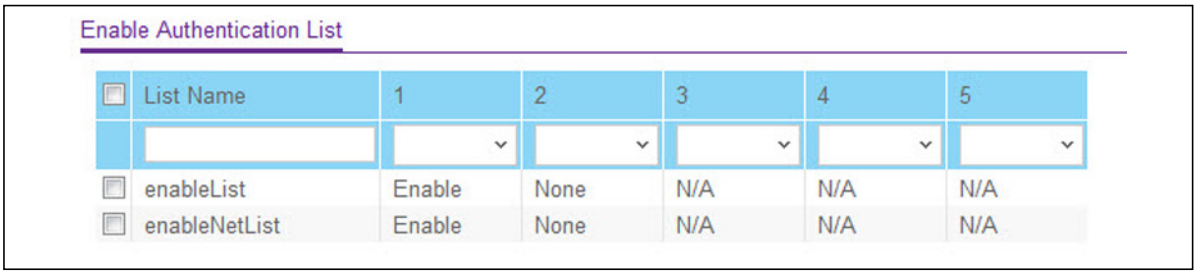
3. Use the menu to select the method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. Note that this parameter will not appear when you first create a new login list.
4. Use the menu to select the method, if any, that should appear third in the selected authentication login list. If you select a method that does not time out as the third method, the fourth method will not be tried.
5. Use the menu to select the method, if any, that should appear fourth in the selected authentication login list. If you select a method that does not time out as the fourth method, the fifth method will not be tried.
6. Use the menu to select the method, if any, that should appear fifth in the selected authentication login list. If you select a method that does not time out as the fifth method, the sixth method will not be tried.
7. Use the menu to select the method, if any, that should appear sixth in the selected authentication login list.
8. Click **Add** to add a new login list to the switch.
9. Click **Delete** to remove the selected authentication login list from the configuration. The delete will fail if the selected login list is assigned to any user (including the default user) for system login. You can only use this button if you have Read/Write access. The change will not be retained across a power cycle unless you perform a save.

Enable Authentication List

You use this page to configure enable lists. A enable list specifies the authentication method(s) you use 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 cannot delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list

Two default lists are present: enableList and enableNetList.

To display the Enable Authentication List page, click **Security** > **Management Security > Authentication List** > **Enable Authentication List**.



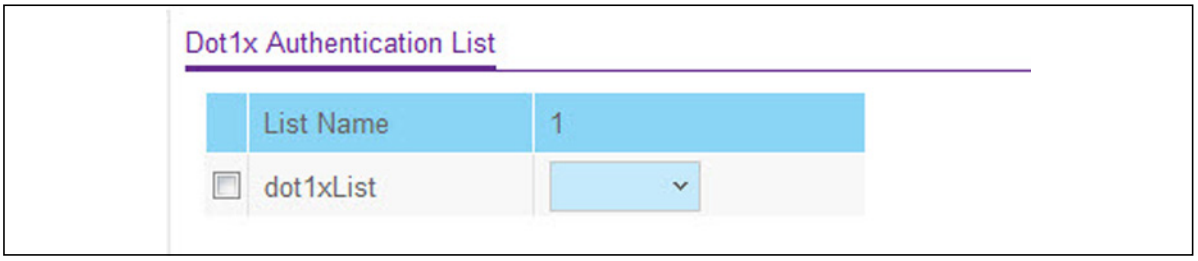
1. **List Name** - If you are creating a new enable list, enter the name you want to assign. It can be up to 15 alphanumeric characters long and is not case sensitive.
2. Use the menu to select the method that should appear first in the selected authentication enable list. The options are:
   - **Enable**- the privileged EXEC password will be used for authentication.
   - **Line**- the line password will be used for authentication.
   - **None**- the user will not be authenticated.
   - **RADIUS**- the user's name and password will be authenticated using the RADIUS server instead of local server.
   - **TACACS**- the user's name and password will be authenticated using the TACACS server.
   - **Deny**- authentication always fails.
3. Use the menu to select the method, if any, that should appear second in the selected authentication enable 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 menu to select the method, if any, that should appear third in the selected authentication enable list. If you select a method that does not time out as the third method, the fourth method will not be tried.
5. Use the menu to select the method, if any, that should appear fourth in the selected authentication enable list. If you select a method that does not time out as the fourth method, the fifth method will not be tried.
6. Use the menu to select the method, if any, that should appear fifth in the selected authentication enable list.
7. Click **Add** to add a new login list to the switch.
8. Click **Delete** to remove the selected authentication enable list from the configuration. You can only use this button if you have Read/Write access. The change will not be retained across a power cycle unless you perform a save.

Dot1x Authentication List

You use this page to configure a dot1x list. A dot1x list specifies the authentication method(s) you want to use to validate port access for the users associated with the list. Only one dot1x method can be supported.

The default list is: dot1xList.

To display the Dot1x Authentication List page, click **Security** > **Management Security > Authentication List** > **Dot1x Authentication List**.

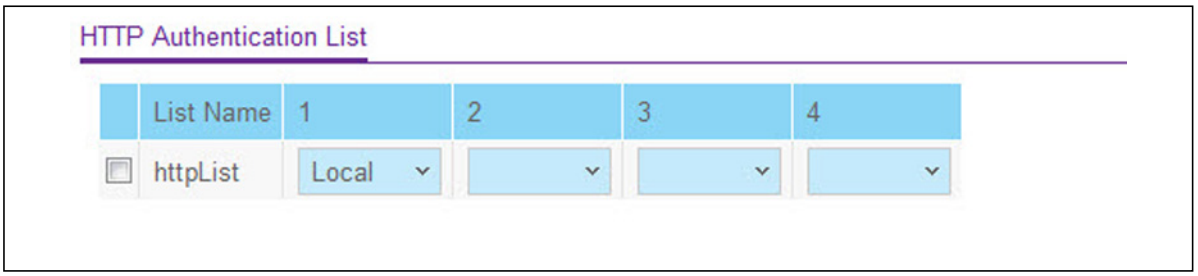


1. **List Name** - Select the dot1x list name for which you want to configure data.
2. Use the menu to select the method that should appear first in the selected authentication login list. The options are:
   - **IAS**- The user's ID and password in Internal Authentication Server Database will be used for authentication.
   - **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 authenticate without a user name and password

HTTP Authentication List

You use this page to configure a HTTP list. A HTTP list specifies the authentication method(s) you want to use to validate the switch or port access through HTTP.

To display the HTTP Authentication List page, click **Security** > **Management Security > Authentication List** > **HTTP Authentication List**.



1. **List Name** - Select the HTTP list name for which you want to configure data.
2. Use the 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.
   - **None** - The user will not be authenticated.
   - **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.

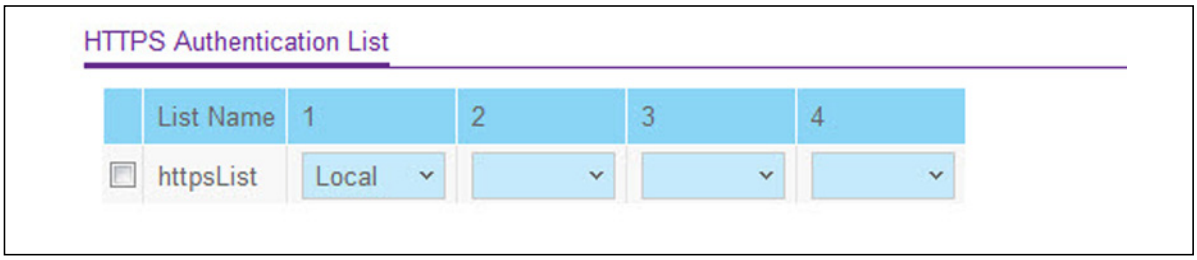
3. Use the menu to select the method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. Note that this parameter will not appear when you first create a new login list.
4. Use the 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 a HTTPS list. A login list specifies the authentication method(s) you want to use to validate the switch or port access through HTTPS for the users associated with the list.

The default list is: httpsList.

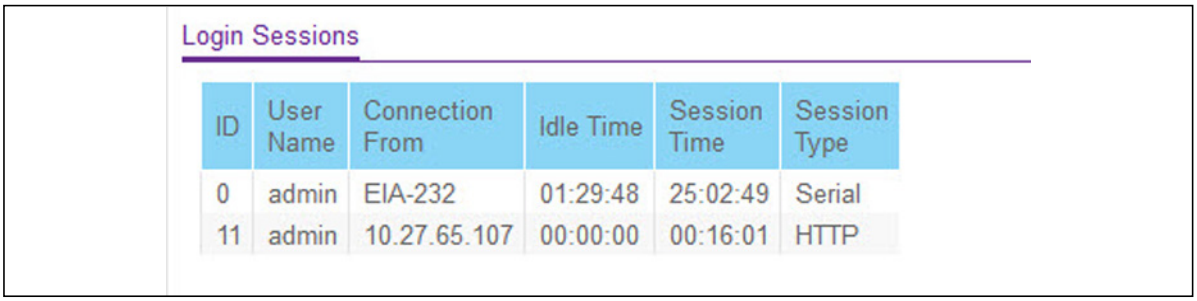
To display the HTTPS Authentication List page, click **Security** > **Management Security > Authentication List** > **HTTPS Authentication List**.



1. **List Name** - Select the HTTPS list name for which you want to configure data.
2. Use the 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 name and password will be used for authentication.
   - **None**- The user will not be authenticated.
   - **RADIUS**- The user's name and password will be authenticated using the RADIUS server instead of local authentication.
   - **TACACS**- The user will authenticate without a username and password.
3. Use the 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 menu to select the method, if any, that should appear third in the selected authentication login list. This is the method that will be used if all previous methods time out. If you select a method that does not time out as the third method, the fourth method will not be tried. Note that this parameter will not appear when you first create a new login list.
5. Use the menu to select the method, if any, that should appear fourth in the selected authentication login list. This is the method that will be used if all previous methods time out. Note that this parameter will not appear when you first create a new login list.

Login Sessions

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



Field	Description
ID	Identifies the ID of this row.
User Name	Shows the user's name whose session is open.
Connection From	Shows from which machine the user is connected.
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 tab, you can configure HTTP and Secure HTTP access to the ProSafe ® Managed switch's management interface.

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

- *HTTP* on page 411
- *HTTPS* on page 413
- *SSH* on page 416
- *Telnet* on page 419
- *Console Port* on page 421
- *Denial of Service Configuration* on page 422
- *Access Control* on page 424

HTTP

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

- *HTTP Configuration* on page 412

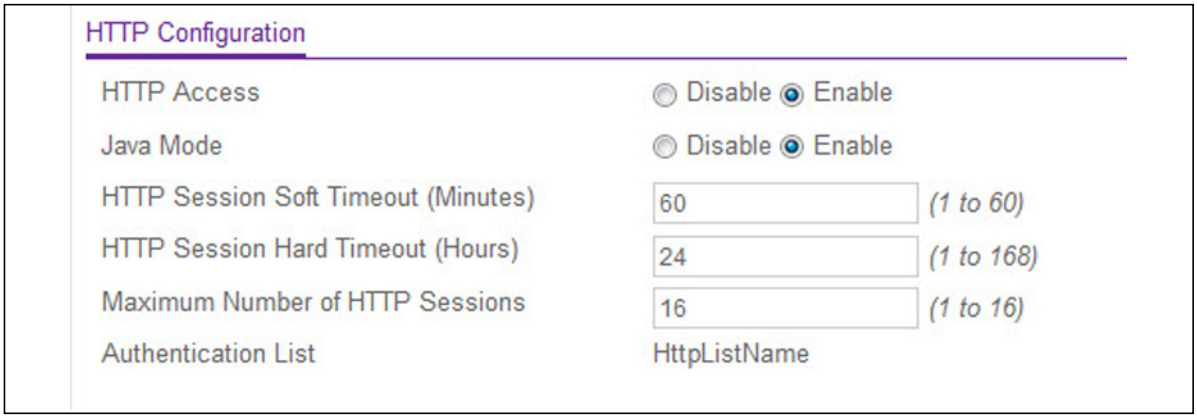
HTTP Configuration

To access the switch over a web page, 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 in the Device view tab of the System tab. 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 on the left side of the screen. The factory default is Enable.
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 is using.

HTTPS

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

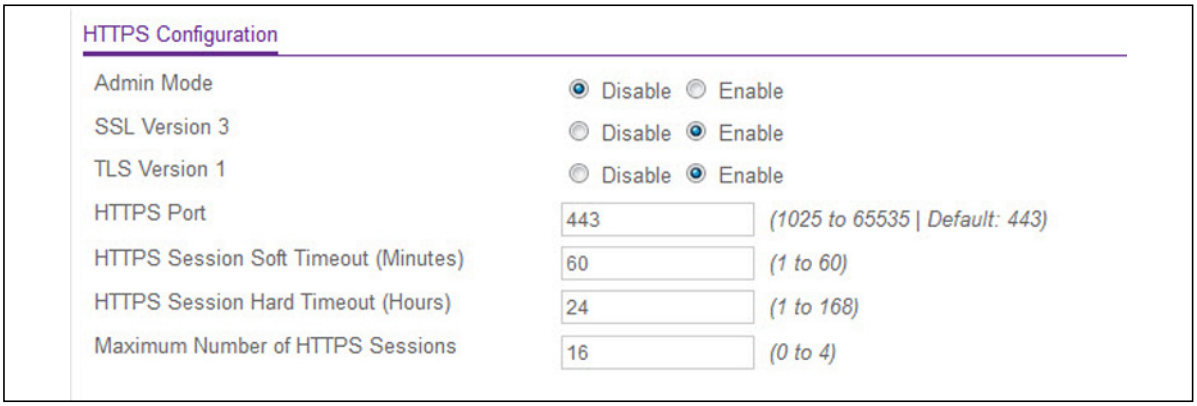
- *HTTPS Configuration* on page 413
- *Certificate Management* on page 414
- *Certificate Download* on page 415

HTTPS Configuration

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

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

To display the Secure HTTP Configuration page, click **Security** > **Access > HTTPS** > **HTTPS Configuration**.



To configure HTTPS settings:

1. Use **HTTPS Admin Mode** to Enable or Disable the Administrative Mode of Secure HTTP. The currently configured value is shown when the web page is displayed. The default value is Disable. You can only download SSL certificates when the HTTPS Admin mode is disabled. HTTPS Admin Mode can be enabled only if a Certificate is present on the device.
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.

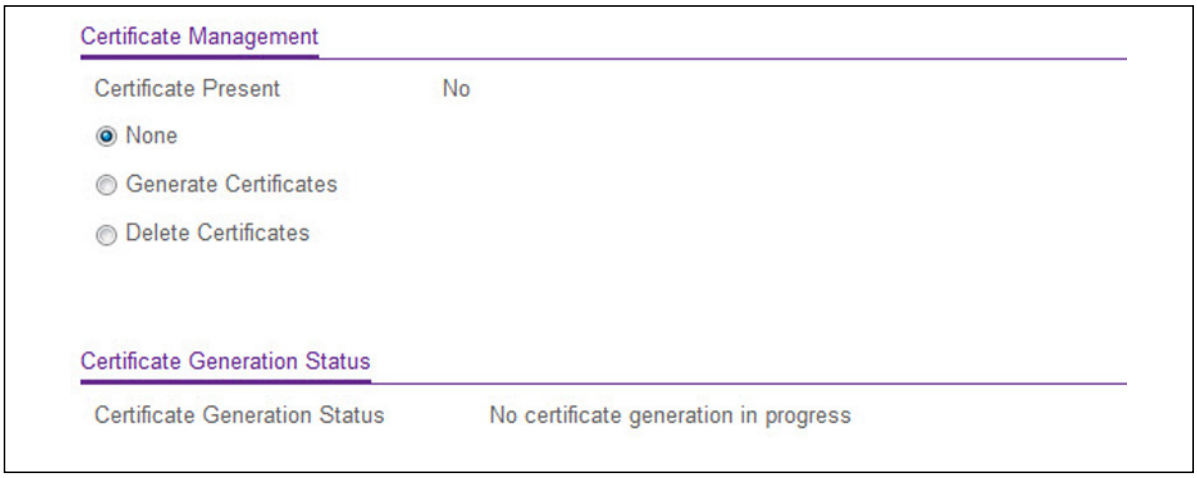
3. Use **TLS Version 1** to Enable or Disable Transport Layer Security Version 1.0. The currently configured value is shown when the web page is displayed. The default value is Enable.
4. Use **HTTPS Port** to set the HTTPS Port Number. The value must be in the range of 1025 to 65535. Port 443 is the 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 5minutes. 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
Authentication List	Displays authentication list for HTTPS.

Certificate Management

Use this page to generate or delete certificates.

To display the Certificate Management page, click **Security** > **Access > HTTPS** > **Certificate Management**.



1. Use **None** when there is nothing to be done with respect to 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 Present	Displays whether there is a certificate present on the device.
Certificate Generation Status	Displays the SSL certificate generation status.

Certificate Download

Use this page to transfer a certificate file to the switch.

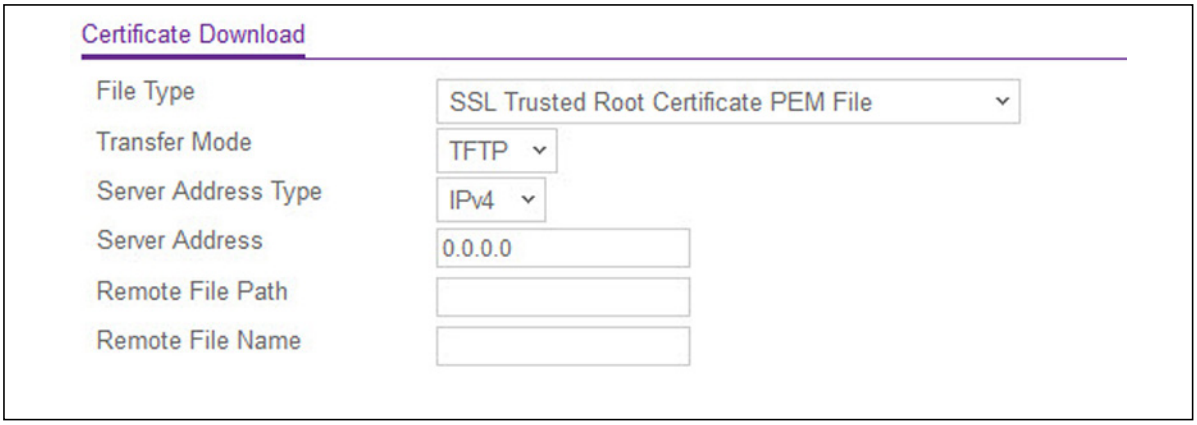
For the Web server on the switch to accept HTTPS connections from a management station, the Web server needs a public key certificate. You can generate a certificate externally (for example, off-line) and download it to the switch.

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, IPv6, or DNS 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 or DNS hostname 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 Path** to enter the path of the file which you want to download. You may enter up to 96 characters. The factory default is blank.
6. Use **Remote File Name** to enter the name of the file on the TFTP server you want to download. You may enter up to 32 characters. The factory default is blank.

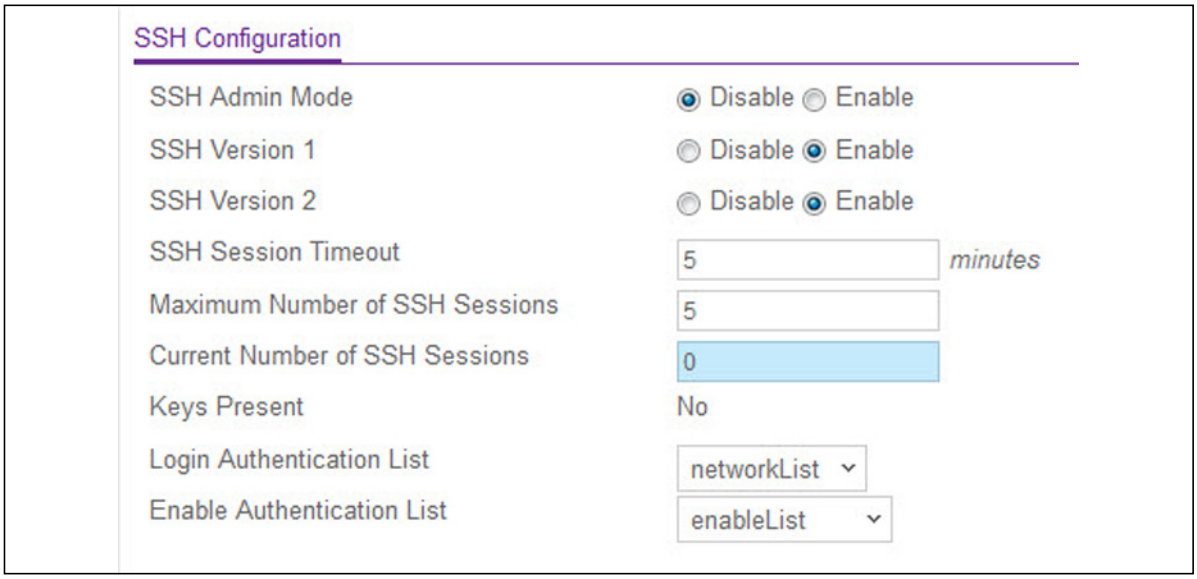
SSH

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

- *SSH Configuration* on page 416
- *Host Keys Management* on page 417
- *Host Keys Download* on page 419

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.

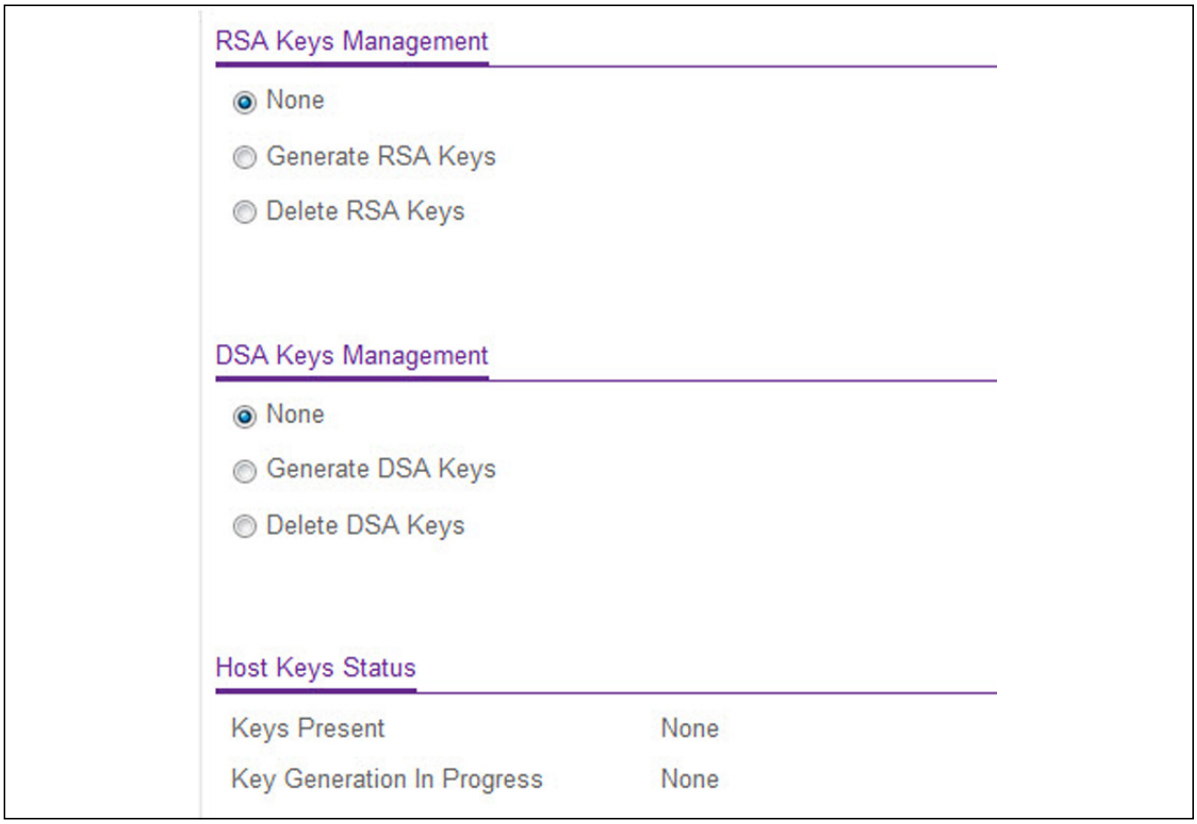
2. Use **SSH Version 1** to Enable or Disable Protocol Level 1 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.
3. Use **SSH Version 2** to Enable or Disable Protocol Level 2 for SSH. The currently configured value is shown when the web page 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 field is (1-5) 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 acceptable range for this field is (0-5).
6. Use **Login Authentication List** to select an authentication list from the menu. This list is used to authenticate users who try to login to the switch.
7. Use **Enable Authentication List** to select an authentication list from the menu. This list is used to authenticate users who try to get “enable” level privilege.
8. Click **Update** to update the page with the latest information on the switch.

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**.



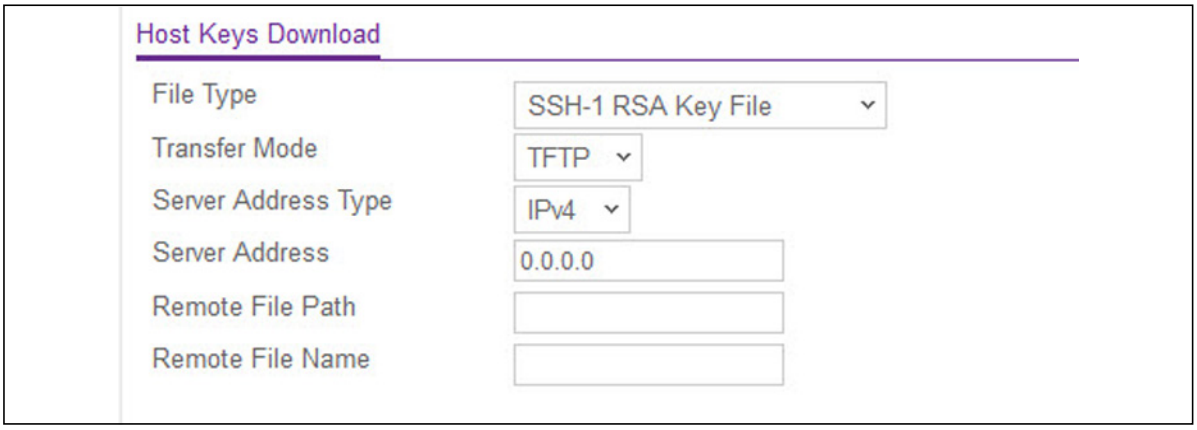
1. **Host Keys Management** - None is the default selection.
2. Use **Generate RSA Keys** to begin generating the RSA host keys. Note that to generate SSH key files SSH must be administratively disabled and there can be no active SSH sessions.
3. Use **Delete RSA Keys** to delete the corresponding RSA 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 downloading 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 **Update** to update the page with the latest information on the switch.

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 page to transfer a file to or from the switch.

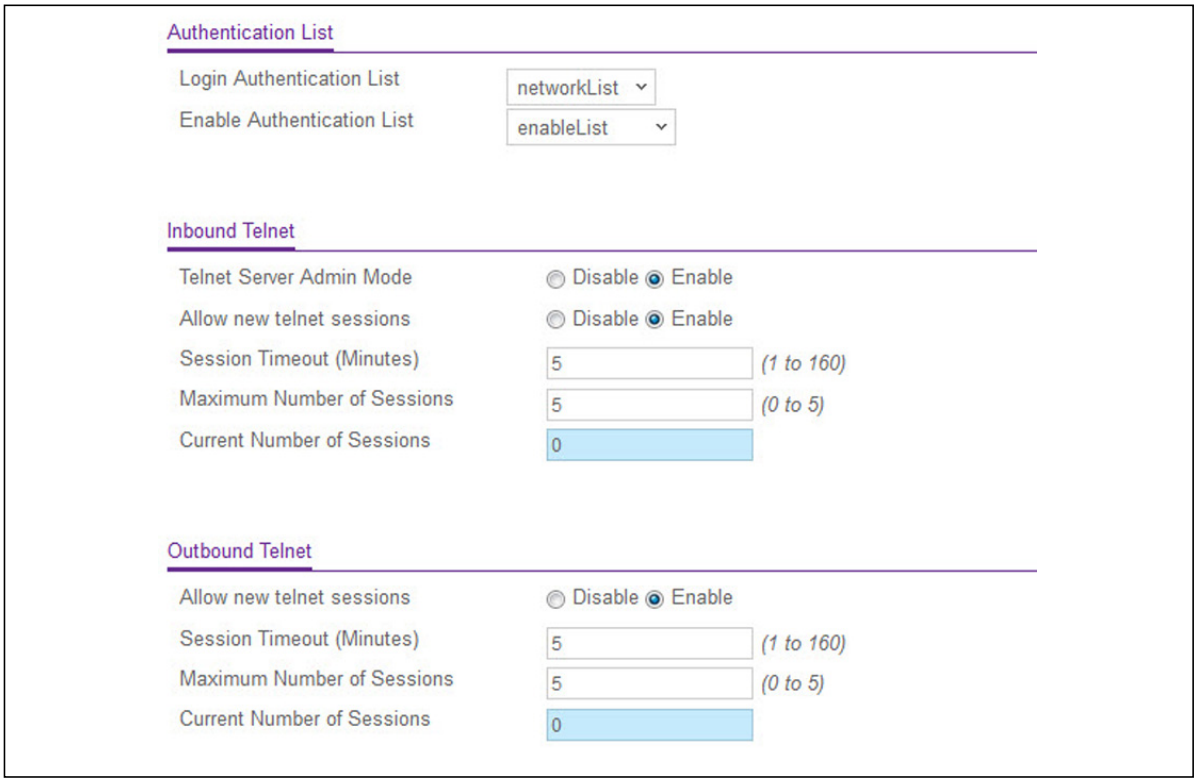
To display the Host Keys Download page, click **Security** > **Access > SSH** > **Host Keys Download**.



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, IPv6, or DNS 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 or DNS hostname 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 Path** to Enter the path of the file which you want to download. You may enter up to 96 characters. The factory default is blank.
6. Use **Remote File Name** to enter the name of the file on the TFTP server you want to download. You may enter up to 32 characters. The factory default is blank.
7. Click **Apply** to start downloading 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**.



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 to use to validate switch or port access for the users associated with the list. The enable list specifies the authentication method(s) you want to use to validate privileged EXEC access for the users associated with the list. These lists can be created through the Authentication List link under Management Security.

1. Use **Login Authentication List** to specify which authentication list to use 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 enableNetList.

Inbound Telnet

This page regulates new telnet sessions. If Allow New Telnet Sessions is enabled, new inbound telnet sessions can be established until there are no more sessions available. If Allow New Telnet Sessions is 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 specify 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.

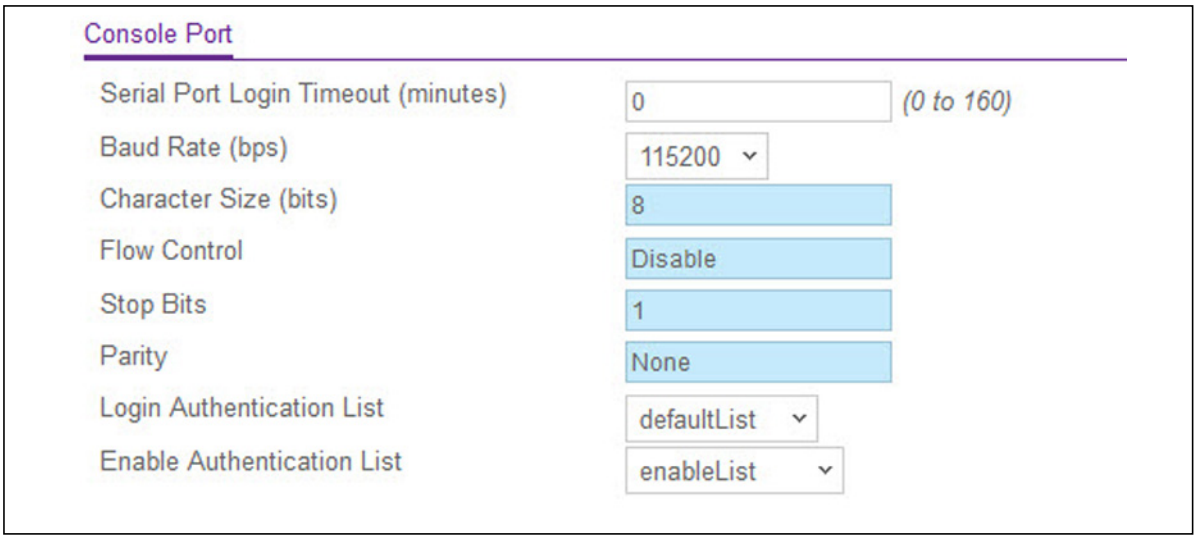
Outbound Telnet

This page regulates new outbound telnet connections. If Allow New Telnet Sessions is enabled, new outbound telnet sessions can be established until there are no more sessions available. If Allow New Telnet Sessions is 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**.



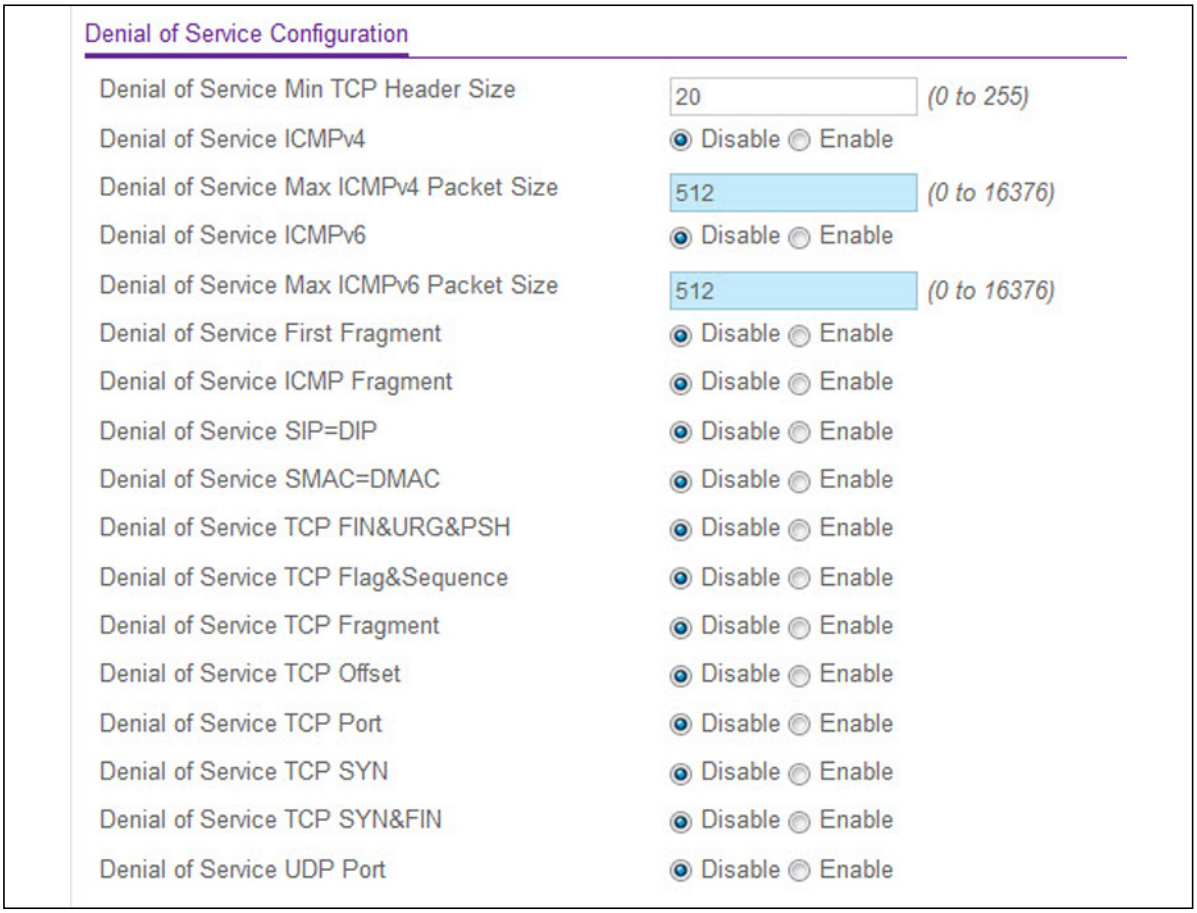
1. Use **Serial Port Login Timeout (minutes)** to specify how many minutes of inactivity should occur on a serial port connection before the switch closes the connection. Enter a number between 0 and 160: the factory default is 5. Entering 0 disables the time-out.

2. Use **Baud Rate (bps)** to select the default baud rate for the serial port connection from the menu. You may choose from 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory default is 115200 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 to use 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 Configuration

To display the Denial of Service page, click **Security** > **Access > Denial of Service Configuration**.



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.
   - Its range is (0 to 255). The default value is 20.
2. Use **Denial of Service ICMPv4** to enable ICMPv4 DoS prevention which causes the switch to drop ICMPv4 packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 Pkt Size. The factory default is disabled.
3. Use **Denial of Service Max ICMPv4 Packet Size** to specify the Max ICMPv4 Pkt Size allowed. If ICMPv4 DoS prevention is enabled, the switch will drop IPv4 ICMP ping packets that have a size greater than this configured Max ICMPv4 Pkt Size. Its range is (0 to 16376). The default value is 512.
4. Use **Denial of Service ICMPv6** to enable ICMPv6 DoS prevention which causes the switch to drop ICMPv6 packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 Pkt Size. The factory default is disabled.
5. Use **Denial of Service Max ICMPv6 Packet Size** to specify the Max IPv6 ICMP Pkt Size allowed. If ICMPv6 DoS prevention is enabled, the switch will drop IPv6 ICMP ping packets that have a size greater than this configured Max ICMPv6 Pkt Size. Its range is (0 to 16376). The default value is 512.

6. Use **Denial of Service First Fragment** to enable First Fragment DoS prevention which causes 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.
7. Use **Denial of Service ICMP Fragment** to enabling ICMP Fragment DoS prevention which causes the switch to drop ICMP Fragmented packets. The factory default is disabled.
8. Use **Denial of Service SIP=DIP** to enable SIP=DIP DoS prevention which causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
9. Use **Denial of Service SMAC=DMAC** to enable SMAC=DMAC DoS prevention which causes the switch to drop packets that have a source MAC address equal to the destination MAC address. The factory default is disabled.
10. Use **Denial of Service TCP FIN&URG&PSH** to enable TCP FIN & URG & PSH DoS prevention which causes the switch to drop packets that have TCP Flags FIN, URG, and PSH set and TCP Sequence Number=0. The factory default is disabled.
11. Use **Denial of Service TCP Flag&Sequence** to enable TCP Flag DoS prevention which causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0. The factory default is disabled.
12. Use **Denial of Service TCP Fragment** to enable TCP Fragment DoS prevention which causes 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.
13. Use **Denial of Service TCP Offset** to enable TCP Offset DoS prevention which causes the switch to drop packets that have a TCP header Offset=1. The factory default is disabled.
14. Use **Denial of Service TCP Port** to enable TCP Port DoS prevention which causes the switch to drop packets that have TCP source port equal to TCP destination port. The factory default is disabled.
15. Use **Denial of Service TCP SYN** to enable TCP SYN DoS prevention which causes the switch to drop packets that have TCP Flags SYN set. The factory default is disabled.
16. Use **Denial of Service TCP SYN&FIN** to enable TCP SYN & FIN DoS prevention which causes the switch to drop packets that have TCP Flags SYN and FIN set. The factory default is disabled.
17. Use **Denial of Service UDP Port** to enable UDP Port DoS prevention which causes the switch to drop packets that have UDP source port equal to UDP destination port. The factory default is disabled.

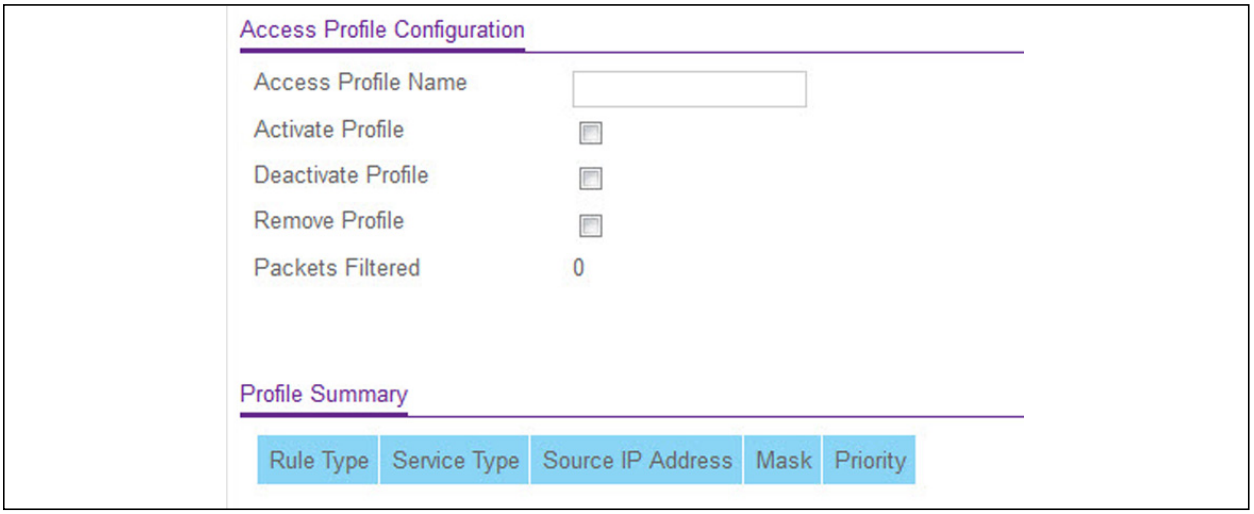
Access Control

From the **Security > Access** link, you can access the following pages that you use to configure and display Access Control data:

- *Access Profile Configuration* on page 425
- *Access Rule Configuration* on page 426

Access Profile Configuration

To display the Access Profile Configuration page, click **Security** > **Access > Access Control > Access Profile Configuration**. The following page is displayed.



- **Configure the Access Profile settings.**

1. In the **Access Profile Name** field, enter the name of the access profile to be added. The maximum length is 32 characters.
2. Select the **Activate Profile** check box to activate an access profile.
3. Select the **Deactivate Profile** check box to deactivate an access profile.
4. Select the **Remove Profile** check box to remove an access profile. The access profile should be deactivated before removing it.
5. The **Packets Filtered** field displays the number of packets filtered.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
8. Click **Update** to update the page with the latest information on the switch.

Profile Summary

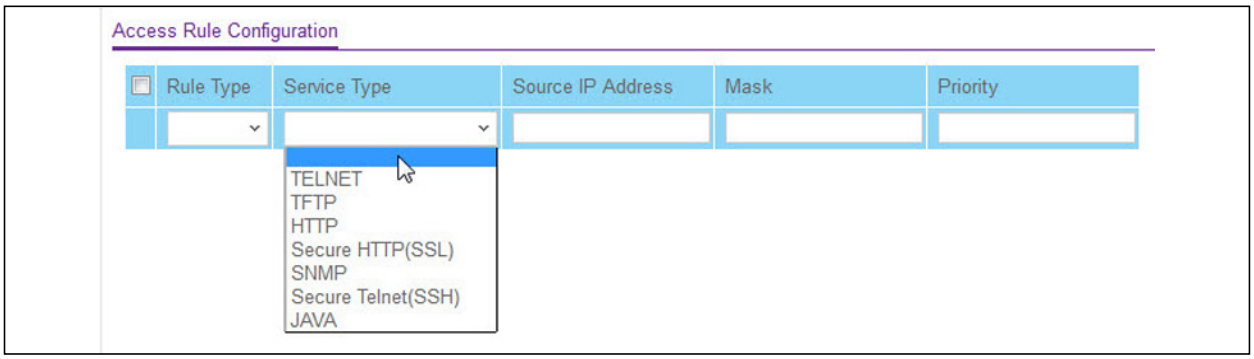
Table 157, Access Profile Configuration Profile Summary describes the non-configurable data that is displayed.

Table 157. Access Profile Configuration Profile Summary

Field	Description
Rule Type	The action performed when the rules are matched.
Service Type	The service type chosen. The policy is restricted by the service type chosen.
Source IP Address	Source IP address of the client originating the management traffic.
Mask	The subnet mask of the IP Address.
Priority	The priority of the rule.

Access Rule Configuration

To display the Access Rule Configuration page, click **Security** > **Access > Access Control > Access Rule Configuration**. The following page is displayed.



➢ **Configure the Access Rule Configuration settings.**

1. From the **Rule Type** list, select to either Permit or Deny access when the rules selected are matched.
2. The policy is restricted by the **Service Type** you select from the list. Possible management methods are:
   - HTTP
   - JAVA
   - Secure HTTP (SSL)
   - Secure Telnet (SSH)
   - SNMP
   - Telnet
   - TFTP
3. Enter the **Source IP Address** of the client originating the management traffic.
4. Enter the Source IP Address **Mask** of the client originating the management traffic.
5. Configure the **Priority** to the rule. The rules are validated against the incoming management request in ascending order of their priorities. If a rule matches, the action is performed and

subsequent rules below that are ignored. For example, if a Source IP 10.10.10.10 is configured with priority 1 to permit, and Source IP 10.10.10.10 is configured with priority 2 to Deny, then access is permitted if the profile is active, and the second rule is ignored.

6. Click **Add** to add a new access rule. Make sure that the access profile is created before adding the rules.
7. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
8. Changes can be applied to the access rule only when the access profile is in deactive state.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. Click **Delete** to delete the selected access rule.

Note: If the access profile is active, then the access rule cannot be deleted. Make sure that the access profile is in deactive state before removing the access rule.

Port Authentication

In port-based authentication, 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 page, you can access the following pages:

- *Basic* on page 427
- *Advanced* on page 429

Basic

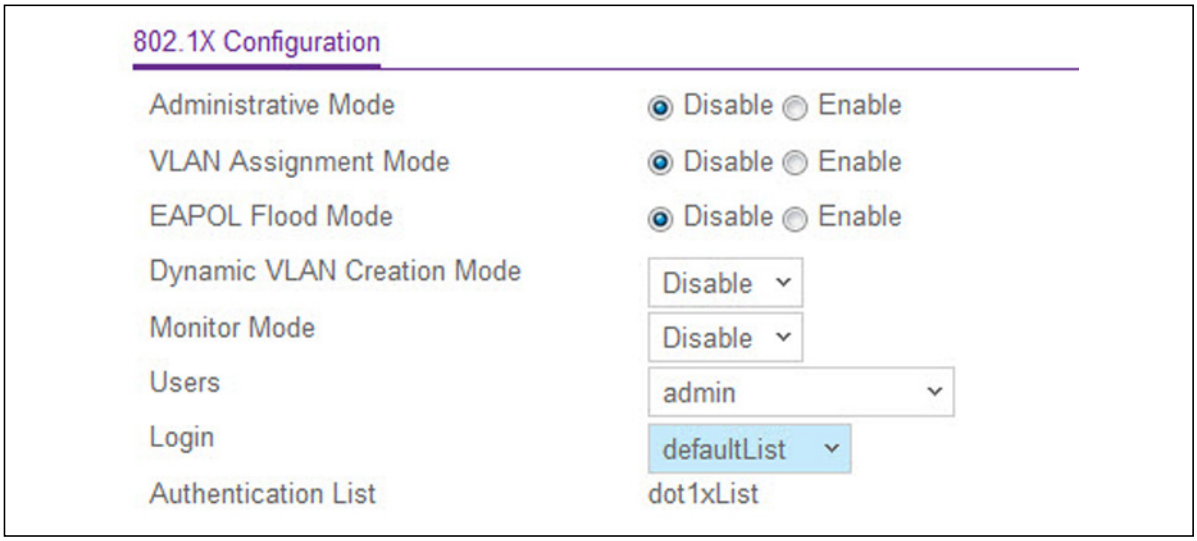
From the Basic link, you can access the following pages:

- *802.1X Configuration* on page 428

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 **Administrative Mode** 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 6-406.

   - **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 the options for VLAN Assignment mode: enable and disable. The default value is disable.
3. Use **EAPOL Flood Mode** to select one of the options for the EAPOL Flood Mode: enable or disable. The default value is disable.
4. Use **Dynamic VLAN Creation Mode** to select one of the options: enable or disable. The default value is disable.

5. Use **Monitor Mode** to select one of the options for Monitor mode: enable or disable. The default value is Disable. The feature monitors the dot1x authentication process and helps in diagnosis of the authentication failure cases.
6. Use **Users** to select the user name that will use the selected login list for 802.1x port security.
7. Use **Login** to select the login list to apply to the specified user. All configured login lists are displayed.

Field	Description
Authentication List	Displays the authentication list which is used by 802.1X.

Advanced

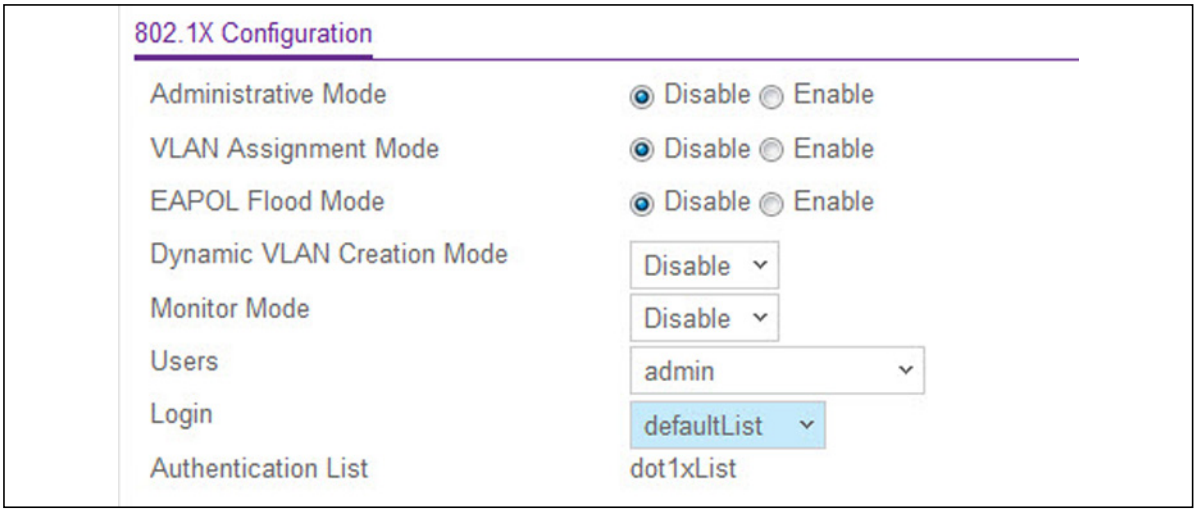
From the Advanced link, you can access the following pages:

- *802.1X Configuration* on page 429
- *Port Authentication* on page 430
- *Port Summary* on page 433
- *Client Summary* on page 435

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 or disable. The default value is disable.
2. Use **VLAN Assignment Mode** to select one of the options for VLAN Assignment mode: enable or disable. The default value is disable.

3. Use **EAPOL Flood Mode** to select one of the options for the EAPOL Flood Mode: enable or disable. The default value is disable.
4. Use **Dynamic VLAN Creation Mode** to select one of the options: enable or disable. The default value is disable.
5. Use **Monitor Mode** to select one of the options for Monitor mode: enable or disable. The default value is Disable. The feature monitors the dot1x authentication process and helps in diagnosis of the authentication failure cases.
6. Use **Users** to select the user name that will use the selected login list for 802.1x port security.
7. Use **Login** to select the login list to apply to the specified user. All configured login lists are displayed.

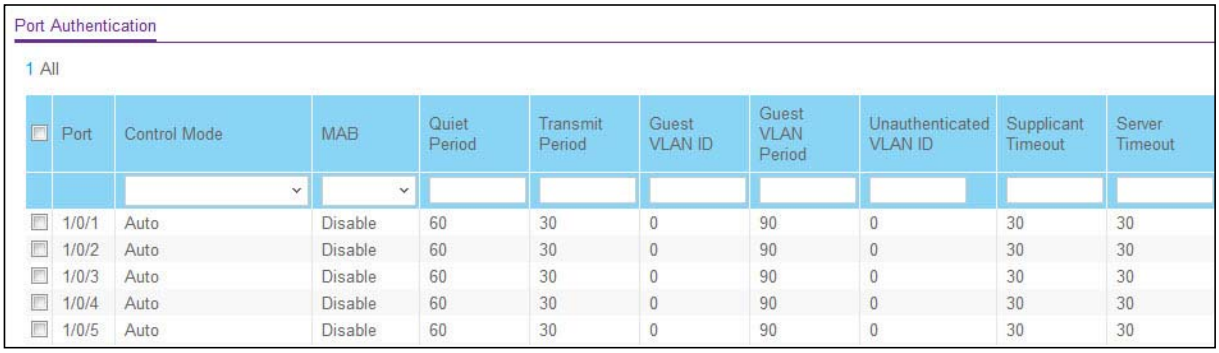
Field	Description
Authentication List	Displays the authentication list which is used by 802.1X.

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.



To configure 802.1X settings for the port:

1. Select the check box next to the port to configure. You can also select multiple check boxes to apply the same settings to the selected ports, or select the check box in the heading row to apply the same settings to all ports.
2. For the selected port(s), specify the following settings:

- **Control Mode** - This selector lists the options for control mode. The control mode is only set if the link status of the port is link up. The options are:
  - **force unauthorized** - The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized
  - **force authorized** - The authenticator PAE unconditionally sets the controlled port to authorized.
  - **auto** - The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.
  - **mac based** - The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.
  - **N/A** - The control mode is not applicable.
- Use **MAB** to enable or disable MAC Based. The default selection is Disable. 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 0-4093.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 0-4093.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.

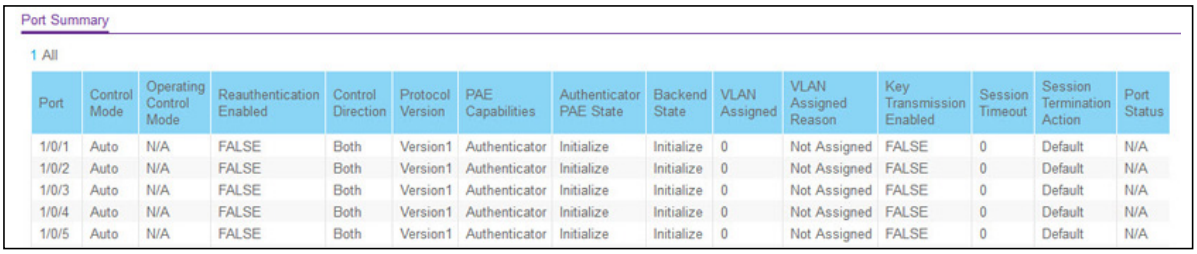
- **Supplicant Timeout** - This input field allows the user to enter the supplicant time-out for the selected port. The supplicant time-out is the value, in seconds, of the timer used by the authenticator state machine on this port to time-out the supplicant. The supplicant time-out must be a value in 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 'enable or disable'. If the value is 'enable' reauthentication will occur. Otherwise, reauthentication will not be allowed. The default value is disable. Changing the selection will not change the configuration until the Apply button is pressed.
- **Reauthentication Period** - 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 **Reauthentication** 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**.



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

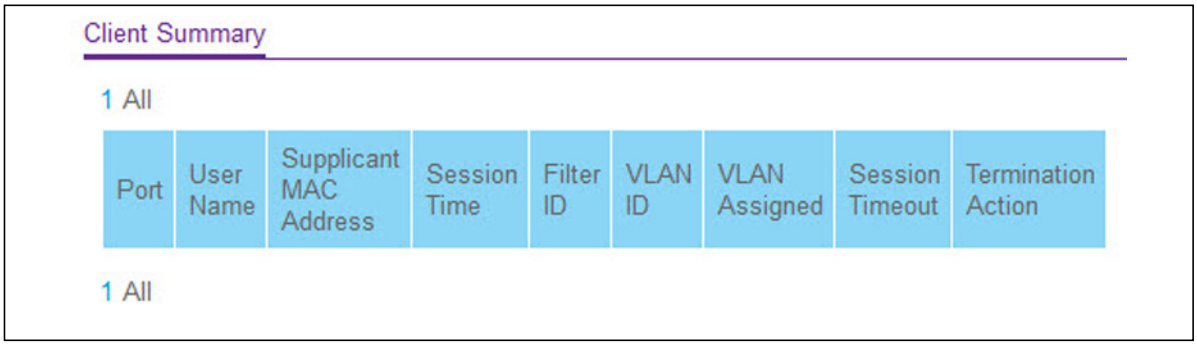
Field	Description
Port	Specifies the port whose settings are displayed in the current table row.
Control Mode	This field indicates the configured control mode for the port. Possible values are: • Force Unauthorized: The authenticator port access entity (PAE) unconditionally sets the controlled port to 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 authentication exchanges between a supplicant, an authenticator, and an authentication server on a per supplicant basis.
Operating Control Mode	This field indicates the control mode under which the port is actually operating. Possible values are: • ForceUnauthorized • ForceAuthorized • Auto • MAC Based • N/A: If the port is in detached state it cannot participate in port access control.

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: • “Initialize” • “Disconnected” • “Connecting” • “Authenticating” • “Authenticated” • “Aborting” • “Held” • “ForceAuthorized” • “ForceUnauthorized”.
Backend State	This field displays the current state of the backend authentication state machine. Possible values are: • “Request” • “Response” • “Success” • “Fail” • “Timeout” • “Initialize” • “Idle”

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: • “Radius” • “Unauth” • “Default” • “Not Assigned”
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: • “Default” • “Reauthenticate” 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.

Client Summary

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



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** tab, 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 tab contains links to the following features:

- *MAC Filter* on page 437
- *Port Security* on page 439
- *Private Group* on page 442
- *Protected Ports Configuration* on page 444
- *Private VLAN* on page 444

- *Storm Control* on page 448

MAC Filter

The MAC Filter link contains links to the following pages:

- *MAC Filter* on page 437
- *MAC Filter Summary* on page 438

MAC Filter

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. Use **Source Port Members** to list the ports you want included in the inbound filter. If a packet with the MAC address and VLAN ID you selected is received on a port that is not in the list, it will be dropped.

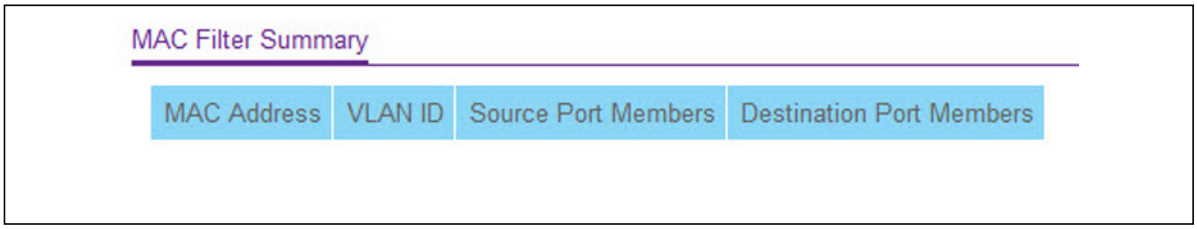
e. Use **Destination Port Members** to list the ports you want to be included in the outbound filter. Packets with the MAC address and VLAN ID you selected will only be transmitted out of ports that are in the list. Destination ports can be included only in the Multicast filter.

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

MAC Filter Summary

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

To display the MAC Filter Summary page, 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.
Destination Port Members	A list of ports to be used for filtering outbound packets.

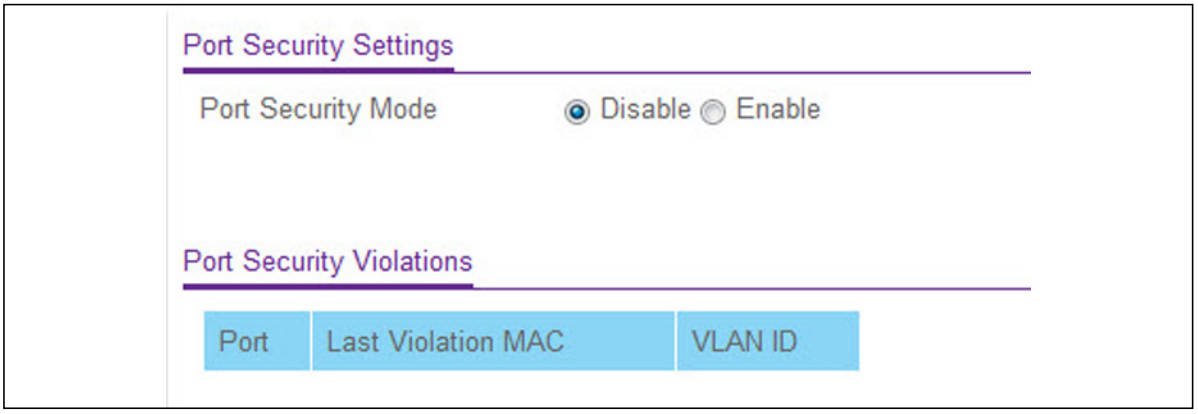
Port Security

The Port Security link contains links to the following pages:

Port Security Administration

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 violations 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 violations 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.

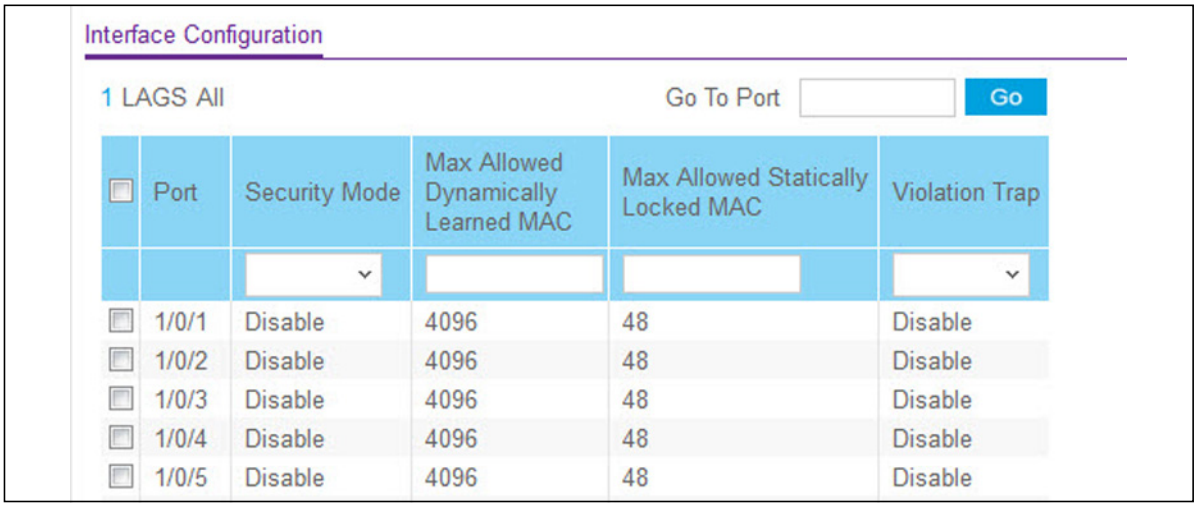
Interface Configuration

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.**



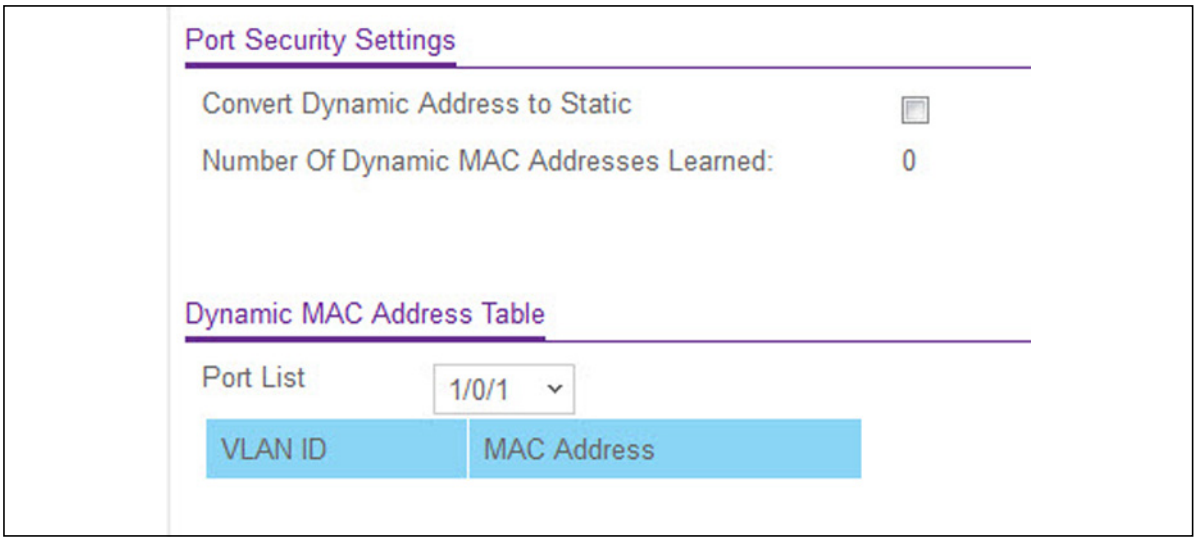
To configure port security settings:

1. **Port** - Selects the interface to be configured.
2. Select the check box next to the port or LAG to configure. Select multiple check boxes to apply the same setting to all selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
3. Specify the following settings:
   - **Security Mode** - Enables or disables the Port Security feature for the selected interface.
   - **Max Allowed Dynamically Learned MAC** - Sets the maximum number of dynamically learned MAC addresses on the selected interface.
   - **Max Allowed Statically Locked MAC** - Sets the maximum number of statically locked MAC addresses on the selected interface.
   - **Violation Traps** - Enables or disables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

Dynamic MAC Address

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

To display the Dynamic MAC Address page, click **Security** > **Traffic Control> Port Security** > **Dynamic MAC Address.**



To convert learned MAC addresses:

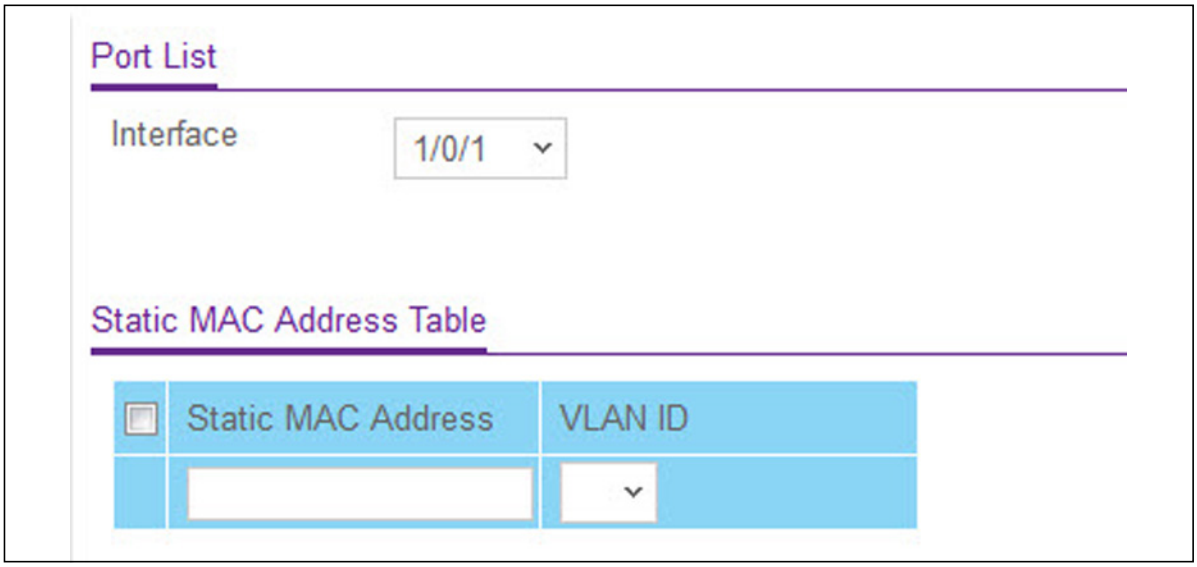
1. **Port List** - Select the physical interface for which you want to display data.
2. Use **Convert Dynamic Address to Static** to convert a dynamically learned MAC address to a statically locked address. The Dynamic MAC address entries are converted to Static MAC address entries in a numerically ascending order until the Static limit is reached.
3. Click **Update** to update the page with the latest information on the switch.

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.**



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 added.
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.

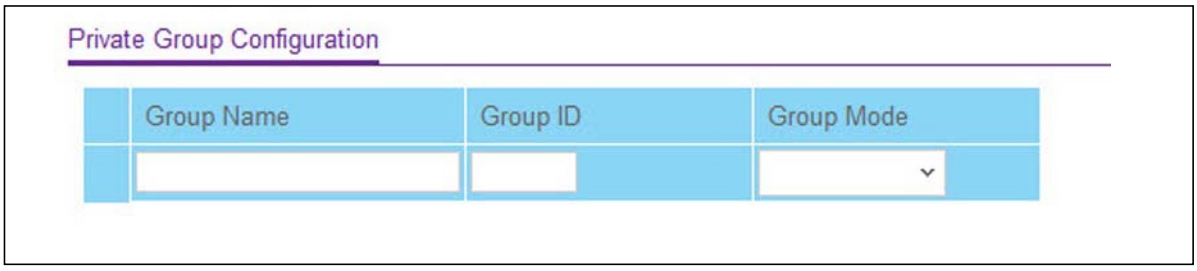
Private Group

The Private Group link contains links to the following pages:

- *Private Group Configuration* on page 442
- *Private Group Membership* on page 443

Private Group Configuration

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

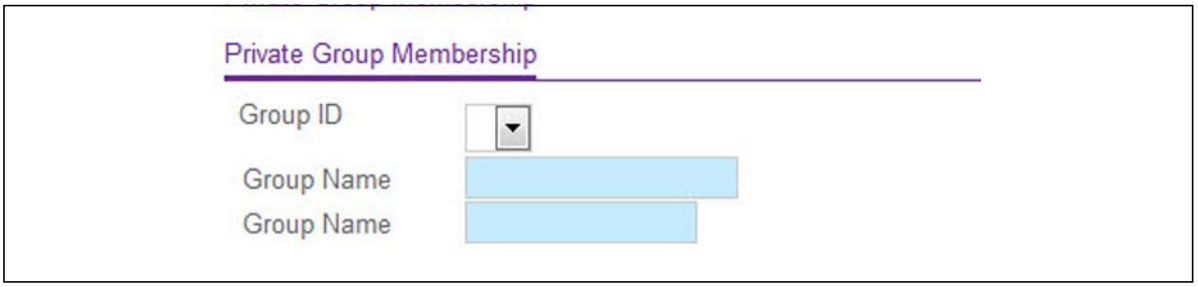


1. Use **Group Name** to enter the Private Group name to be configured. The name string can be up to 24 bytes of non-blank characters.
2. Use the optional **Group ID** field to specify the private group identifier. The range of group id is (1 to 192).

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.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of 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. The port list shows up when at least one group is configured.

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: • **community** • **isolated** 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.

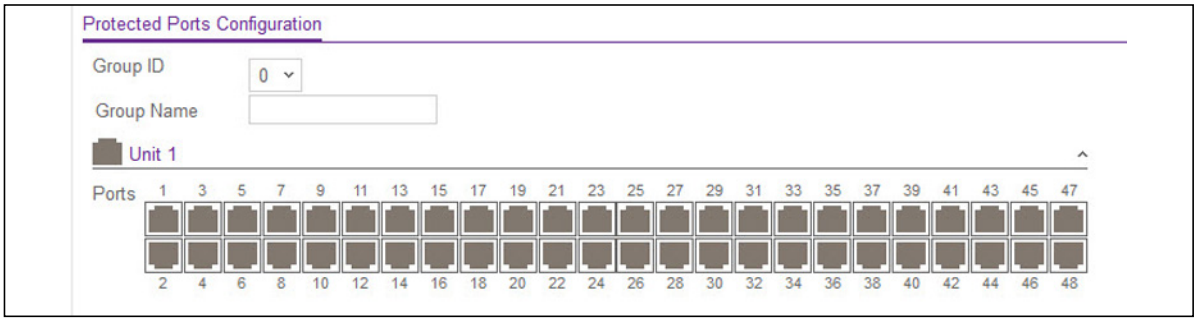
Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

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

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.
5. Click **Update** to update the page with the latest information on 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.

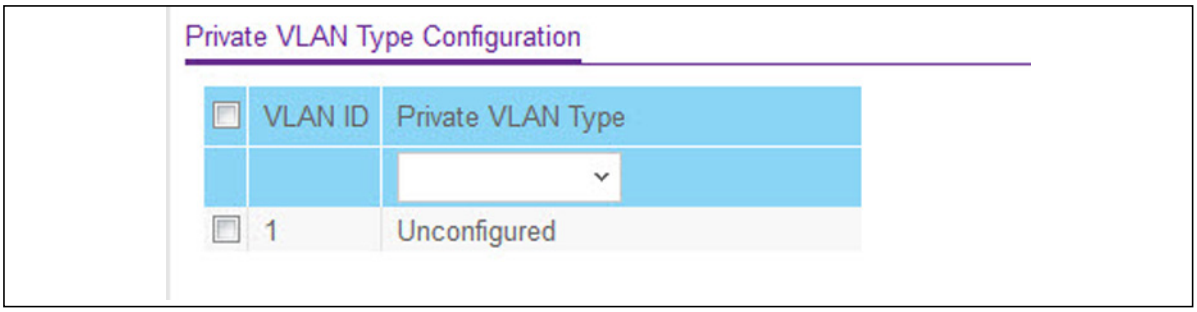
Private VLAN

A private VLAN contains switch ports that cannot communicate with each other, but can access another network. These ports are called private ports. Each private VLAN contains one or more private ports and a single uplink port or uplink aggregation group. Note that all traffic between private ports is blocked at all layers, not just Layer 2 traffic, but also traffic such as FTP, HTTP, and Telnet.

The Private VLAN link contains links to the following pages:

Private VLAN Type Configuration

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

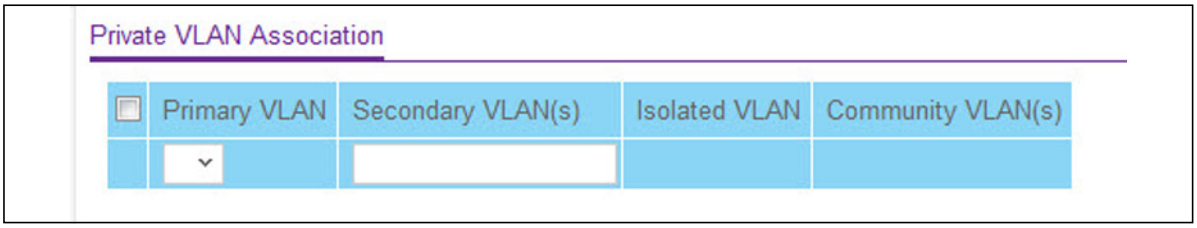


1. Use **Private VLAN Type** to specify the type of Private VLAN. The factory default is 'Unconfigured'.
2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

Field	Description
VLAN ID	Specifies the VLAN ID for which Private VLAN type is being set. The factory default is 'Unconfigured'.

Private VLAN Association Configuration

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



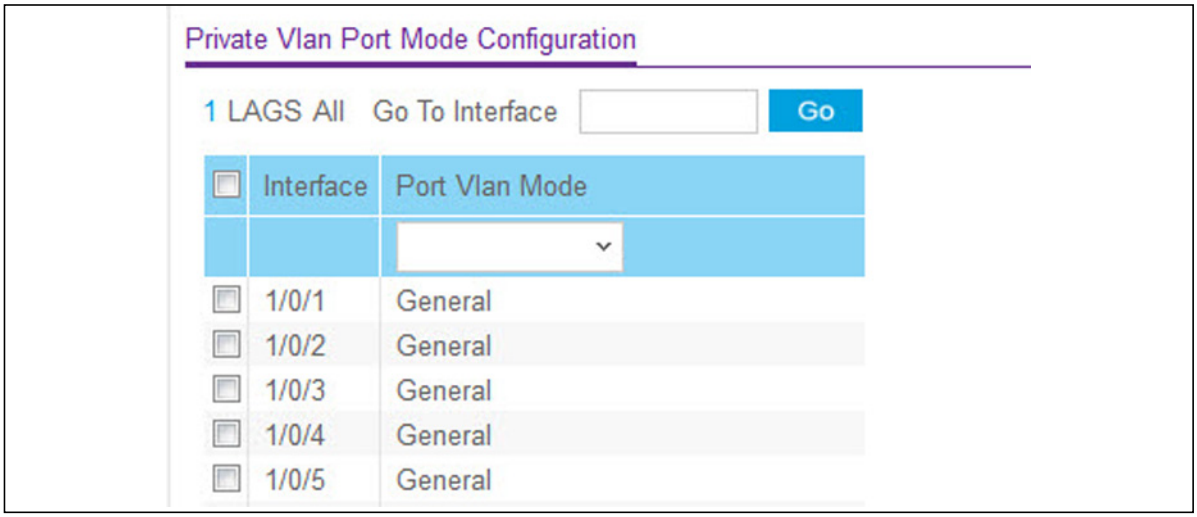
1. Use **Primary VLAN** to select the primary VLAN ID of the domain. This is used to associate Secondary VLANs to the domain.

2. Use **Secondary VLAN(s)** to display all the statically created VLANs (excluding the primary and default VLANs). This control is used to associate VLANs to the selected primary VLAN.
3. Click **Delete** to delete the IP subnet-based VLAN from the switch.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

Field	Description
Isolated VLAN	Displays the isolated VLAN associated with the selected primary VLAN.
Community VLAN(s)	Displays the list of community VLAN(s) associated with the selected primary VLAN.

Private VLAN Port Mode Configuration

To display the Private VLAN Port Mode Configuration page, click **Security** > **Traffic Control> Private VLAN > Private VLAN Port Mode Configuration.**



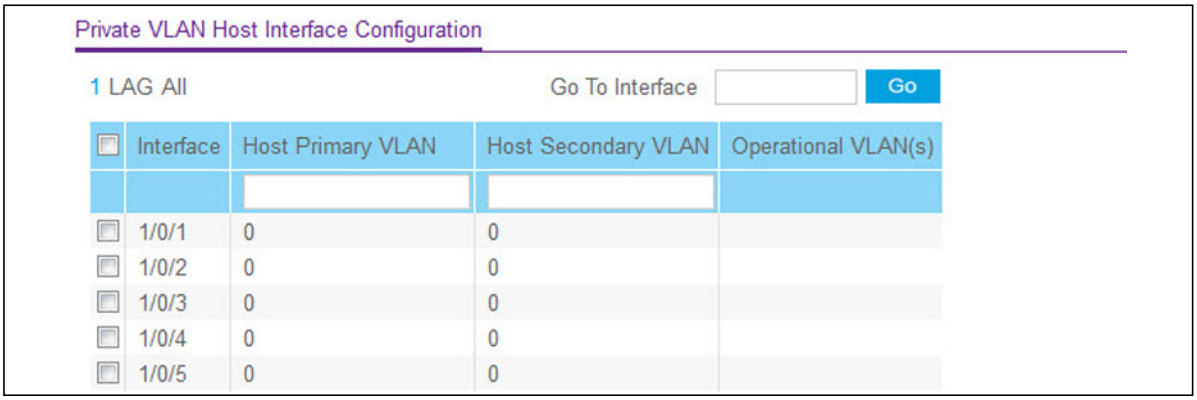
1. Use **Switch Port Mode** to select the Switch Port Mode. The factory default is 'General'.
   - **General**: Sets port in General Mode.
   - **Host**: Sets port in Host Mode. Used for Private VLAN configuration.
   - **Promiscuous**: Sets port in Promiscuous Mode. Used for Private VLAN configuration.
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. Configuration changes take effect immediately.

Field	Description
Interface	Select the physical or LAG interface for which you want to display or configure data.

Private VLAN Host Interface Configuration

To display the VLAN Host Interface Configuration page, click **Security** > **Traffic Control> Private VLAN > Private VLAN Host Interface Configuration.**

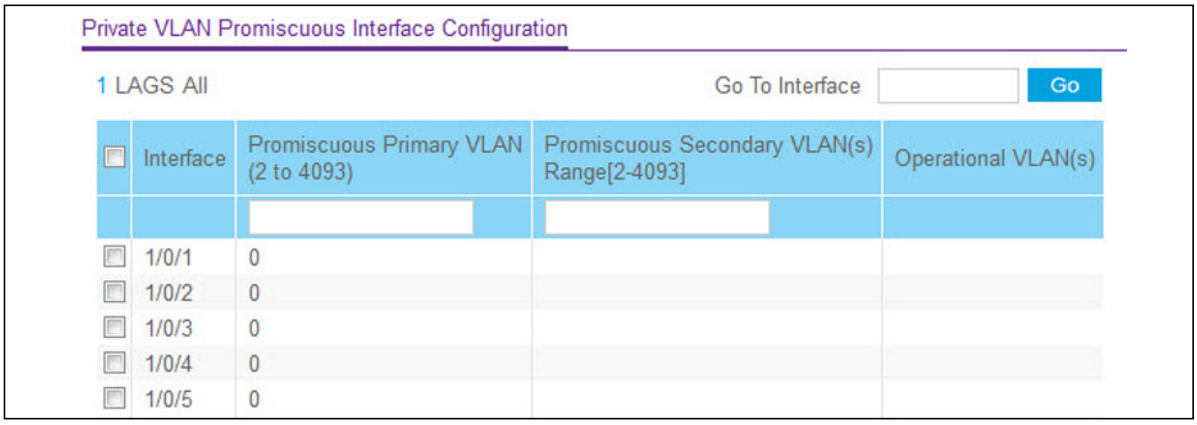


1. Use **Host Primary VLAN** to set the Primary VLAN ID for Host Association Mode. The range of the VLAN ID is 2-4093.
2. Use **Host Secondary VLAN** to set the Secondary VLAN ID for Host Association Mode. The range of the VLAN ID is 2-4093.
3. Click **Delete** to delete the IP subnet-based VLAN from the switch.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

Field	Description
Interface	Select the physical or LAG interface for which you want to display or configure data.
Operational VLAN(s)	Displays the operational VLAN(s).

Private VLAN Promiscuous Interface Configuration

To display the Private VLAN Promiscuous Interface Configuration page, click **Security** > **Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration.**



1. Use **Promiscuous Primary VLAN** to set the Primary VLAN ID for Promiscuous Association Mode. The range of the VLAN ID is 2-4093.
2. Use **Promiscuous Secondary VLAN ID(s)** to set the Secondary VLAN ID List for Promiscuous Association Mode. This field can accept single VLAN ID or range of VLAN IDs or a combination of both in sequence separated by ','. You can specify individual VLAN ID. Eg: 10 You can specify the VLAN range values separated by a '-'. E.g. 10-13 You can specify the combination of both separated by ','. Eg: 12,15,40-43,1000-1005,2000 The range of the VLAN ID is 2-4093.

   Note: The VLAN ID List given in this control will replace the configured Secondary VLAN list in the association.

3. Click **Delete** to delete the IP subnet-based VLAN from the switch.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

Field	Description
Interface	Select the physical or LAG interface for which you want to display or configure data.
Operational VLAN(s)	Displays the operational VLAN(s).

Storm Control

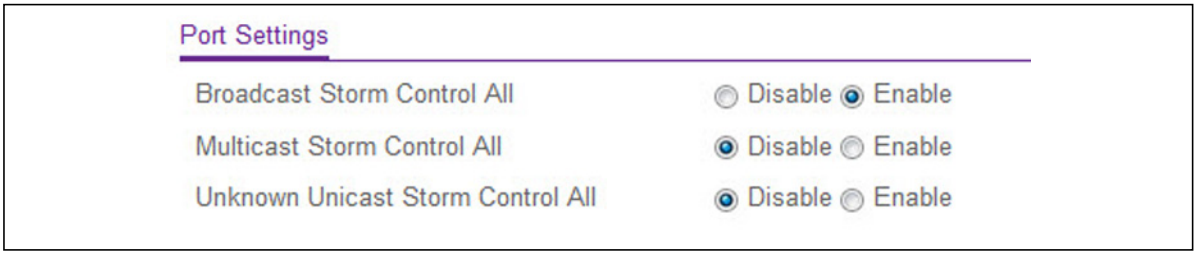
A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources and/or cause the network to time out.

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 link contains links to the following pages:

Storm Control Global Configuration

To display the Storm Control Global Configuration page, click **Security** > **Traffic Control> Storm Control** > **Storm Control Global Configuration.**

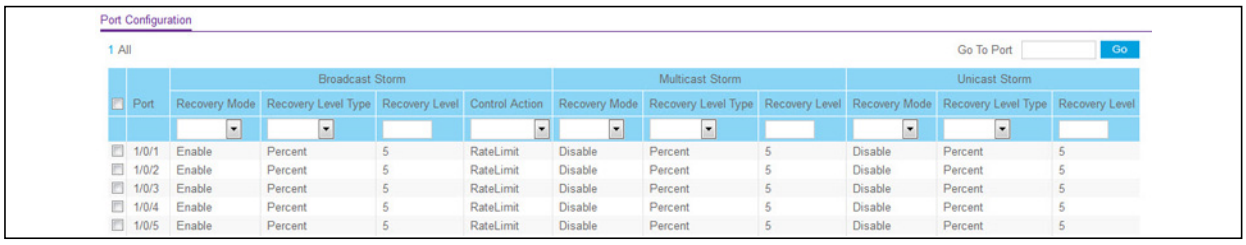


The following three controls provide an easy way to enable or disable each type of packets to be rate-limited on every port in a global fashion. The effective storm control state of each port can be viewed by going to the port configuration page.

- **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.**



Field	Description
Broadcast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the drop-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 enable.
Broadcast Storm Recovery Level Type	Specify the Broadcast Storm Recovery Level as a percentage of link speed or as packets 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.
Broadcast Storm Control Action	Provides configurability to shut down the port when the configured threshold of the broadcast storm recovery feature gets breached. Select the option to either ShutDown or RateLimit mode. The default is RateLimit.
Multicast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the drop-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 packets per second.
Multicast Storm Recovery Level	Specify the threshold at which storm control activates. The factory default is 5 percent of port speed for pps type.
Unicast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the drop-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 packets 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

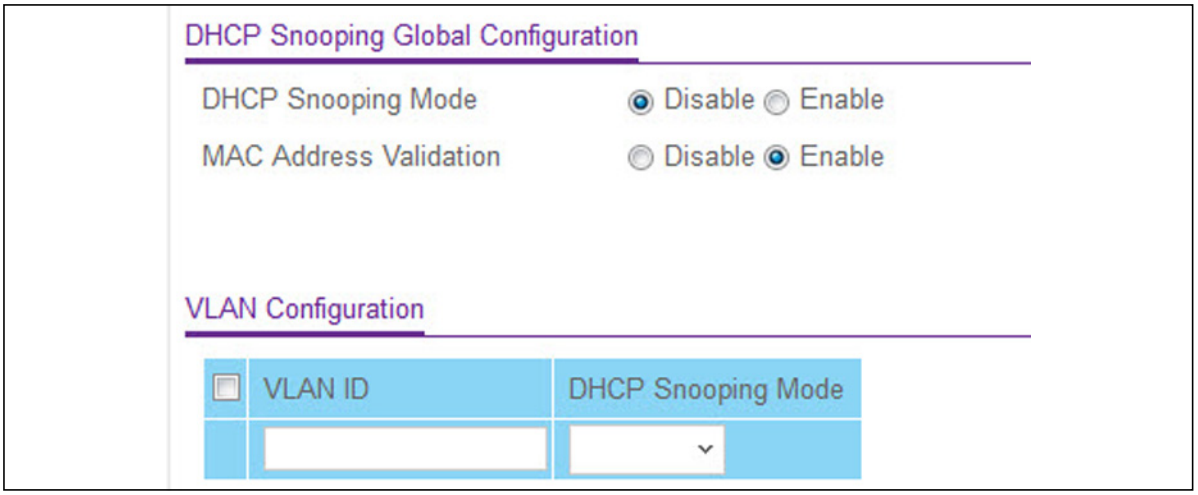
To display the page, click the **Security** > **Control** tab. The Control tab contains links to the following features:

DHCP Snooping

The DHCP Snooping link contains links to the following pages:

DHCP Snooping Global Configuration

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



DHCP Snooping Configuration

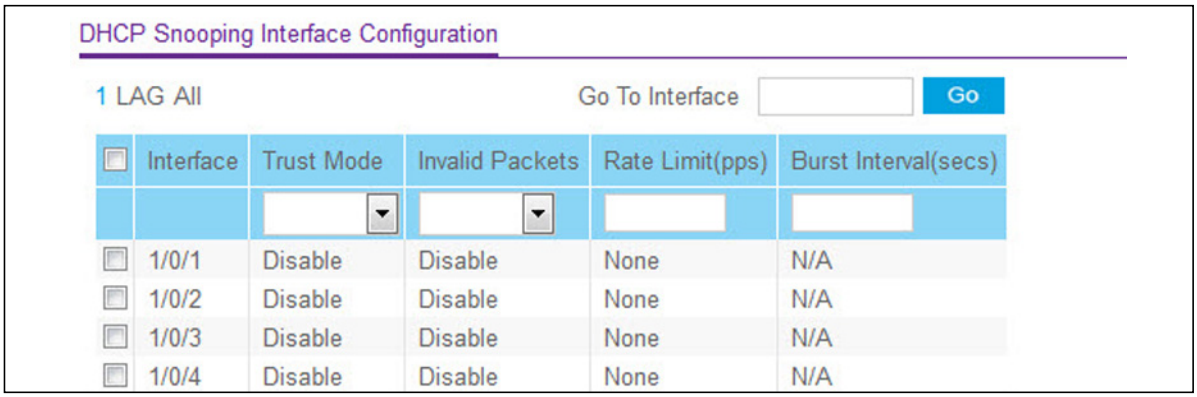
1. Use **DHCP Snooping Mode** to enable or disable the DHCP Snooping feature. The factory default is disabled.
2. Use **MAC Address Validation** to enable or disable the validation of sender MAC Address for DHCP Snooping. The factory default is enabled.

DHCP Snooping VLAN Configuration

1. Use **VLAN ID** to enter the VLAN for which the DHCP Snooping Mode is to be enabled.
2. Use **DHCP Snooping Mode** to enable or disable the DHCP Snooping feature for entered VLAN. The factory default is disabled.
3. Click **Apply** to apply the new configuration and cause the changes to take effect. These changes will not be retained across a power cycle unless a save configuration is performed.

DHCP Snooping Interface Configuration

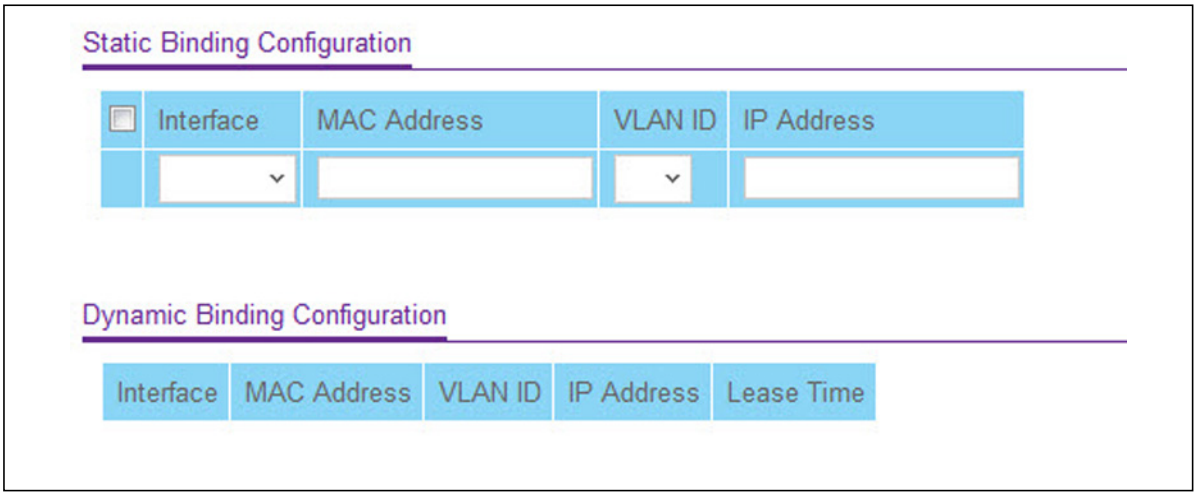
To display the DHCP Snooping Interface Configuration page, click **Security** > **Control> DHCP Snooping** > **Interface Configuration.**



1. **Interface** - Selects the interface for which data is to be configured.
2. If **Trust Mode** is enabled, DHCP Snooping application considers the port as trusted. The factory default is disabled.
3. If **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 N/A then burst interval has no meaning, hence it is disabled. The default value is N/A. It can be set to value -1, which means N/A. 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 N/A burst interval has no meaning and it is N/A. The default value is N/A. It can be set to value -1, which means N/A. The range of Burst Interval is 1 to 15).

DHCP Snooping Binding Configuration

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



Static Binding Configuration

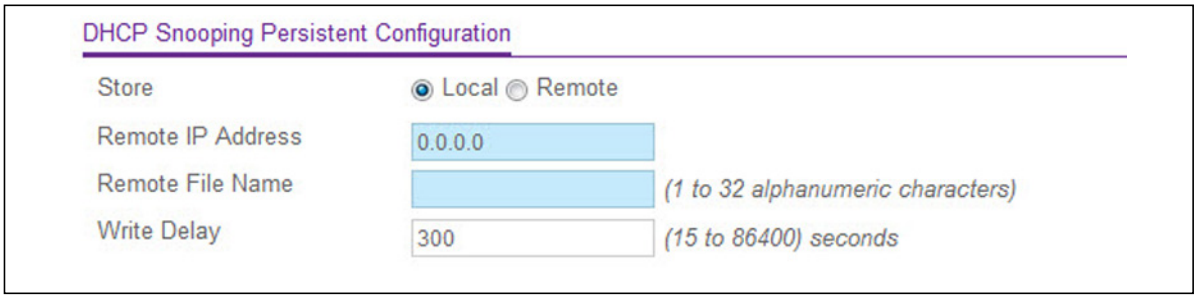
1. **Interface** - Selects the interface to add a binding into the DHCP Snooping database.
2. Use **MAC Address** to specify the MAC address for the binding entry to be added. This is the Key to the binding database.
3. Use **VLAN ID** to select the VLAN from the list for the binding rule. The range 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 is associated in the DHCP Snooping database.
2. Use **MAC Address** to display the MAC address for the binding in the binding database.
3. Use **VLAN ID** to display the VLAN for the binding entry in the binding database. The range of the VLAN ID is (1 to 4093).
4. **IP Address** - Displays IP Address for the binding entry in the binding database.
5. **Lease Time** - Displays the remaining Lease time for the Dynamic entries
6. Click **Clear** to delete all DHCP Snooping binding entries.

DHCP Snooping Persistent Configuration

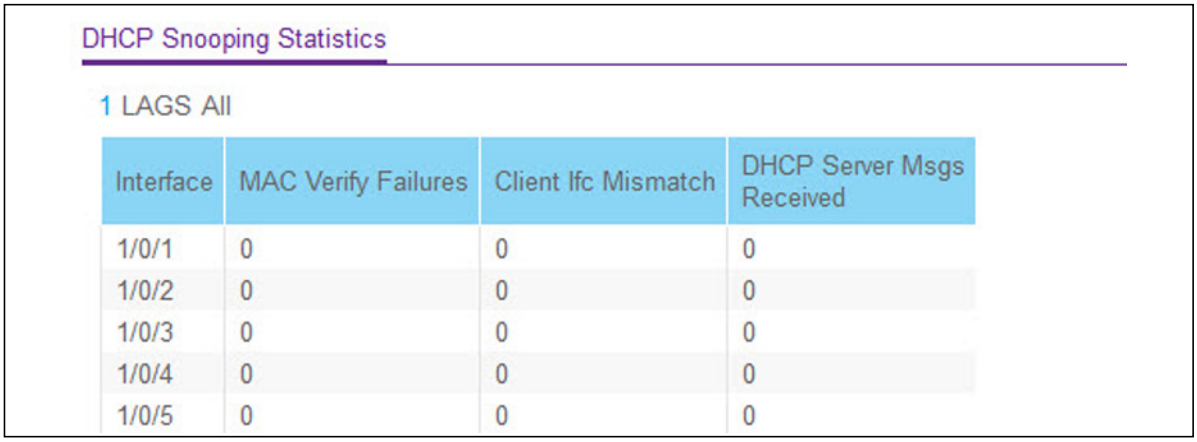
To display the DHCP Snooping Persistent Configuration page, click **Security** > **Control> DHCP Snooping** > **Persistent Configuration.**



1. Use **Store** to select the local store or remote store. Selecting Local will disable the Remote fields 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.**



Field	Description
Interface	The untrusted and Snooping-enabled interface for which statistics are 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.

Field	Description
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 untrusted port.

Click **Clear** to clear all interfaces statistics.

Click **Update** to update the page with the latest information on the switch.

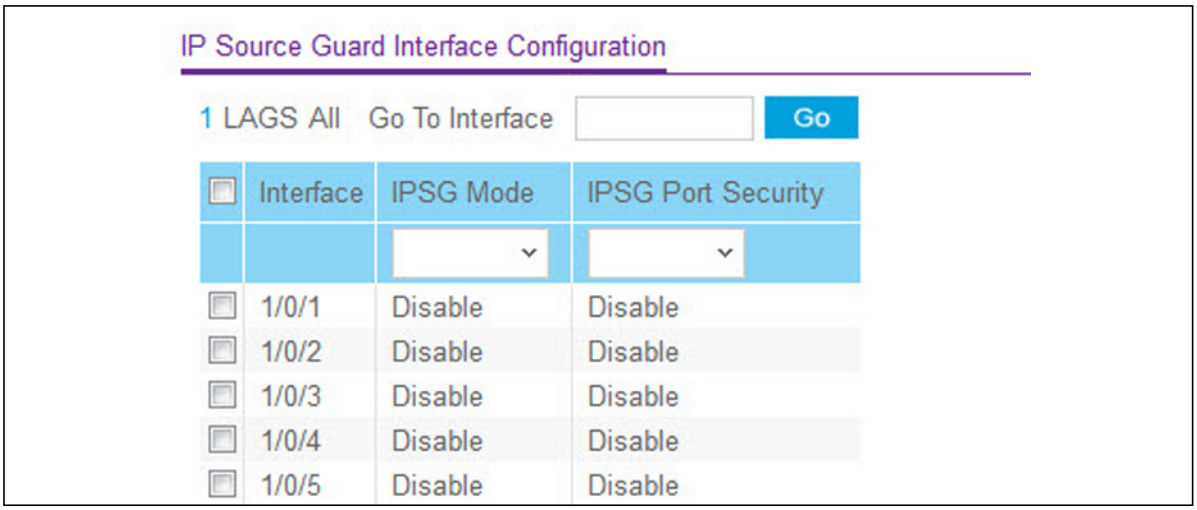
IP Source Guard

The IP Source Guard link contains links to the following pages:

- *IP Source Guard Interface Configuration* on page 455
- *IP Source Guard Binding Configuration* on page 456

IP Source Guard Interface Configuration

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



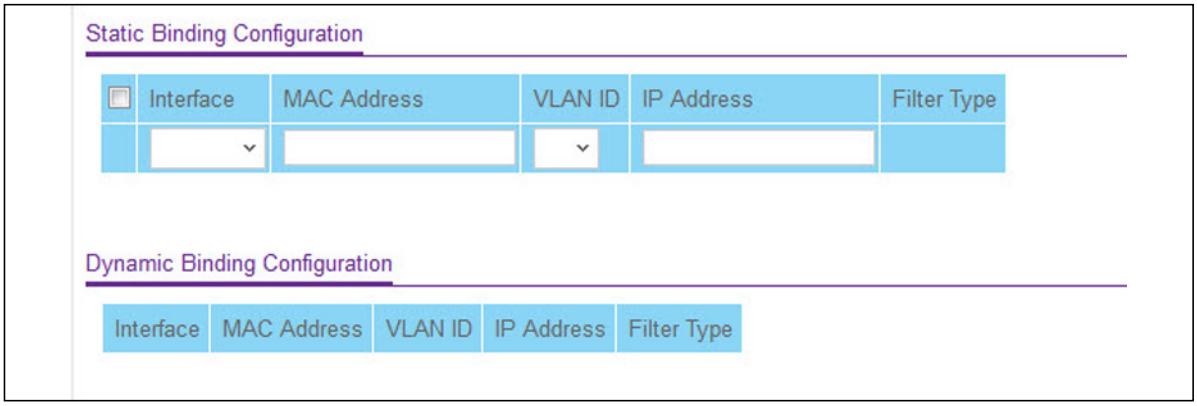
1. **Interface** - Selects the interface to enable IPSG.
2. Use **IPSG Mode** to enable or disable validation of Sender IP Address on this interface. If IPSG is enabled, Packets will not be forwarded if Sender IP Address is not in DHCP Snooping Binding database. The factory default is disabled.
3. Use **IPSG Port Security** to enable or disables the IPSG Port Security on the selected interface. If IPSG Port Security is enabled then the packets will not be forwarded if the sender MAC Address is not in FDB table and it is not in DHCP Snooping binding database. To enforce filtering based on MAC address other required configurations are:
   - Enable port-security globally.

- Enable port-security on the interface level.

IPSG Port Security can't be Enabled if IPSG is Disabled. The factory default is disabled.

IP Source Guard Binding Configuration

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



Static Binding Configuration

1. **Interface** - Selects the interface to add a binding into the IPSG database.
2. Use **MAC Address** to specify the MAC address for the binding.
3. Use **VLAN ID** to select the VLAN from the list for the binding rule.
4. Use **IP Address** to specify valid IP Address for the binding rule.
5. Click **Add** to add IPSG static binding entry into the database.
6. Click **Delete** to delete selected static entries from the database.

Dynamic Binding Configuration

Field	Description
Interface	Displays the interface to add a binding into the IPSG database.
MAC Address	Displays the MAC address for the binding entry.
VLAN ID	Displays the VLAN from the list for the binding entry.
IP Address	Displays valid IP Address for the binding entry.
Filter Type	Filter Type used on the interface. One is source IP address filter type, the other is source IP address and MAC address filter type.

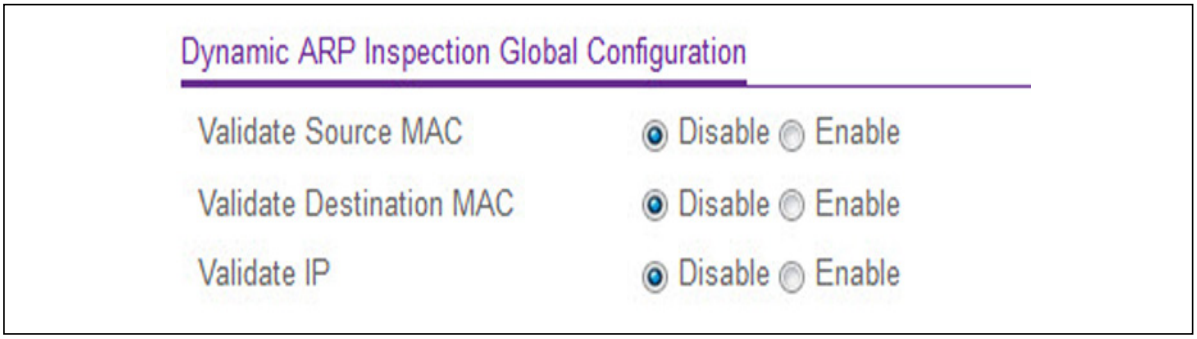
Click **Clear** to clear all the dynamic binding entries.

Dynamic ARP Inspection

The Dynamic ARP Inspection (DAI) link contains links to the following pages:

DAI Configuration

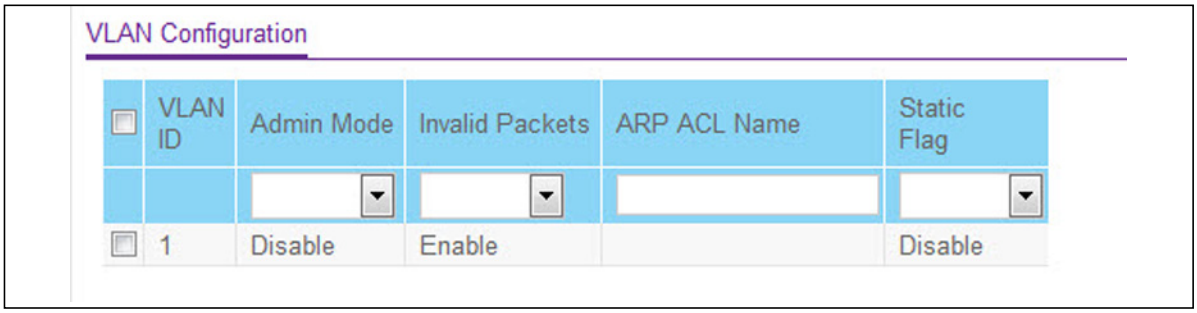
To display the DAI Configuration page, click **Security** > **Control> Dynamic ARP Inspection** > **DAI Configuration.**



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

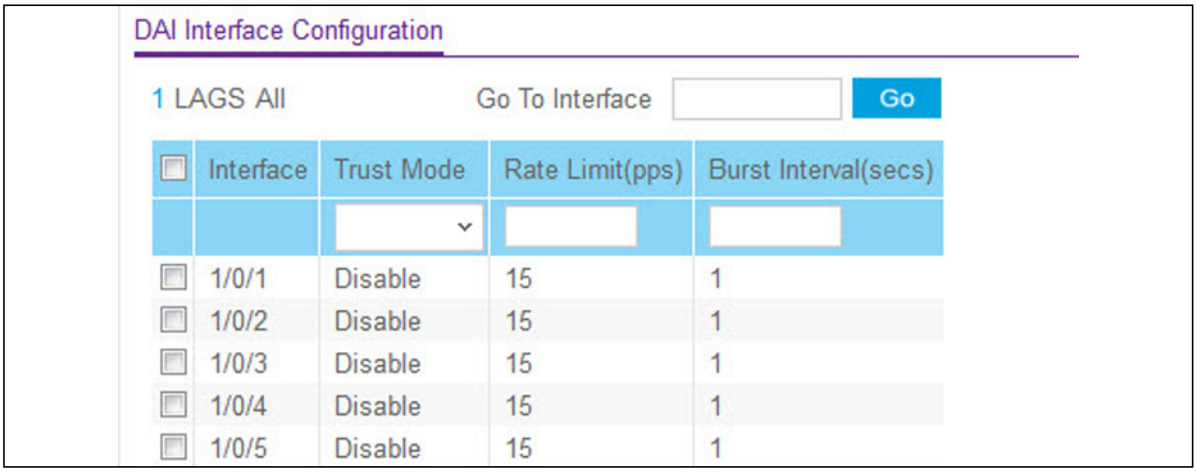
To display the DAI VLAN Configuration page, click **Security** > **Control> Dynamic ARP Inspection** > **DAI VLAN Configuration.**



1. **VLAN ID** - Select the DAI Capable VLANs for which information has to be displayed or configured.
2. Select from the **Admin Mode** menu to indicate whether the Dynamic ARP Inspection is enabled on this VLAN. If this object is set to **Enable**, then Dynamic ARP Inspection is enabled. If this object is set to **Disable**, then Dynamic ARP Inspection is disabled. The default is **Disable.**
3. Use **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. The default is **Enable.**
4. Use **ARP ACL Name** to specify a name for the ARP Access list. A VLAN can be configured to use this ARP ACL containing rules as the filter for ARP packet validation. The name can contain up to <1-31> alphanumeric characters. The ARP ACL Name is deleted if you specify N/A.
5. Use **Static Flag** to determine whether the ARP packet needs validation using the DHCP Snooping database in case ARP ACL rules do not 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**.
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.

DAI Interface Configuration

To display the DAI Interface Configuration page, click **Security** > **Control> Dynamic ARP Inspection** > **DAI Interface Configuration.**

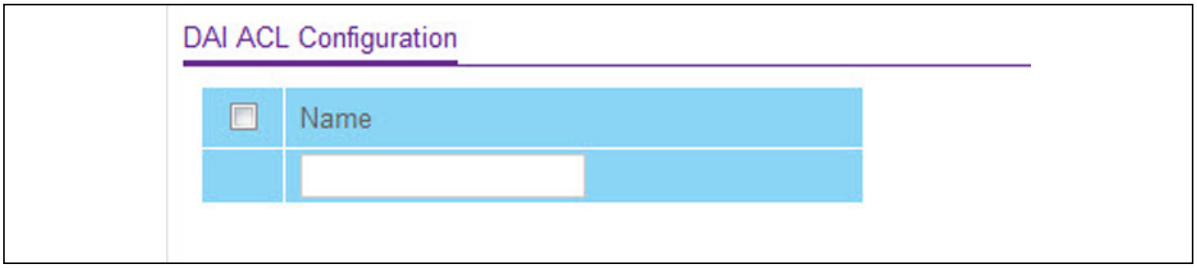


1. **Interface** - Selects the physical interface for which data is to be configured.
2. Use **Trust Mode** to indicate whether the interface is trusted for Dynamic ARP Inspection purpose. If this object is set to 'Enable', the interface is trusted. ARP packets coming to this interface will be forwarded 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 N/A there is no limit. The value can set to -1, which means N/A. The range of Rate Limit is 0 - 300. 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.**

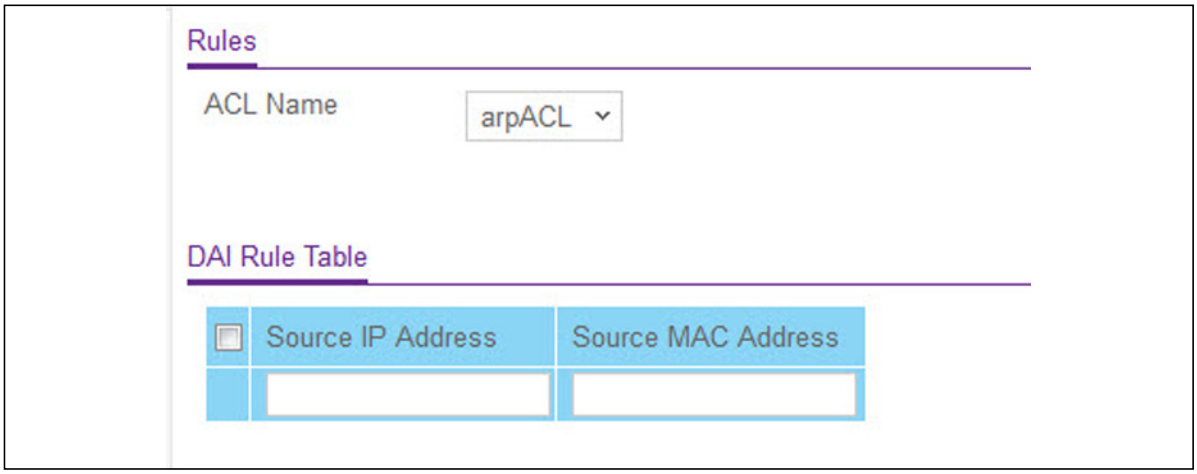


1. Use **Name** to create New ARP ACL for DAI.
2. Click **Add** to add a new DAI ACL to the switch configuration.
3. Click **Delete** to remove the currently selected DAI ACL from the switch configuration.

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.**



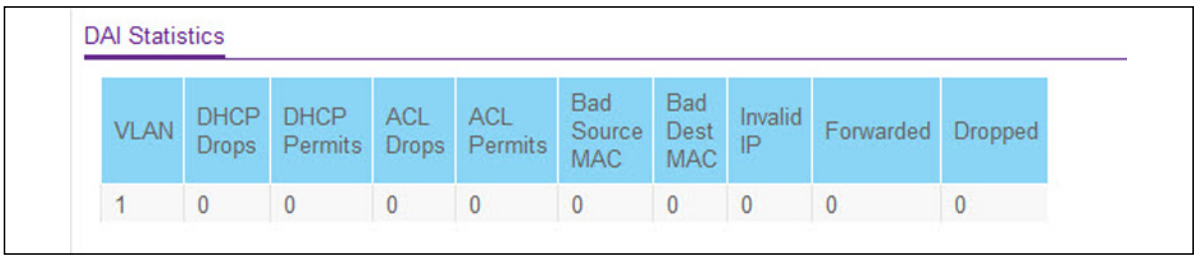
1. **ACL Name** - Selects the DAI ARP ACL for which information want to be displayed or configured.
2. Click **Add** to add a new Rule to the selected ACL.
3. Click **Delete** to remove the currently selected Rule from the selected ACL.

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.**



Field	Description
VLAN	The enabled VLAN ID for which statistics are 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 **Update** to update the page with the latest information on the switch.

Captive Portal

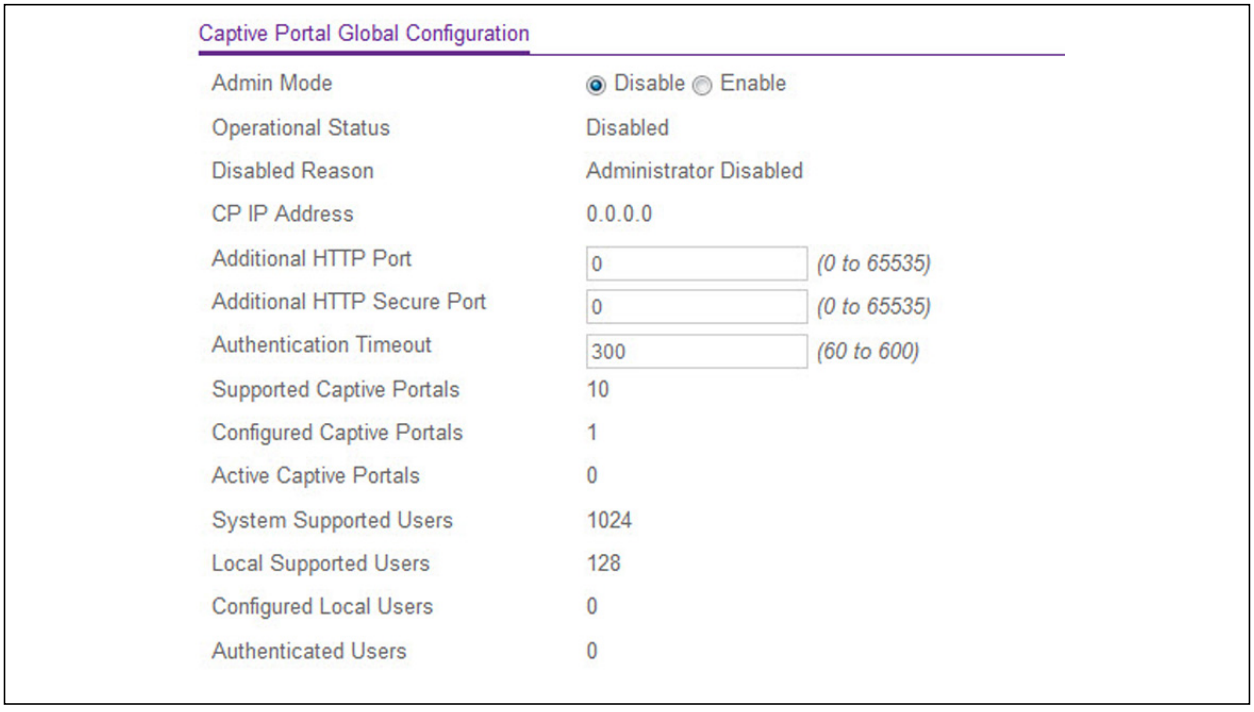
The captive portal feature allows you to prevent clients from accessing the network until user verification has been established. You can configure captive portal verification to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted. The database can be stored locally on the device or on a RADIUS server.

From the **Security** > **Control > Captive Portal** link, you can access the following web pages that configure and display Captive Portal (CP) data:

CP Global Configuration

Use this page to control the administrative state of the Captive Portal feature, and configure global settings that affect all captive portals configured on the switch.

To display the Captive Portal Global Configuration page, click **Security** > **Control** > **Captive Portal** > **CP Global Configuration** in the navigation menu. The following page is displayed.



➢ Configure Captive Portal Global Configuration.

1. In **Admin Mode** list, select to **Enable** or **Disable** the administrative mode of the Captive Portal feature. By default CP is disabled.

2. HTTP traffic uses standard port 80, but you can use the **Additional HTTP Port** field to configure an additional port for HTTP traffic. Enter a port number between 0-65535 (excluding port 80). Enter 0 to unconfigure the Additional HTTP Port. The default is 0.
3. HTTP Secure traffic uses standard port 443, but you can configure an additional port for HTTP Secure traffic using the **Additional HTTP Secure Port** field. Enter a port number between 0-65535 (excluding port 443). Enter 0 to unconfigure the Additional HTTP Secure Port. The default is 0.
4. To access the network through a portal, the client must first enter authentication information on an authentication Web page. Use the **Authentication Timeout** field to enter the number of seconds that captive portal keeps the authentication session open with a client that is attempting to access the network through a portal. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client. The valid range is 60 to 600 seconds. The default Authentication Timeout is 300 seconds.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Table 158, Captive Portal Global Configuration on page 463 describes the non-configurable data that is displayed.

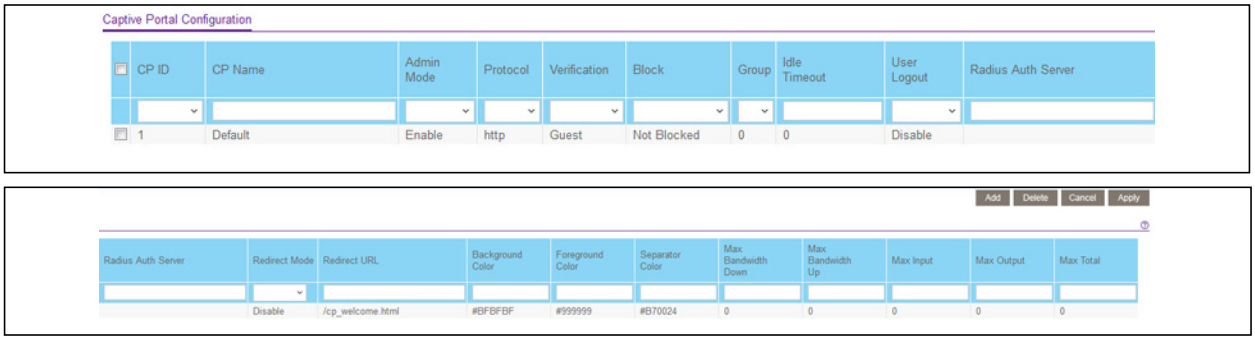
Table 158. Captive Portal Global Configuration

Field	Description
Operational Status	The operational status of the captive portal feature, which is either Enabled or Disabled. The default is Disabled.
Disabled Reason	If CP is disabled, this field displays the reason, which can be one of the following: • Administratively disabled • IP address not configured • No IP routing interface • Routing disabled
CP IP Address	The IP address that the captive portal uses.
Supported Captive Portals	Displays the number of supported captive portals in the system.
Configured Captive Portals	Shows the number of captive portals configured on the switch.
Active Captive Portals	Shows the number of captive portal instances that are operationally enabled.
System Supported Users	Shows the number of authenticated users that the system can support.
Local Supported Users	Shows the number of entries that the Local User database supports.
Configured Local Users	The number of local users configured.
Authenticated Users	Shows the number of users currently authenticated to all captive portal instances on this switch.

CP Configuration

By default, the switch has one captive portal. You can change the settings for that captive portal, and you can also create and configure up to nine additional portals.

To display the Captive Portal Global Configuration page, click **Security** > **Control** > **Captive Portal** > **CP Configuration**. The following page is displayed.



➢ **To add a Captive Portal instance, configure the desired fields below:**

1. Enter the name of the configuration in the **CP Name** field. The name can contain 1 to 31 alphanumeric characters.
2. In the **Admin Mode** list, select to **Enable** or **Disable** the administrative mode of the Captive Portal feature. By default CP is disabled.
3. Select either HTTP or HTTPS as the **Protocol** the captive portal instances use for communication with clients during the verification process.
   - HTTP does not use encryption during verification.
   - HTTPS uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption. The certificate is presented to the user at connection time.
4. Select the type of user **Verification** that the captive portal instance performs with clients that attempt to connect:
   - Guest—The user does not need to be authenticated by a database.
   - Local—The device uses a local database to authenticate users.
   - RADIUS—The device uses a database on a remote RADIUS server to authenticate users.
5. Select the **Block** status. If the CP is blocked, users cannot gain access to the network through the CP. Use this function to temporarily protect the network during unexpected events, such as denial of service attacks.
6. If the Verification Mode is Local or RADIUS, use the **Group** field to assign an existing User Group to the captive portal. All users who belong to the group are permitted to access the network through this portal. The User Group list is the same for all CP configurations on the switch.
7. In the **Idle Timeout** field, enter the number of seconds to wait before terminating a session. A user is logged out once the session idle timeout is reached. If you set the value to 0, then the timeout is not enforced. The valid range is 0 to 900 seconds. The default value is 0.

8. In the **User Logout** list, select the **Enable** or **Disable** option to allow an authenticated client to deauthenticate from the network. If this option is clear or the user does not specifically request logout, the client connection status remains authenticated until the captive portal deauthenticates the user, for example by reaching the idle timeout or session timeout values.
9. If the verification mode is RADIUS, use the **Radius Auth Server** field to enter the IP address of the RADIUS server to use for client authentication. The device acts as the RADIUS client and performs all RADIUS transactions on behalf of the clients.
10. Select the **Redirect Mode** to whether the CP should redirect the newly authenticated client to the configured URL (enable). If this mode is disabled, the default locale specific welcome is used.
11. Specify the **Redirect URL** to which the newly authenticated client is redirected. The maximum length for the URL is 512 alphanumeric characters.
12. In the **Background Color** field, specify the value of the background color. For example, #BFBFBF.
13. In the **Foreground Color** field, specify the value of the foreground color. For example, #999999.
14. In the **Separator Color** field, specify the value of the separator color. For example, #46008F.
15. In the **Max Bandwidth Down** field, specify the maximum rate at which a client can receive data from the network. Rate is in bytes per seconds. 0 indicates the limit is not enforced. The range is 0 to 536870911.
16. In the **Max Bandwidth Up** field, specify the maximum rate, in bytes per second, at which a client can send data into the network. 0 indicates the limit is not enforced. The range is 0 to 536870911.
17. In the **Max Input** field, specify the maximum number of octets that the user is allowed to transmit. After this limit has been reached, the user will be disconnected. 0 indicates the limit is not enforced. The range is 0 to 4294967295.
18. In the **Max Output** field, specify the maximum number of octets that the user is allowed to receive. After this limit has been reached, the user will be disconnected. 0 indicates the limit is not enforced. The range is 0 to 4294967295.
19. In the **Max Total** field, specify the maximum number of octets that the user is allowed to transfer, meaning the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. 0 indicates the limit is not enforced. The range is 0 to 4294967295.
20. Click **Add** to add the new Captive Portal instance.

- **To change the settings for an existing Captive Portal instance:**

1. Select the **CP ID** from the list. The ID is a unique value that identifies the captive portal instance. This value is automatically assigned to the instance when it is created and cannot be changed.
2. Update the configuration using the steps above.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

- **To delete an existing Captive Portal instance:**

  1. Select the **CP ID** from the list.
  2. Click **Delete** to remove the currently selected CP instance.

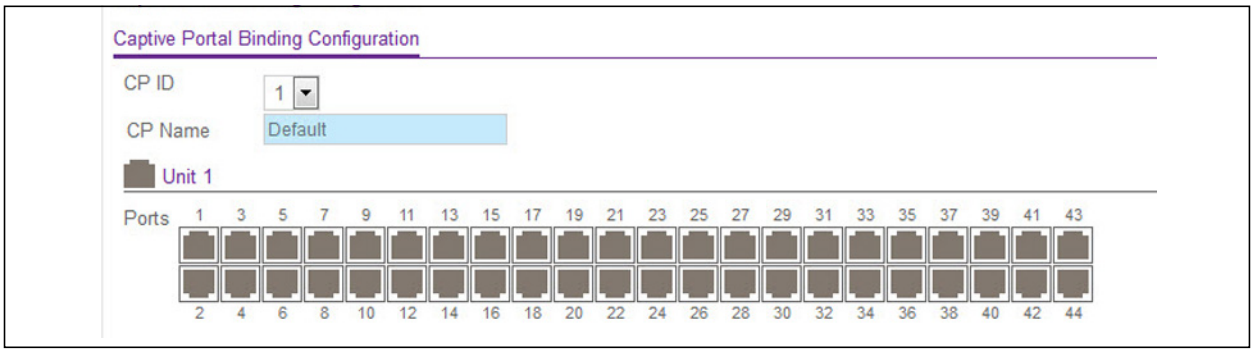
- **To cancel the configuration on the screen:**

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

CP Binding Configuration

You can associate a configured captive portal with a specific network (SSID). The CP feature only runs on the interfaces you specify. A CP can have multiple interfaces associated with it, but an interface can be associated to only one CP at a time.

To display the Captive Portal Binding Configuration page, click **Security** > **Control** > **Captive Portal** > **CP Binding Configuration**. The following page is displayed.



- **To select the Captive Portal instance:**

  1. Select the **CP ID** from the list to select the CP ID for which to create or update a CP instance. The ID is a unique value that identifies the captive portal instance. This value is automatically assigned to the instance when it is created and cannot be changed.

- **To create or update a Captive Portal instance, configure the desired fields below:**

  1. In the **CP Name** field, specify the name of the configuration. The name can contain from 1 to 31 alphanumeric characters.
  2. Select the interface or interfaces from the **Port List**.
  3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
  4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

CP Binding Table

To display the Captive Portal Binding Table page, click **Security** > **Control** > **Captive Portal** > **CP Binding Table**. The following page is displayed.

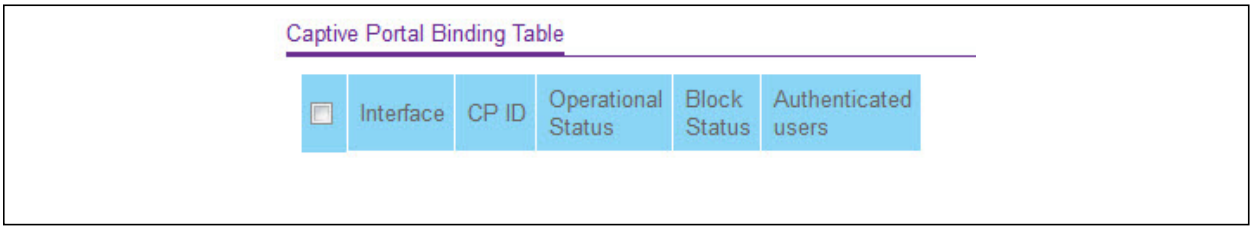


Table 159, Captive Portal Binding Table describes the non-configurable data that is displayed.

Table 159. Captive Portal Binding Table

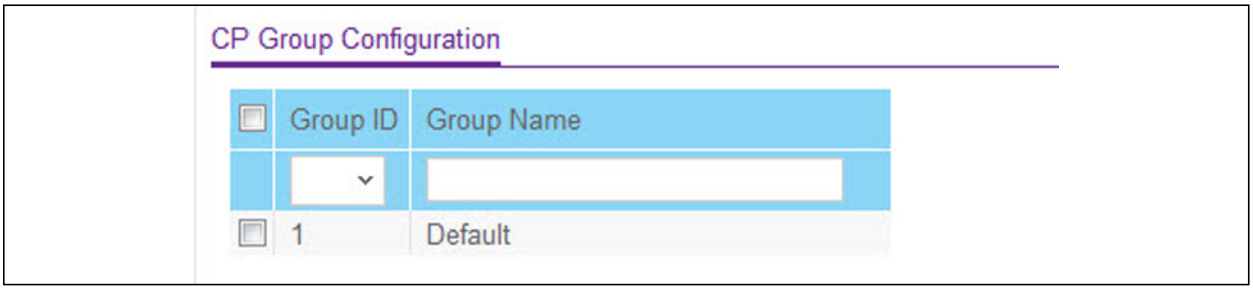
Field	Description
Interface	The interface for which you want to view information.
CP ID	The ID of the captive portal instance.
Operational Status	Indicates whether the portal is active on the specified interface.
Block Status	Indicates whether the captive portal is temporarily blocked for authentication.
Authenticated Users	Shows the number of authenticated users using the captive portal instance on this interface.

- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
- Click **Delete** the remove the currently selected interface.
- Click **Update** to update the page with the latest information on the switch.

CP Group Configuration

Use this page to configure the Captive Portal Group settings on the device.

To display the Captive Portal Group Configuration page, click **Security** > **Control** > **Captive Portal** > **CP Group Configuration**. The following page is displayed.



➢ **To select the Captive Portal Group:**

1. Select the **Group ID** from the list to select the Group ID for which to create or update a Captive Portal group.

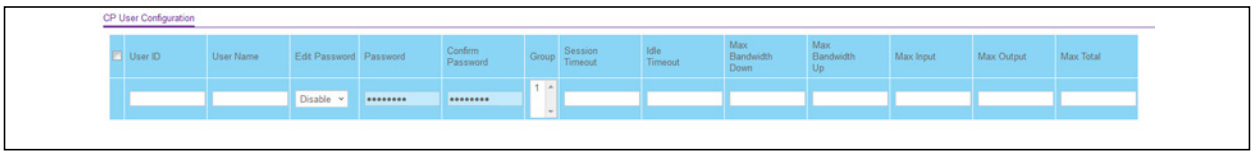
➢ **To create or update a Captive Portal instance, configure the desired fields below:**

2. In the **Group Name** field, specify the name of the user group. The name can contain from 1 to 31 alphanumeric characters.
3. Click **Add** to add a new group.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Delete** the remove the currently selected group.

CP User Configuration

Use this page to configure the Captive Porter User settings on the device.

To display the Captive Portal User Configuration page, click **Security** > **Control** > **Captive Portal** > **CP User Configuration**. The following page is displayed.



➢ **Configure the Captive Portal User Configuration settings:**

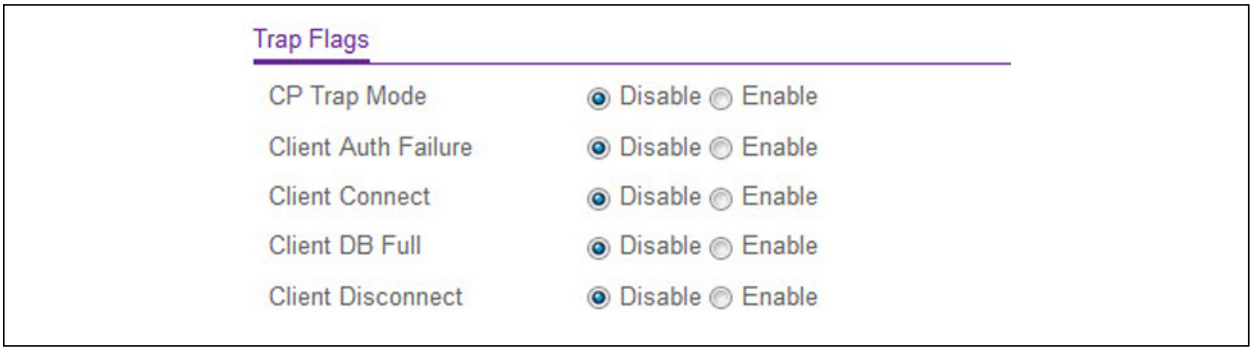
1. Enter the local **User ID** to identify the name of the user.
2. In the **User Name** field, enter the name of the user. The name can contain 1 to 31 alphanumeric characters. Once created, user names cannot be changed or modified.
3. In the **Edit Password** list, select Enable only when you want to change the password. The default value is Disable.
4. In the **Password** field, enter a password for the user. The password length can be from 8 to 64 characters.
5. In the **Confirm Password** field, enter the password for the user again.
6. Use the **Group** field to assign the user to a least one User Group. To assign a user to more than one group, press the Ctrl key and click each group. New users are assigned to the 1-Default user group by default.
7. In the **Session Timeout** field, enter the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically.
8. In the **Idle Timeout** field, enter the number of seconds to wait before terminating a session. A user is logged out once the session idle timeout is reached. If the attribute is 0 or not present, then use the value configured for the captive portal.

9. In the **Max Bandwidth Down** field, enter the maximum rate, in bits per second, at which a client can receive data from the network. 0 indicates use global configuration. The range is 0 to 536870911 bps.
10. In the **Max Bandwidth Up** field, enter the maximum rate, in bits per second, at which a client can send data into the network. 0 indicates use the global limit. The range is 0 to 536870911 bps.
11. In the **Max Input** field, enter the number of octets the user is allowed to receive. After this limit has been reached, the user will be disconnected. 0 indicates to use the global limit. The range is 0 to 4294967295.
12. In the **Max Output** field, enter the number of octets the user is allowed to transmit. After this limit has been reached, the user will be disconnected. 0 indicates to use the global limit. The range is 0 to 4294967295.
13. In the **Max Total** field, enter the number of bytes the user is allowed to transmit and receive. The maximum number of octets is the sum of octets transmitted and received. After this limit has been reached, the user will be disconnected. 0 indicates to use the global limit. The range is 0 to 4294967295.
14. Click **Add** to add a new user to the Local User database.
15. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
16. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
17. Click **Delete** to delete the selected user from the Local User database.

CP Trap Flags

Use this page to configure whether or not SNMP traps are sent from the Captive Portal and to specify Captive Portal events that will generate a trap. All CP SNMP traps are disabled be default.

To display the Captive Portal Trap Flags page, click **Security** > **Control** > **Captive Portal** > **CP Trap Flags**. The following page is displayed.



➢ **Configure the Captive Portal Trap Flag settings:**

1. In the **CP Trap Mode**, select the option to enable or disable the Captive Portal Trap Mode.

2. Select the option to enable or disable **Client Authentication Failure**. If you enable this field, the SNMP agent sends a trap when a client attempts to authenticate with a Captive Portal but is unsuccessful.
3. Select the option to enable or disable **Client Connect**. If you enable this field, the SNMP agent sends a trap when a client authenticates with, and connects to, a Captive Portal.
4. Select the option to enable or disable **Client Database Full**. If you enable this field, the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.
5. Select the option to enable or disable **Client Disconnect**. If you enable this field, the SNMP agent sends a trap when a client disconnects from a captive portal.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

CP Client

Use this page to view information about the traffic a client has sent or received.

To display the Captive Portal Client page, click **Security** > **Control** > **Captive Portal** > **CP Client**. The following page is displayed.

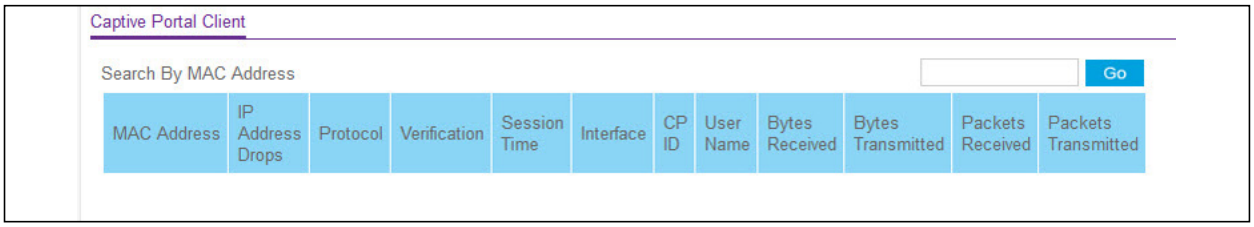


Table 160, Captive Portal Client describes the non-configurable data that is displayed.

- Click **Clear** to clear the information in the client table.
- Click **Update** to update the page with the latest information on the switch.

Table 160. Captive Portal Client

Field	Description
MAC Address	Shows the client MAC address.
IP Address Drops	Identifies the IP address of the client (if applicable).
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.
Session Time	Shows the amount of time that has passed since the client was authorized.

Field	Description
Interface	Identifies the interface the client is using.
CP ID	The ID of the Captive Portal instance.
User Name	Displays the user name (or Guest ID) of the connected client.
Bytes Received	Total bytes the client has received.
Bytes Transmitted	Total bytes the client has transmitted.
Packets Received	Total packets the client has received.
Packets Transmitted	Total packets the client has transmitted.

Configuring Access Control Lists

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network. ProSafe Managed switch's software supports IPv4, IPv6, and MAC ACLs.

You first create an IPv4 based or IPv6 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.

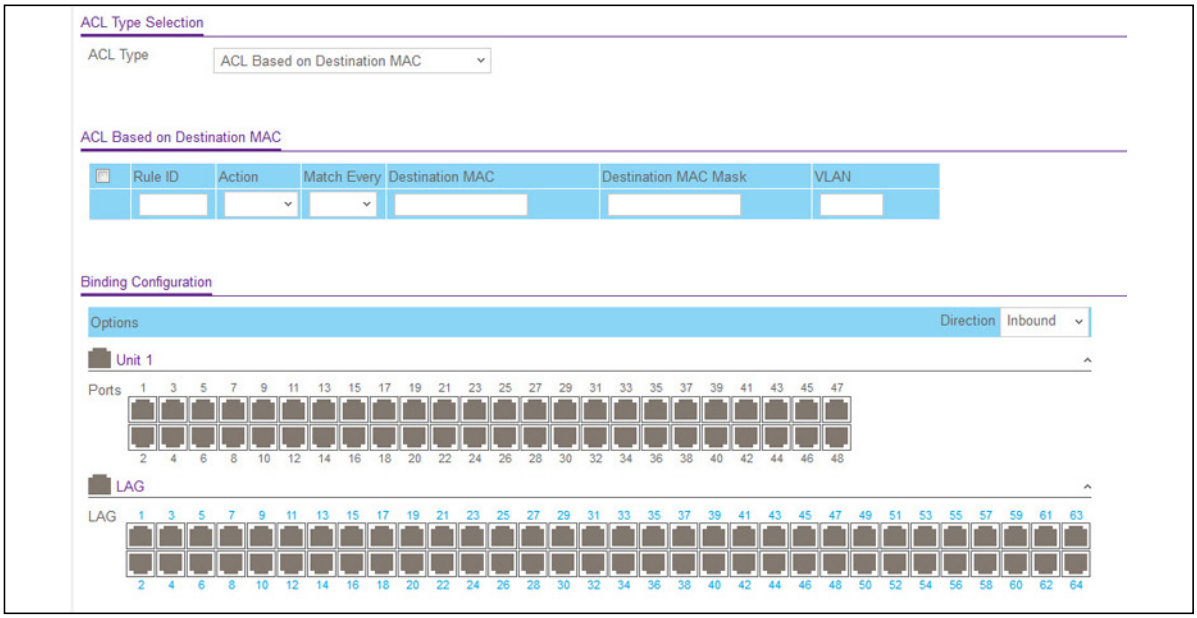
The **Security** > **ACL** tab contains links to the following pages:

- *ACL Wizard*
- *Basic* on page 474
- *Advanced* on page 479

ACL Wizard

The ACL Wizard helps a user to create a simple ACL and apply it to the selected ports easily and quickly. Firstly you must select an ACL type with which you will create an ACL. Then add ACL rule to this ACL and at last apply this ACL on the selected ports. The ACL Wizard allows you to create the ACL, but does not allow you to modify it. If you want to modify the ACL, go to the ACL configuration screen. See *IP ACL* on page 480.

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



ACL Type Selection

➢ **Create a simple ACL.**

Note: The steps in this written procedure describe creating an ACL Based on Destination MAC. If you select a different ACL Type, for example, ACL Based on Source IPv4, then what is shown on this screen varies, depending on the current step in the rule configuration process.

1. Use **ACL Type** to specify 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 an ACL based on the destination MAC address, destination MAC mask and VLAN.
   - **ACL Based on Source MAC** - To create an ACL based on the source MAC address, source MAC mask and VLAN.
   - **ACL Based on Destination IPv4** - To create an ACL based on the destination IPv4 address and IPv4 address mask.
   - **ACL Based on Source IPv4** - To create an ACL based on the source IPv4 address and IPv4 address mask.
   - **ACL Based on Destination IPv6** - To create an ACL based on the destination IPv6 prefix and IPv6 prefix length.
   - **ACL Based on Source IPv6** - To create an ACL based on the source IPv6 prefix and IPv6 prefix length.
   - **ACL Based on Destination IPv4 L4 Port** - To create an ACL based on the destination IPv4 layer4 port number.

- **ACL Based on Source IPv4 L4 Port** - To create an ACL based on the source IPv4 layer4 port number.
- **ACL Based on Destination IPv6 L4 Port** - To create an ACL based on the destination IPv6 layer4 port number.
- **ACL Based on Source IPv6 L4 Port** - To create an ACL based on the source IPv6 layer4 port number.

Note: Two rules will be created (one for TCP and one for UDP) in the case of L4 port options.

ACL Based on Destination MAC

➢ **Use the ACL Based on Destination MAC table to configure rules based on Destination MAC.**

Note: Binding ACLs to interface fails when the system has no resources to bind a new ACL.

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. In the **Match Every** list, select either True or False.
   - True signifies that all packets will match the selected 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.
5. 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.
6. 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.
7. Specify the **VLAN ID** to compare against an Ethernet frame. Valid range of values is 1 to 4093. Either VLAN Range or VLAN can be configured.
8. Click **Add** to add a new rule to the ACL based on Destination MAC.
9. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

10. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
11. Click **Delete** to remove the currently selected Rule from the ACL based on Destination MAC.

ACL Binding Configuration

12. In the **Directions** field, select the packet filtering direction for an ACL. The options are Inbound or Outbound.
13. The Port Selection Table specifies the list of all available valid interfaces for ACL mapping. All non-routing physical interfaces and interfaces participating in LAG are listed.

Basic

The Basic link contains links to the following pages:

- *MAC ACL* on page 474
- *MAC Rules* on page 475
- *MAC Binding Configuration* on page 477
- *MAC Binding Table* on page 479

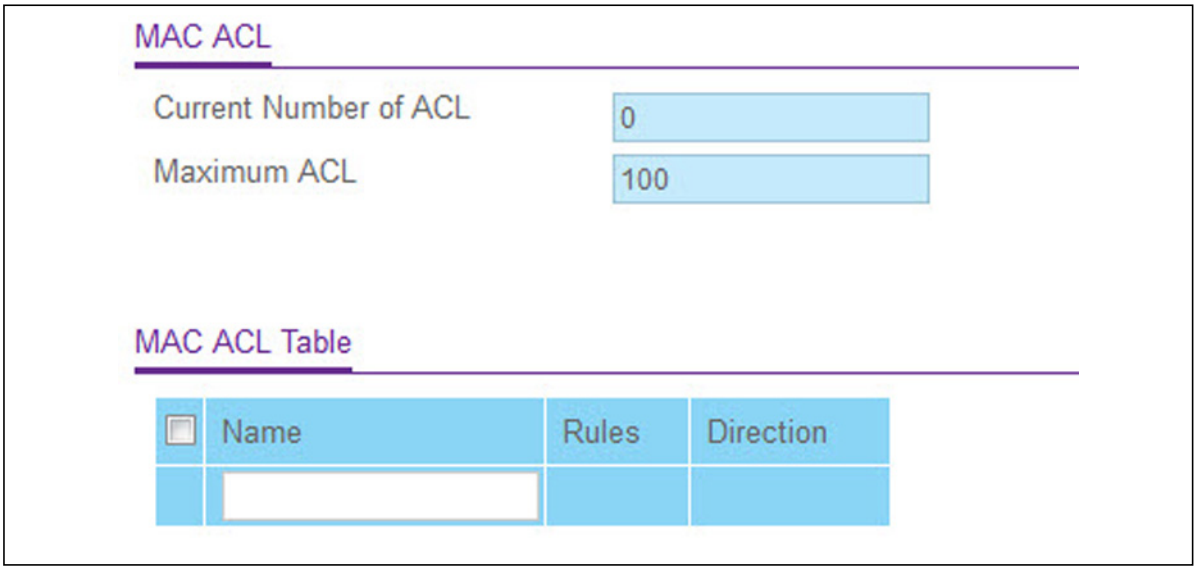
MAC ACL

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. Rules for the MAC ACL are specified/created using the MAC ACL Rule Configuration page.

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 Name.
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 name to a port.
4. Optionally, use the *MAC Binding Table* page to view the configurations.

To display the MAC ACL page, click **Security** > **ACL > Basic > MAC ACL.**



The MAC ACL page displays the number of ACLs currently configured in the switch and the maximum number of ACLs that can be configured. The current number is equal to the number of configured IPv4 and IPv6 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:

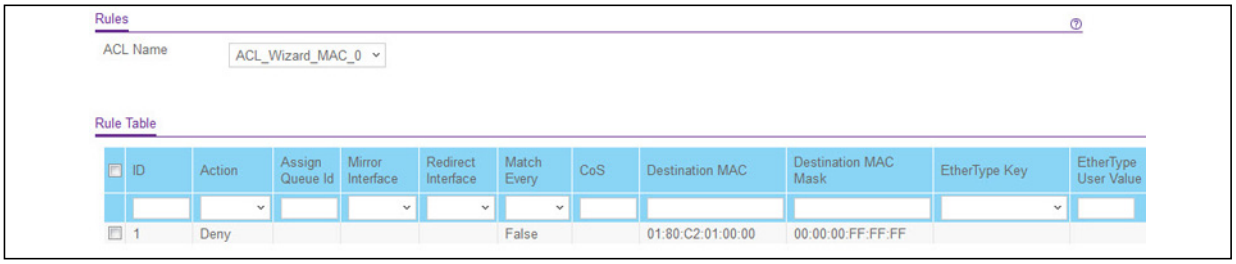
   - **Rules** - Displays the number of rules currently configured for the MAC ACL.
   - **Direction** - Displays the direction of packet traffic affected by the MAC ACL, which can be Inbound or blank.

2. Click **Add** to add a new MAC ACL to the switch configuration.
3. To change the name of a MAC ACL, select the check box next to the Name field, update the name, then click **Apply.**
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. To delete a MAC ACL, select the check box next to the Name field, then click **Delete**.

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. Use **ID** to enter a whole number in the range of (1 to 1023) that will be used to identify the rule.
2. Use **Action** to specify what action should be taken if a packet matches the rule's criteria. The choices are permit or deny.
3. Use **Assign Queue ID** to specify the hardware egress queue identifier used to handle all packets matching this ACL rule. Valid range of Queue Ids is (0 to 7).
4. **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.
5. 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.
6. Use **Match Every** to specify an indication to match every Layer 2 MAC packet.

   Valid values are

   - **True** - Signifies that every packet is considered to match the selected ACL Rule.
   - **False** - Signifies that it is not mandatory for every packet to match the selected ACL Rule.
7. Use **CoS** to specifies the 802.1p user priority to compare against an Ethernet frame. Valid range of values is (0 to 7).
8. 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.
9. 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.
10. Use **EtherType Key** to specify the EtherType value to compare against an Ethernet frame.

    Valid values are

    - Appletalk
    - ARP
    - IBM SNA
    - IPv4

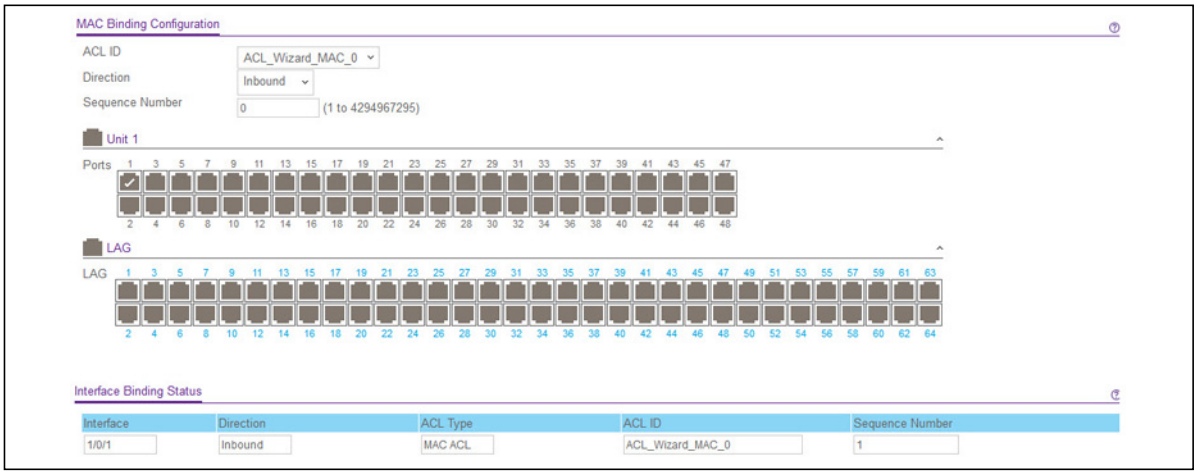
- IPv6
- IPX
- MPLS multicast
- MPLS unicast
- NetBIOS
- Novell
- PPPoE
- Reverse ARP
- User Value

11. Use **EtherType User Value** to specify 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).
12. Use **Source MAC** to specify the Source MAC address to compare against an Ethernet frame. Valid format is (xx:xx:xx:xx:xx:xx).
13. Use **Source MAC Mask** to specify 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).
14. Use **VLAN** to specify the VLAN ID to compare against an Ethernet frame. Valid range of values is (1 to 4095). Either VLAN Range or VLAN can be configured.
15. **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.
16. **Rate Limit Conform Data Rate** - Value of Rate Limit Conform Data Rate specifies the conforming data rate of MAC ACL Rule. Valid values are (1 to 4294967295) in Kbps.
17. **Rate Limit Burst Size** - Value of Rate Limit Burst Size specifies burst size of MAC ACL Rule. Valid values are (1 to 128) in Kbytes.
18. **Time Range** - Name of time range associated with the MAC ACL Rule.
19. Use **Rule Status** - Displays if the ACL rule is active or inactive. Blank means that no timer schedules are assigned to the rule.
20. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
21. To delete a rule, select the check box associated with the rule and click **Delete**.
22. 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**.



1. Select an existing MAC ACL from the **ACL ID** menu. You can select one and bind it to the interfaces you want.
2. The packet filtering **Direction** for ACL is Inbound, which means the MAC ACL rules are applied to traffic entering the port.
3. 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.
4. 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.

The following table describes the information displayed in the **Interface Binding Status**.

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

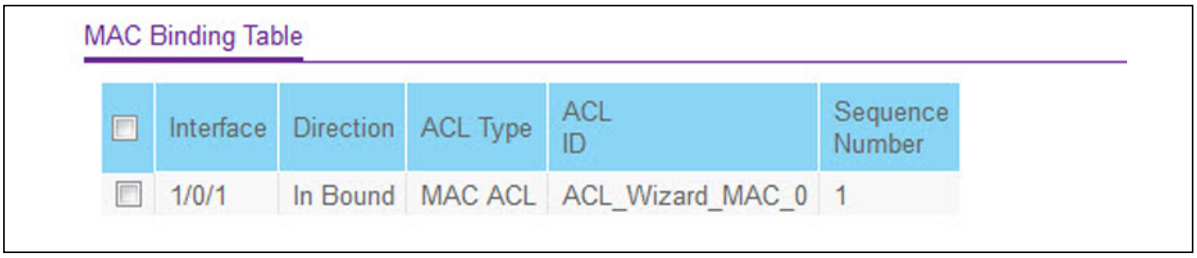
Field	Description
ACL ID	Displays the ACL Number (in case of IP ACL) or ACL Name (in case of MAC ACL) identifying the ACL assigned to selected interface and direction.
Sequence Number	Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Apply** to 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** > **MAC 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.
ACL Type	Displays the type of ACL assigned to selected interface and direction.
ACL ID	Displays the ACL Name identifying the ACL assigned to selected interface and direction.
Sequence Number	Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

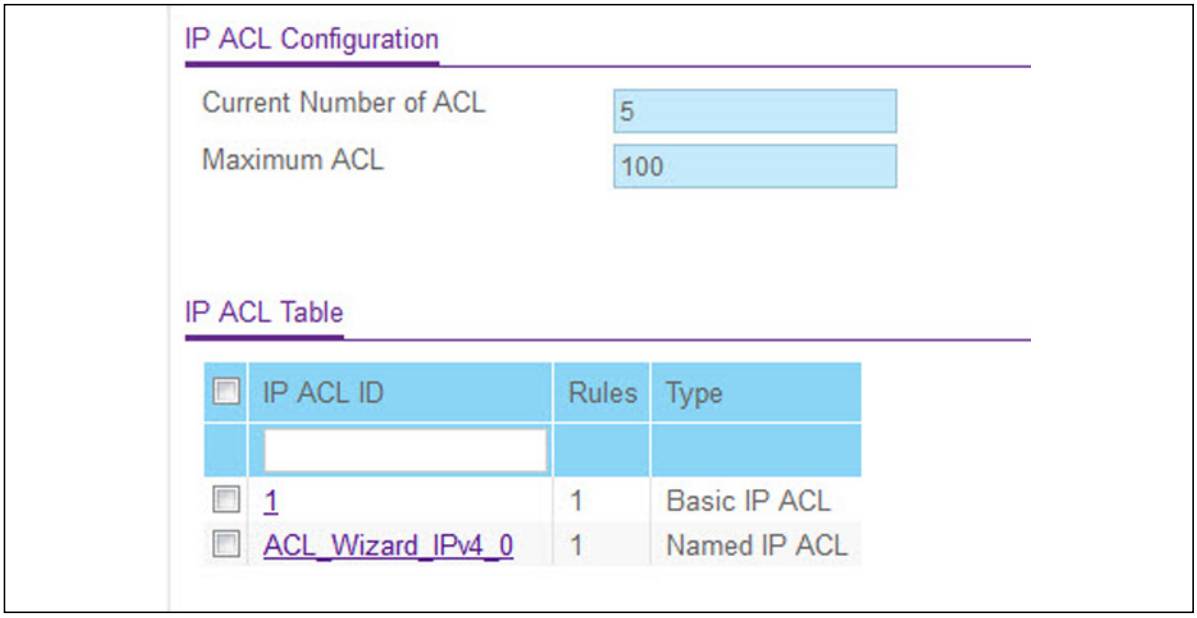
Advanced

The Advanced link contains links to the following pages:

IP ACL

An IP or IPv6 ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken, and the additional rules are not checked for a match. On this menu the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the IP ACL are specified/created using the IPv6 ACL Rule Configuration page.

To display the IP ACL page, click **Security** > **ACL> Advanced** > **IP ACL**.



The IP ACL page shows the current size of the ACL table and the maximum size of the ACL table. The current size is equal to the number of configured IPv4 and IPv6 ACLs plus the number of configured MAC ACLs. The maximum size is 100.

To configure an IP ACL:

1. The **Current Number of ACL** displays the current number of the all ACLs configured on the switch.

2. The **Maximum ACL** displays the maximum number of IP ACL can be configured on the switch, it depends on the hardware.
3. In the **IP ACL** field, specify the ACL ID or IP ACL name which depends on the IP ACL Type. The IP ACL 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 an IPv4 ACL Name string which includes up to 31 alphanumeric characters in length. The name must start with an alphabetic character.

   Each configured ACL displays the following information:

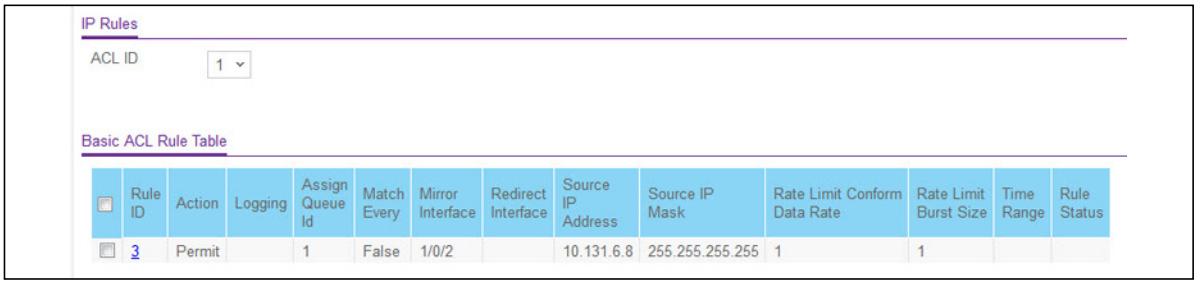
   - **Rules** - Displays the number of rules currently configured for the IP ACL.
   - **Type** - Identifies the ACL as a basic IP ACL (with ID from 1 to 99), extended IP ACL (with ID from 100 to 199), or for Named IP ACL.
4. To delete an IP ACL, select the check box next to the IP ACL ID field, then click **Delete**.
5. Click **Add** to add a new IP ACL to the switch configuration.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IP Rules

Use these screens to display the rules for the IP Access Control Lists created using the IP Access Control List Configuration screen. What is shown on this screen varies depending on the current step in the rule configuration process.

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

To display the IP Rules page, click **Security** > **ACL > Advanced** > **IP Rules**.



To configure rules for an IP ACL:

1. 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** - Enter a whole number in the range of 1 to 1023 that will be used to identify the rule. An IP ACL may have up to 1023 rules.
   - **Action** - Specify what action should be taken if a packet matches the rule's criteria. The choices are permit or deny.
   - **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 IP ACL rule. Valid range of Queue Ids is (0 to 6). This field is visible when 'Permit' is chosen as 'Action'.
   - **Match Every** - Select true or false from the 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 enabled for a 'Permit' Action.
   - **Source 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.
   - **Source IP Mask** - Specify the IP Mask in dotted-decimal notation to be used with the Source IP Address value.

- **Rate Limit Conform Data Rate** - Value of Rate Limit Conform Data Rate specifies the conforming data rate of IP ACL Rule. Valid values are (1 to 4294967295) in Kbps.
- **Rate Limit Burst Size** - Value of Rate Limit Burst Size specifies burst size of IP ACL Rule. Valid values are (1 to 128) in Kbytes.
- **Time Range** - Name of time range associated with the IP ACL Rule.
- **Rule Status** - Displays if the ACL rule is active or inactive. Blank means that no timer schedules are assigned to the rule.

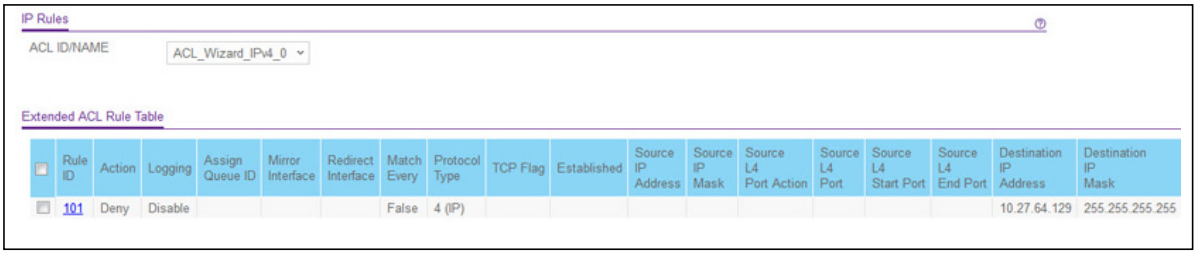
2. To delete an IP ACL rule, select the check box associated with the rule, and then click **Delete**.
3. To update an IP ACL rule, select the check box associated with the rule, update the desired fields, and then click **Apply**. You cannot modify the Rule ID of an existing IP rule.
4. Click **Cancel** 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.
6. To modify an existing IP Extended ACL rule, click the **Rule ID**. The number is a hyperlink to the Extended ACL Rule Configuration page.

IP Extended Rules

Use these screens to display the rules for the IP Access Control Lists created using the IP Access Control List Configuration screen. What is shown on this screen varies depending on the current step in the rule configuration process.

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

To display the IP extended Rules page, click **Security** > **ACL> Advanced** > **IP Extended Rules**.



➢ **To configure rules for an Extended IP ACL:**

1. **ACL ID/Name** - Use the menu to select the IP ACL for which to create or update a rule.
2. Configure **Rule ID** by entering a whole number in the range of 1 to 1023 that will be used to identify the rule. An IP ACL may have up to 1023 rules.

3. Specify the **Action** to take if a packet matches the rule's criteria. The choices are Permit or Deny.
4. Set **Logging** to Enable 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. In the **Assign Queue ID,** specify the hardware egress queue identifier used to handle all packets matching this IP ACL rule. The valid range of Queue IDs is 0 to 6.
6. Use the **Mirror Interface** field 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 the **Redirect Interface** field 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 enabled for a *Permit* Action.
8. Select True or False from the **Match Every** 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.
9. Use the **Protocol Type** field to 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, UDP, EIGRP, GRE, IPINIP, OSPF, and PIM.
10. In the **TCP Flag** field, 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, and FIN. Each TCP flag has the possible values below and can be set separately:
    - **Ignore**—A packet matches this ACL rule whether 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.
11. When **Established** is specified, a match occurs if either RST- or ACK-specified bits are set in the TCP header. These fields are enabled only when TCP protocol is selected.
12. In the **Src** field, enter a source 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.
    a. Select the **IP Address** option and enter an IP address with a relevant wild card mask to apply this criteria. If this field is left empty, it means *any*.
    b. When you select the **Host** option, the wild card mask is configured as 0.0.0.0. If this field is left empty, it means *any*.

    The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 0.0.0.0 indicates that *none* of the bits are important. A wild card of 255.255.255.255 indicates that *all* of the bits are important.

13. Use **Source L4 Port Action** to specify relevant matching conditions for L4 port numbers in the current extended ACL rule:
    - Equal—IP ACL rule matches only if the layer 4 source port number is equal to the specified port number or port key.
    - Less Than—IP ACL rule matches if the layer 4 source port number is less than the specified port number or port key.
    - Greater Than—IP ACL rule matches if the layer 4 source port number is greater than the specified port number or port key.
    - Not Equal—IP ACL rule matches only if the layer 4 source port number is not equal to the specified port number or port key.
14. **Src L4 Port** and **Src L4 Range** options are available only when protocol is set to TCP or UDP. When you select the **Port** option, choose *port key* from the list or enter the port number yourself.
    - The source IP TCP port names are bgp, domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, www, pop2, pop3.
    - The source IP UDP port names are domain, echo, ntp, rip, snmp, tftp, time, who.

    Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

    Only when you select **Other** in the list of port keys, can you enter your own port number. If you leave the Other field empty, it means *any*.
15. When you select the **Range** option, IP ACL rule matches only if the layer 4 port number is within the specified port range. The Start Port and End Port parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535.

    The possibility of entering your own port number is available only when *Other* is selected in the list of port keys. The starting port, ending port, and all ports in between will be a part of the layer 4 port range. If these fields are left empty, it means *any*.

    The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 0.0.0.0 indicates that *none* of the bits are important. A wild card of 255.255.255.255 indicates that *all* of the bits are important.
16. In the **Dst** field, specify a Destination IP Address, using dotted-decimal notation, and with a relevant wild card mask, to be compared to a packet's destination IP Address as a match criteria for the selected extended IP ACL rule.
17. Select the **IP Address** option and enter an IP address with a relevant wild card mask to apply this criteria. If these fields are left empty, it means *any*.
18. When you select the **Host** option, the wild card mask is configured as 0.0.0.0. If this field is left empty, it means *any*.
19. In the **Destination IP Mask** field, specify the IP Mask, in dotted-decimal notation, to be used with the Destination IP Address value.
20. In the **Dst L4 Port** and **Dst L4 Range** fields, specify the layer 4 destination port match condition for the selected extended IP ACL rule. These options are available only when the protocol is set to TCP or UDP.

Only when you select **Other** in the list of port keys, can you enter your own port number. If you leave the Other field empty, it means *any*.

- The Destination IP TCP possible port names are bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3.
- The Destination IP UDP possible port names are domain, echo, ntp, rip, snmp, tftp, time, who.

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.

21. Use **Destination L4 Port Action** to specify relevant matching conditions for L4 port numbers in the current extended ACL rule:
    - Equal—IP ACL rule matches only if the layer 4 source port number is equal to the specified port number or port key.
    - Less Than—IP ACL rule matches if the layer 4 source port number is less than the specified port number or port key.
    - Greater Than—IP ACL rule matches if the layer 4 source port number is greater than the specified port number or port key.
    - Not Equal—IP ACL rule matches only if the layer 4 source port number is not equal to the specified port number or port key.
22. When you select the **Range** option, IP ACL rule matches only if the layer 4 port number is within the specified port range. The Start Port and End Port parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535.

    The possibility of entering your own port number is available only when *Other* is selected in the list of port keys. The Destination L4 Start Port starting port, Destination L4 End Port ending port, and all ports in between will be a part of the layer 4 port range. If these fields are left empty, it means *any*.
23. **IGMP Type** - When IGMP type is specified, IP ACL rule matches with the specified IGMP message type. Possible values are in the range 0 to 255. If this field is left empty, it means *any*.
24. **ICMP Type** and **ICMP Code** - The ICMP Type and ICMP Code fields are enabled only if the protocol is ICMP. Use the ICMP Type and ICMP Code fields to specify a match condition for ICMP packets.
    - When the ICMP Type option is selected, IP ACL rule matches with the specified ICMP message type, a possible type number is in the range from 0 to 255.
    - When the ICMP Code option is specified, IP ACL rule matches with the specified ICMP message code. Possible values for Code could be in the range from 0 to 255.
    - If these fields are left empty, it means *any*.
    - When the *Message* option is selected, choose the type of the ICMP message to match with the selected IP ACL rule. Specifying Message implies that both ICMP type and ICMP code are specified. ICMP message is decoded into corresponding ICMP type and ICMP code within that ICMP type. IPv4 ICMP message types are: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect,

packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded, and unreachable.

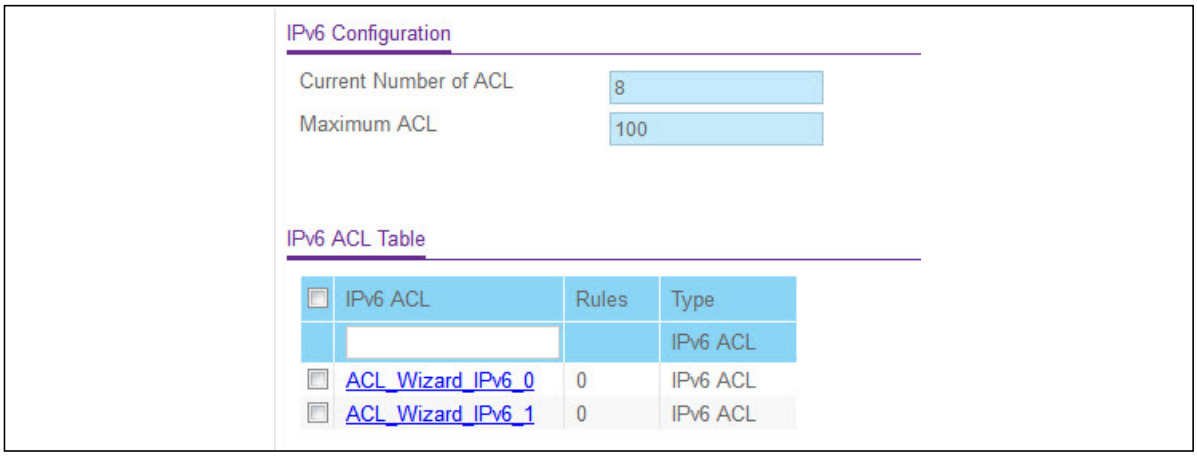
25. **Service Type** - Select a Service Type match condition for the extended IP ACL rule from the menu. The possible values are IP DSCP, IP precedence, and IP TOS, which are alternative ways of specifying a match criterion for the same Service Type field in the IP header, however each uses a different 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 drop-down box. If a value is to be selected by specifying its numeric value, then select the 'Other' option in the drop-down 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.
26. **Rate Limit Conform Data Rate** - Value of Rate Limit Conform Data Rate specifies the conforming data rate of IP ACL Rule. Valid values are (1 to 4294967295) in Kbps.
27. **Rate Limit Burst Size** - Value of Rate Limit Burst Size specifies burst size of IP ACL Rule. Valid values are (1 to 128) in Kbytes.
28. **Time Range** - Name of time range associated with the IP Extended ACL Rule.
29. **Rule Status** - Displays if the ACL rule is active or inactive. Blank means that no timer schedules are assigned to the rule.
30. To modify an existing IP Extended ACL rule, click the **Rule ID**. The number is a hyperlink to the Extended ACL Rule Configuration (100-199) screen, which is used for configuration ACL Rules. Click the **Add** button on the IP Extended Rules screen.
31. For standard ACL Rule Configuration (1-99), click the **Add** button on the IP Rules screen.
32. To delete an IP ACL rule, select the check box associated with the rule, and then click **Delete**.
33. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IPv6 ACL

An IP or IPv6 ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken, and the additional rules are not checked for a match. On this menu the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or

outbound traffic. Rules for the IP ACL are specified/created using the IPv6 ACL Rule Configuration page.

To display the IPv6 ACL page, click **Security** > **ACL > Advanced** > **IPv6 ACL**.



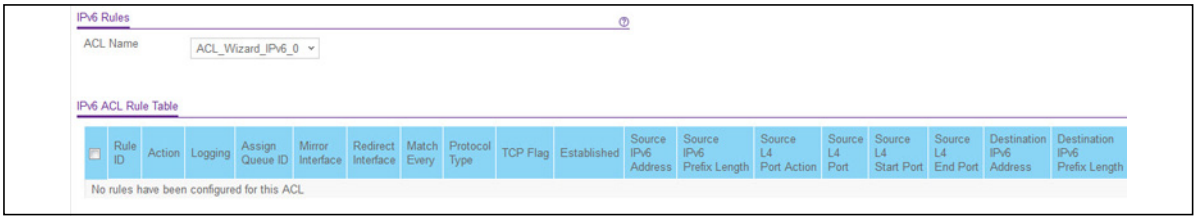
1. **IPv6 ACL** is the IPv6 ACL Name string which includes up to 31 alphanumeric characters only. The name must start with an alphabetic character.
2. Click **Add** to add a new IPv6 ACL to the switch configuration.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Delete** to remove the currently selected IPv6 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 that can be configured on the switch, it depends on the hardware.
Rules	The number of the rules associated with the IP ACL.
Type	The type is IPv6 ACL.

IPv6 Rules

Use these screens to display the rules for the IPv6 Access Control Lists, which are 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 **Rule ID** to enter a whole number in the range of 1 to 1023 that will be used to identify the rule. An IP ACL may have up to 1023 rules.
2. Use **Action** to specify what action should be taken if a packet matches the rule's criteria. The choices are permit or deny.
3. 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.
4. 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 7). This field is visible for a 'Permit' Action.
5. 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.
6. 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.
7. Use **Match Every** to select true or false from the 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 re-create it, or re-configure 'Match Every' to 'False' for the other match criteria to be visible.
8. There are two ways to configure IPv6 protocol.
   a. Specify an integer ranging from 1 to 255 after selecting the protocol keyword other. This number represents the IP protocol.
   b. Select the name of the protocol from the existing list of Internet Protocols (IPv6), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMPv6).
9. Use **TCP Flag** to specify that a packet's TCP flag is a match condition for the selected IPv6 ACL rule. The TCP flag values are URG, ACK, PSH, RST, SYN, FIN. Each TCP flag has the following possible values and can be set separately:
   - Ignore—A packet matches this ACL rule whether 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.

- When Established is specified, a match occurs if either RST or ACK specified bits are set in the TCP header.
- The following fields are enabled only when TCP protocol is selected.

10. **Protocol** - There are two ways to configure IPv6 protocol.
    a. Specify an integer ranging from 1 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 (IPv6), Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMPv6).

Note: The following fields are enabled only when TCP protocol is selected.

11. Src - Specify a source IPv6 address to match with the selected IPv6 ACL rule.
    - When *IPv6 Address* radio-button is selected, enter an IPv6 address with prefix length to match for the IPv6 ACL rule. If these fields are left empty, it means *any*.
    - When *Host* radio-button is selected, enter a host source IPv6 address to match with specified IPv6 address. If this field is left empty, it means *any*.

    This source IPv6 address argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
12. **Src L4 Port** options are enabled only for TCP or UDP protocols.
    - Source L4 TCP port names are bgp, domain, echo, ftp, ftpdata, http, smtp, telnet, www, pop2, pop3.
    - Source L4 UDP port names are domain, echo, ntp, rip, snmp, tftp, time, who.

    When the Port option is selected, choose port key from the list or enter a port number by yourself. You can enter your own port number only when **Other** is selected in the list of port keys. If this field is left empty, it means *any*.
13. **Src L4 Port Action** specifies the relevant matching condition for layer 4 port numbers in the current extended rule:
    - Equal—IPv6 ACL rule matches only if the layer 4 source port number is equal to the specified port number or port key.
    - Less Than—IPv6 ACL rule matches if the layer 4 source port number is less than the specified port number or port key.
    - Greater Than—IPv6 ACL rule matches if the layer 4 source port number is greater than the specified port number or port key.
    - Not Equal—IPv6 ACL rule matches only if the layer 4 source port number is not equal to the specified port number or port key.
14. **Dst L4 Port** options are enabled only for TCP or UDP protocols.
    - Destination L4 TCP port names are bgp, domain, echo, ftp, ftpdata, http, smtp, telnet, www, pop2, pop3.

- Destination L4 UDP port names are domain, echo, ntp, rip, snmp, tftp, time, who.

When the Port option is selected, choose port key from the list or enter a port number by yourself. You can enter your own port number only when **Other** is selected in the list of port keys. If this field is left empty, it means *any*.

15. **Destination L4 Port Action** specifies the relevant matching condition for layer 4 port numbers in the current extended ACL rule:
    - Equal—IPv6 ACL rule matches only if the layer 4 source port number is equal to the specified port number or port key.
    - Less Than—IPv6 ACL rule matches if the layer 4 source port number is less than the specified port number or port key.
    - Greater Than—IPv6 ACL rule matches if the layer 4 source port number is greater than the specified port number or port key.
    - Not Equal—IPv6 ACL rule matches only if the layer 4 source port number is not equal to the specified port number or port key.
16. Fragments—Specifies the rule to match the packets that are non-initial fragments (fragment bit asserted). This option is not valid for rules that match L4 information such as TCP port number, since that information is carried in the initial packet.
17. Routing—Specifies the rule to match the packets that have a routing extension header.
18. ICMPv6 Type - Specifies a match condition for ICMP packets.
    - When *Type* radio-button is selected, IPv6 ACL rule matches with the specified ICMPv6 message type, a possible type number is in range from 0 to 255. When ICMPv6 code is specified, IP ACL rule matches with the specified ICMPv6 message code. Possible value is in range from 0 to 255. If these fields is left empty, it means 'any'.
19. When *Message* radio-button is selected, choose type of the ICMPv6 message to match with the selected IPv6 ACL rule.
    - Specifying Message implies that both ICMPv6 type and ICMPv6 code are specified. ICMPv6 message is decoded into corresponding ICMPv6 type and ICMPv6 code within that ICMPv6 type. IPv6 ICMPv6 message types: destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, port-unreachable, router-solicitation, router-advertisement, router-renumbering, time-exceeded and unreachable.

Note: The following fields are enabled only if the protocol is ICMPv6.

20. **Flow Label** - Flow label is 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers. Flow label can specified within the range (0 to 1048575).
21. Use **IPv6 DSCP Service** to specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IPv6 header. This is an optional configuration. Enter an integer from 0 to 63. The IPv6 DSCP is selected by possibly

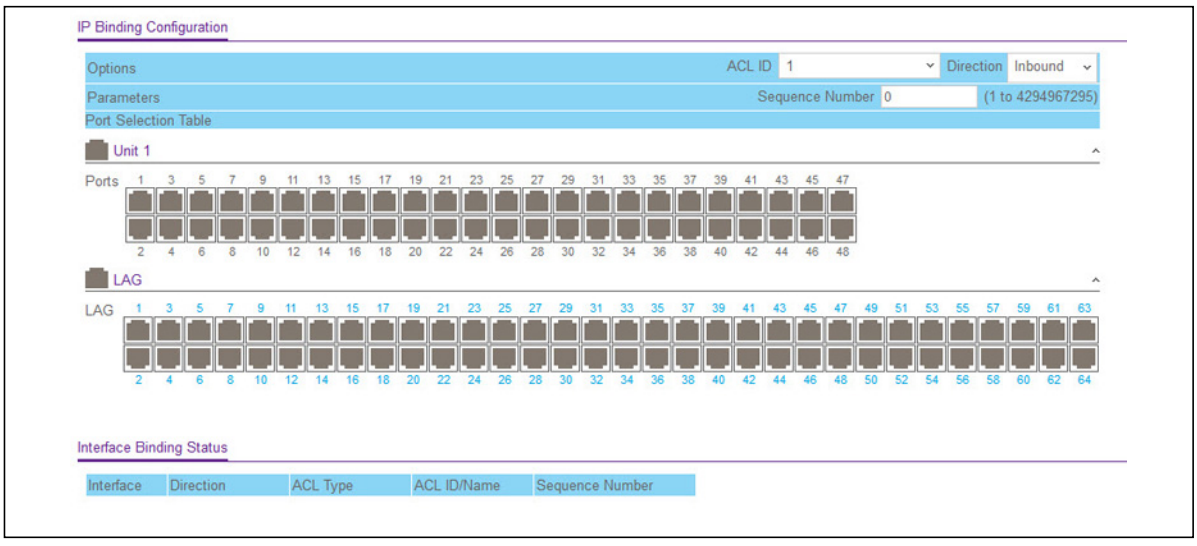
selection one of the DSCP keyword from a drop-down box. If a value is to be selected by specifying its numeric value, then select the 'Other' option in the drop-down box and a text box will appear where the numeric value of the DSCP can be entered.

22. **Rate Limit Conform Data Rate** - Value of Rate Limit Conform Data Rate specifies the conforming data rate of IPv6 ACL Rule. Valid values are (1 to 4294967295) in Kbps.
23. **Rate Limit Burst Size** - Value of Rate Limit Burst Size specifies burst size of IPv6 ACL Rule. Valid values are (1 to 128) in Kbytes.
24. **Time Range** - Name of time range associated with the IPv6 ACL Rule.
25. **Rule Status** - Displays if the ACL rule is active or inactive. Blank means that no timer schedules are assigned to the rule.
26. To modify an existing IP Extended ACL rule, click the **Rule ID**. The number is a hyperlink to the Extended IPv6 ACL Rule Configuration (100-199) screen, which is used for configuration ACL Rules. Click the **Add** button on the IP Extended Rules screen.
27. For standard ACL Rule Configuration (1-99), click the **Add** button on the IPv6 Rules screen.
28. Use **Delete** to select the check box 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.

Note: Binding ACLs to interface fails when the system has no resources to bind a new ACL. IPv4 ACLs and IPv6 ACLs cannot be bound at the same time to an interface.

2. Select the packet filtering **Direction** for ACL. Valid directions are Inbound or Outbound. The packet filtering direction for ACL is Inbound, which means the IP ACL rules are applied to traffic entering the port.
3. 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.

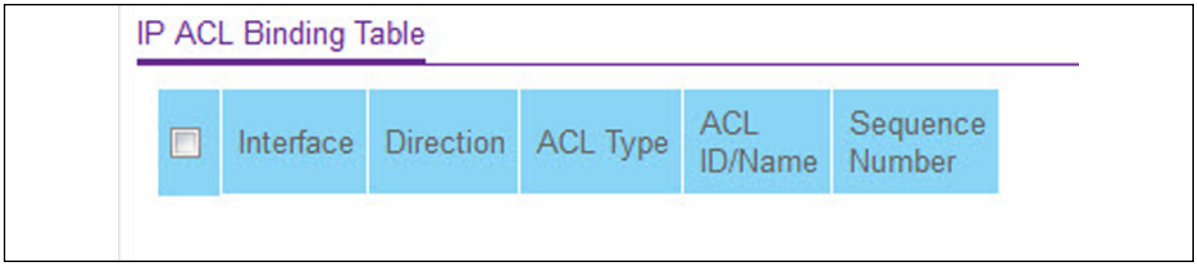
   A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user (meaning that the value is 0), a 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.
4. The **Port Selection Table** lists all available valid interfaces for ACL mapping. All non-routing physical interfaces, and interfaces participating in LAGs, are listed. Click the appropriate unit name to expose the available ports or LAGs.
   - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that 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.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. Click **Apply** to 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 ACL Binding Table

Use the IP ACL 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**.

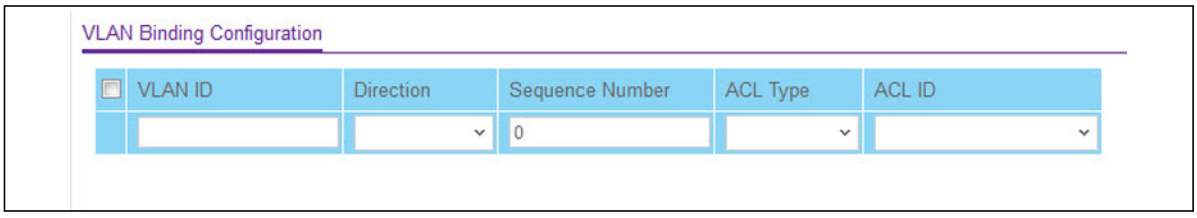


Table 161, ACL VLAN Binding Table on page 495 describes the information displayed in the **ACL VLAN Binding Table**.

1. Use **ACL Type** to specify the type of ACL. Valid ACL Types include IP ACL, MAC ACL, and IPv6 ACL.
2. Use **ACL ID** to display all the ACLs configured, depending on the ACL Type selected.

Table 161. ACL VLAN Binding Table

Field	Description
Direction	Specifies the packet filtering direction for ACL.
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).

3. Click **Add** to add a VLAN ID to the selected ACL ID.
4. To delete a VLAN ACL-to-interface binding, select the check box next to the interface and click **Delete**.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

7. Monitoring the System

Use the features available from the Monitoring tab to view a variety of information about the switch and its ports and to configure how the switch monitors events. The **Monitoring** tab contains links to the following features:

- *Ports* on page 496
- *Logs* on page 506
- *Mirroring* on page 513
- *sFlow* on page 515

Ports

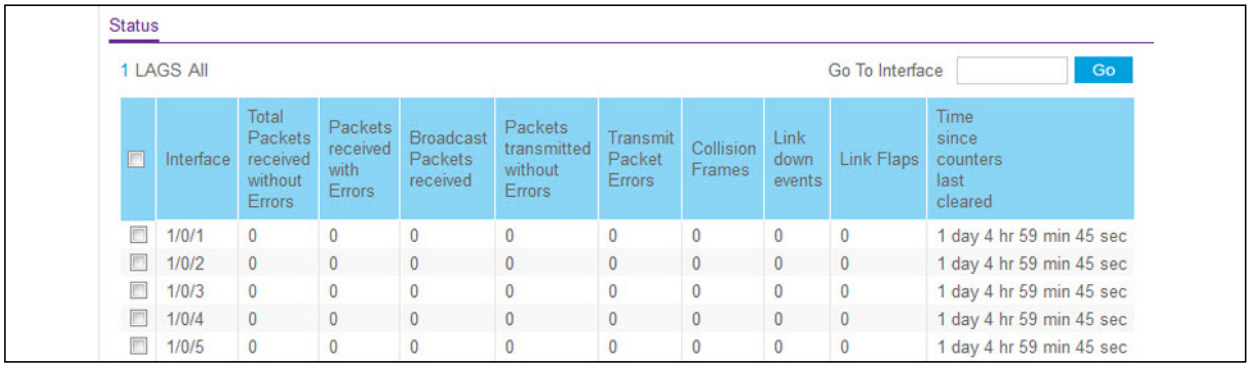
The pages available from the Ports link contain a variety of information about the number and type of traffic transmitted from and received on the switch. From the Ports link, you can access the following pages:

- *Port Statistics* on page 496
- *Port Detailed Statistics* on page 498
- *EAP Statistics* on page 504
- *Cable Test* on page 505

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 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:

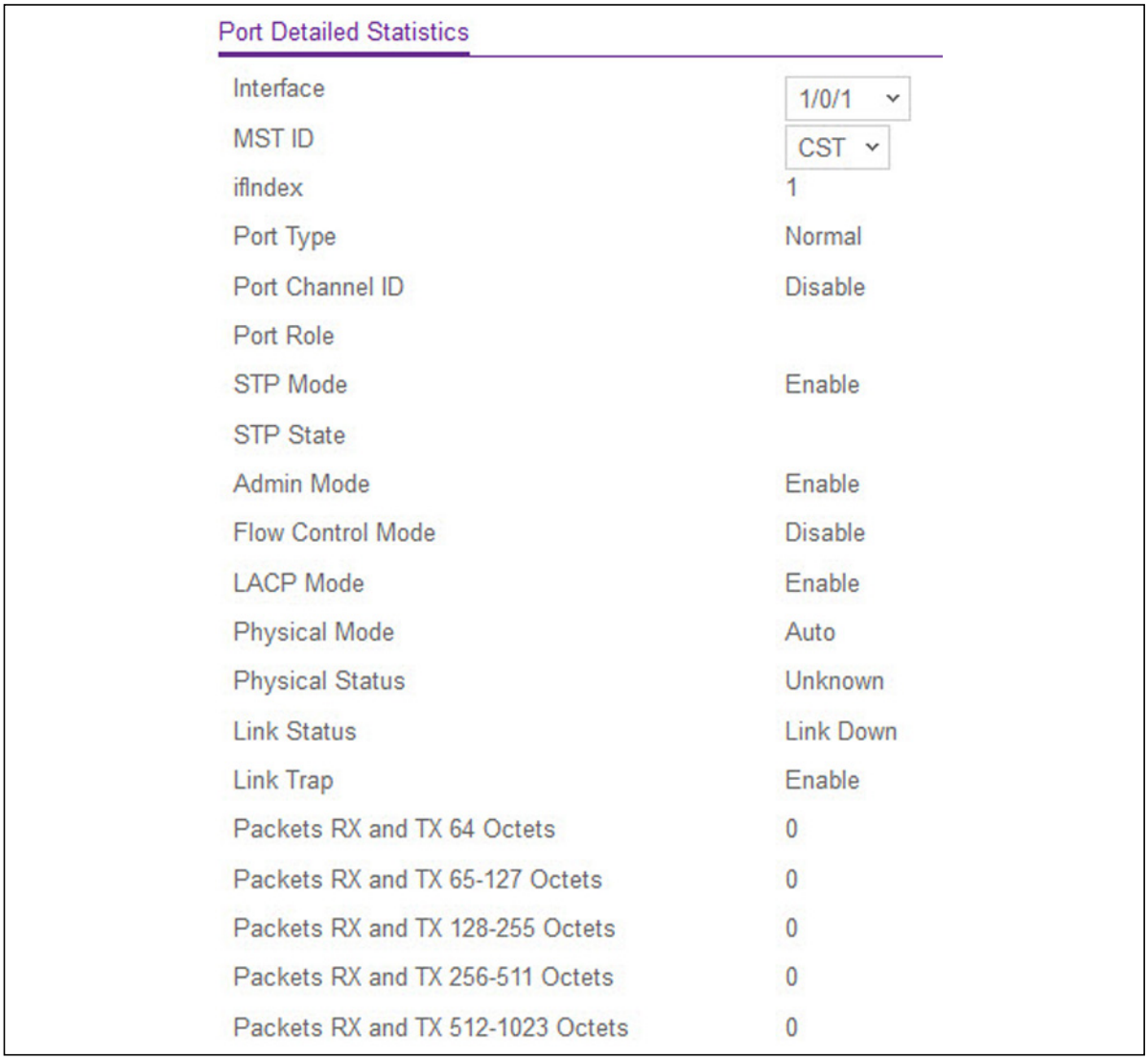
- To clear all the counters for all ports on the switch, select the check box in the row heading and click **Clear**. The button resets all statistics for all ports to default values.
- To clear the counters for a specific port, select the check box associated with the port and click **Clear**.
- Click **Update** to update the page with the latest information on the switch.

Field	Description
Interface	This object indicates the interface of the interface table entry associated with this port on an adapter.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that have been transmitted by this port to its segment.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The best estimate of the total number of collisions on this Ethernet segment.
Number of Link Down Events	The total number of link down events on a physical port.
Link Flaps	The total number of occurrences of link down to link up event (makes one link flap) during debouncing time.
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**. (The following figure shows some, but not all, of the fields on the Port Detailed Statistics page.)



The figure above shows only partial information for the page.

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 **Update** to update the page with the latest information on the switch.

Field	Description
MST ID	Display the MST instances associated with the interface.
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: • Mirrored - This port is a participating in port mirroring as a mirrored port. Look at the Port Mirroring screens for more information. • Probe - This port is a participating in port mirroring as the probe port. Look at the Port Mirroring screens for more information. • Trunk Member - The port is a member of a Link Aggregation trunk. Look at the Port Channel screens for more information.
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, Designated, Alternate, Backup, Master, or Disabled.
STP Mode	The Spanning Tree Protocol Administrative Mode associated with the port or Port Channel. The possible values are: • Enable - Spanning tree is enabled for this port. • Disable - Spanning tree is disabled for this port.
STP State	The port's current 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 five states are defined in IEEE 802.1D: • Disabled • Blocking • Listening • Learning • Forwarding • Broken
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.
Flow Control Mode	Indicates whether flow control is enabled or disabled for the port. This field is not valid for Lag interfaces.
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.

Field	Description
Link Trap	Indicates whether or not the port will send a trap when link status changes.
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1519-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Received 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
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).

Field	Description
Packets Received 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received > 1518 Octets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Total Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
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

Field	Description
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Total Received Packets Not Forwarded	A count of valid frames received which were discarded (i.e. filtered) by the forwarding process.
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.
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).
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.

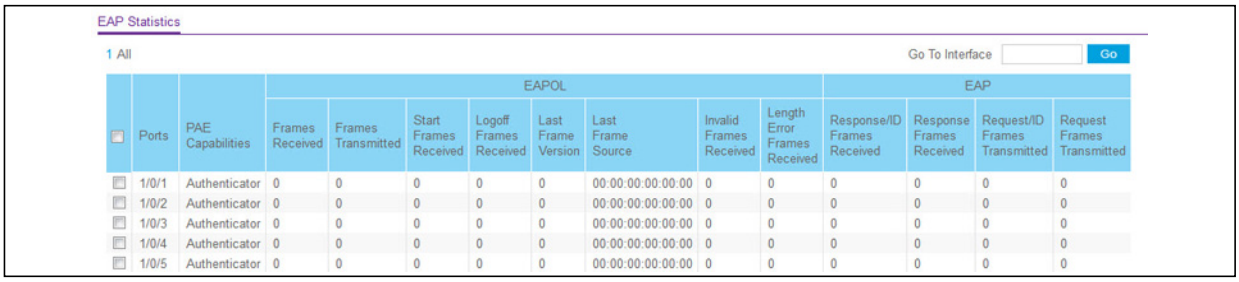
Field	Description
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested 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.
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.
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.

Field	Description
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**.



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:

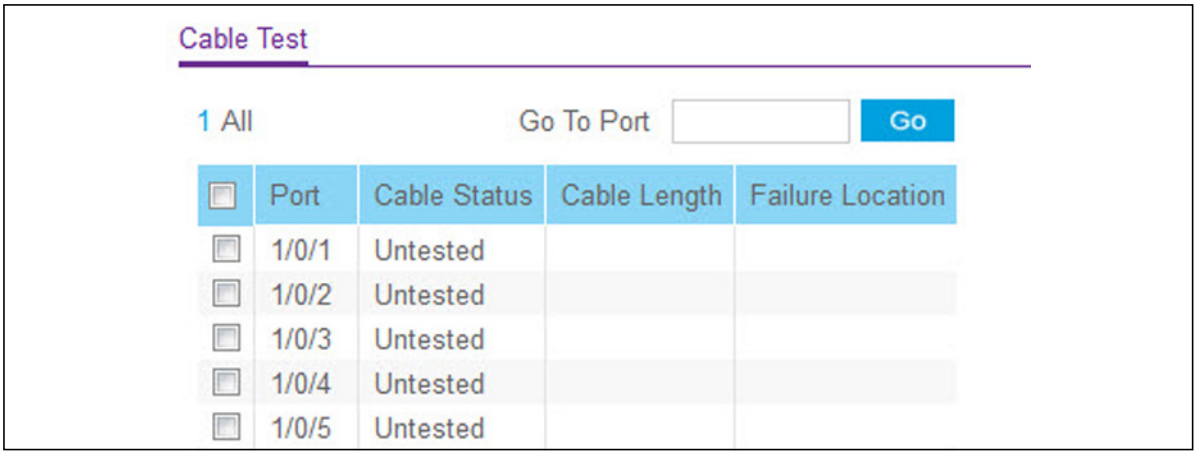
- To clear all the EAP counters for all ports on the switch, select the check box in the row heading and click **Clear**. The button resets all statistics for all ports to default values.
- To clear the counters for a specific port, select the check box associated with the port and click **Clear**.
- Click **Update** to update the page with the latest information on the switch.

Field	Description
Port	Selects the port to be displayed. When the selection is changed, a screen update 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.

Field	Description
EAPOL Logoff Frames Received	This displays the number of EAPOL logoff frames that have been received by this authenticator.
EAPOL Last Frame Version	This displays the protocol version number carried in the most recently received EAPOL frame.
EAPOL Last Frame Source	This displays the source MAC address carried in the most recently received EAPOL frame.
EAPOL Invalid Frames Transmitted	This displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAPOL Length Error Frames Received	This displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Response/ID Frames Received	This displays the number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	This displays the number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/ID Frames Transmitted	This displays the number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	This displays the number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.

Cable Test

To display the Cable Test page, click **Monitoring** > **Ports**> **Cable Test**.



1. **Port** - 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, 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	This displays the cable status as Normal, Open or Short. • Normal: the cable is working correctly. • Open: the cable is disconnected or there is a faulty connector. • Short: there is an electrical short in the cable. • Cable Test Failed: The cable status could not be determined. The cable may in fact be working. • Untested: The cable is not yet tested. • Invalid cable type: The cable type is unsupported.
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.

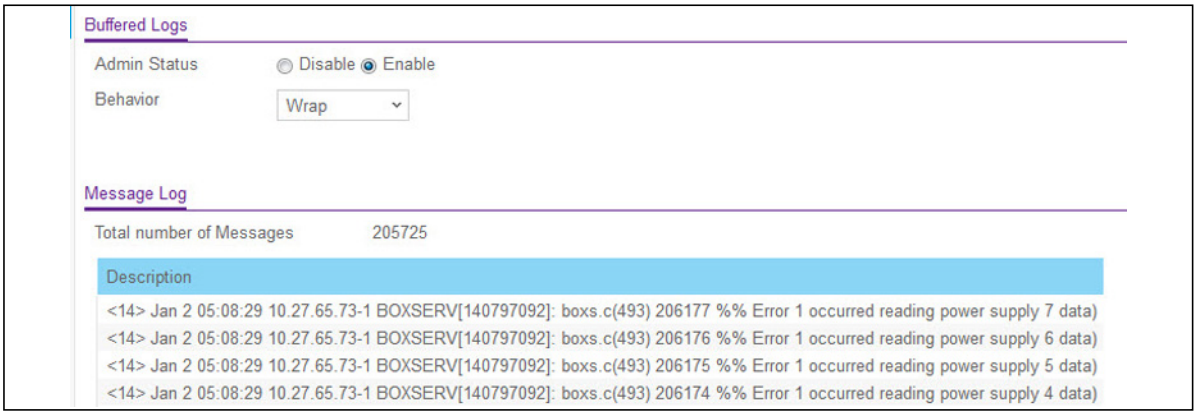
Logs

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 pages:

Buffered Logs

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



Buffered Log Configuration

This log stores messages in memory based upon the settings for message component and severity. On chassis systems, this log exists only on the top of chassis platform. Other platforms in the chassis forward their messages to the top of chassis 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 **Update** to update the page with the latest information on the switch.
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:

- <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 chassis 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.

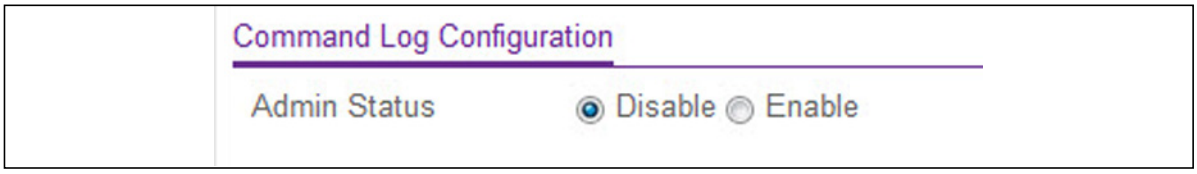
  The above example indicates a user-level message (1) with severity 7 (debug) on a system that is not a chassis and generated by component MSTP running in thread id

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 screen.

Command Log Configuration

To access the Command Log Configuration page, click **Monitoring** > **Logs > Command Log Configuration**.

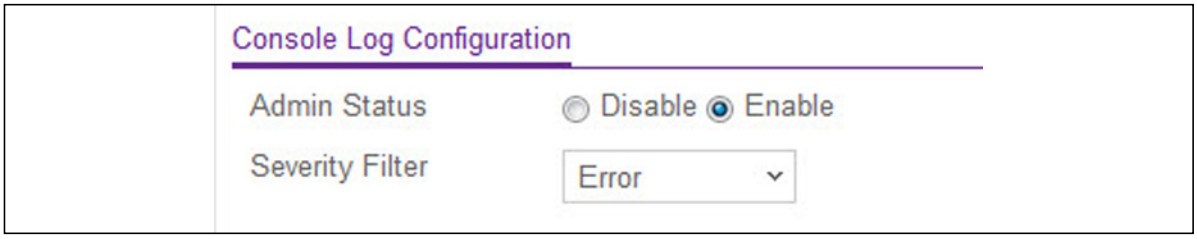


1. Use **Admin Mode** to enable/disable the operation of the CLI Command logging by selecting the corresponding radio button.

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**.

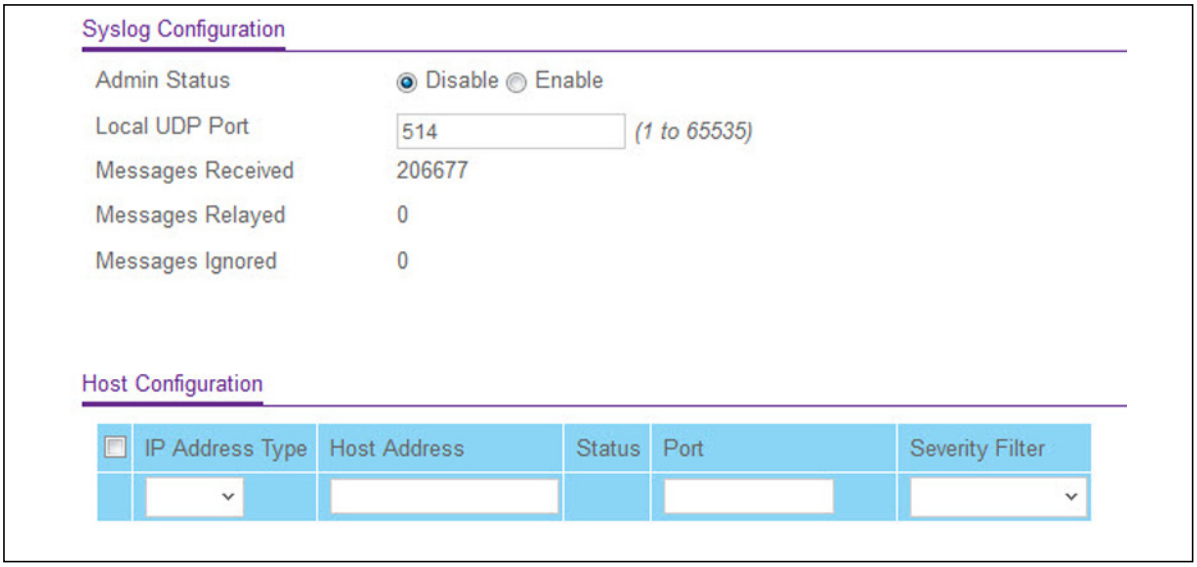


1. A log that is “Disabled” shall not log messages. A log that is “Enabled” shall log messages. Enable or Disable logging by selecting the corresponding radio button.
2. **Severity Filter**. A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the drop-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 > Syslog Configuration**.



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 Received	The number of messages received by the log process. This includes messages that are dropped or ignored.
Messages Relayed	The count of syslog messages relayed.
Messages Ignored	The count of syslog messages ignored.

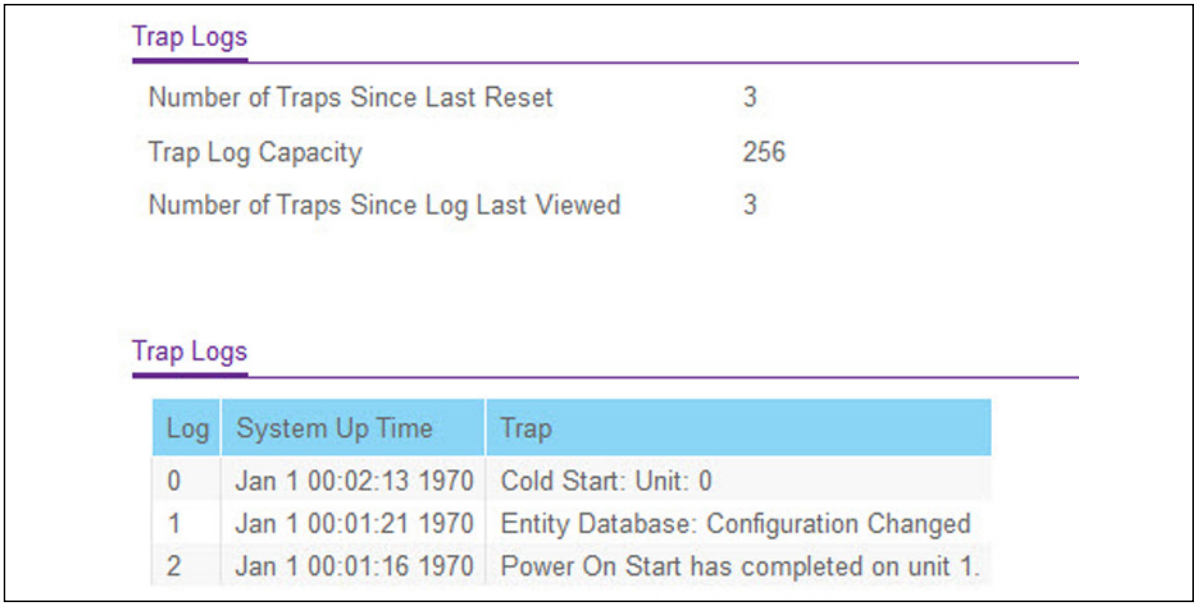
3. Use **IP Address Type** to specify the Address Type of Host. It may be one of the following:
   - IPv4
   - IPv6
   - DNS
4. **Host Address** - This is the address of the host configured for syslog.
5. **Port** - This is the port on the host to which syslog messages are sent. The default port is 514. Specify the port in the text field.

6. **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 drop-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

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**.



The following table describes the Trap Log information displayed on the screen.

The page also displays information about the traps that were sent.

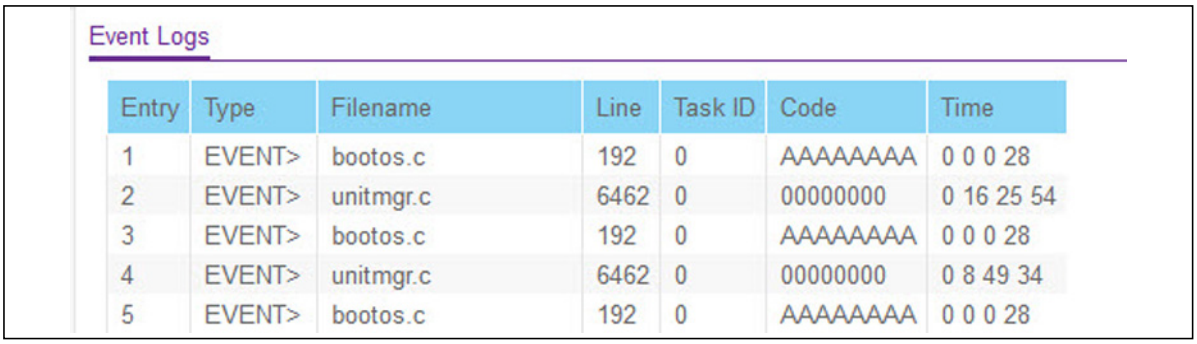
Click **Clear** to clear all the counters. This resets all statistics for the trap logs to the default values.

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**.



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 **Update** to update the page with the latest information on the switch.

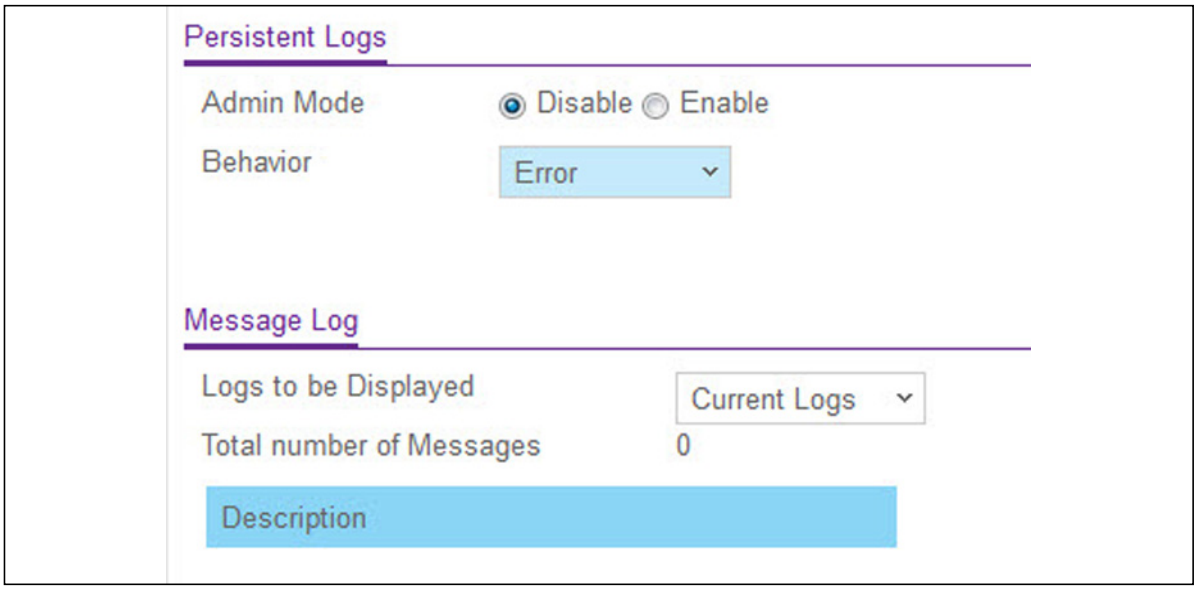
Field	Description
Entry	The sequence number of the event.
Type	The type of the event.
File Name	The file in which the event originated.

Field	Description
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 drop-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 drop-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 **Update** to update the page with the latest information on the switch.

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 a chassis 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.

Mirroring

The page under the Mirroring link allows you to view and configure port mirroring on the system.

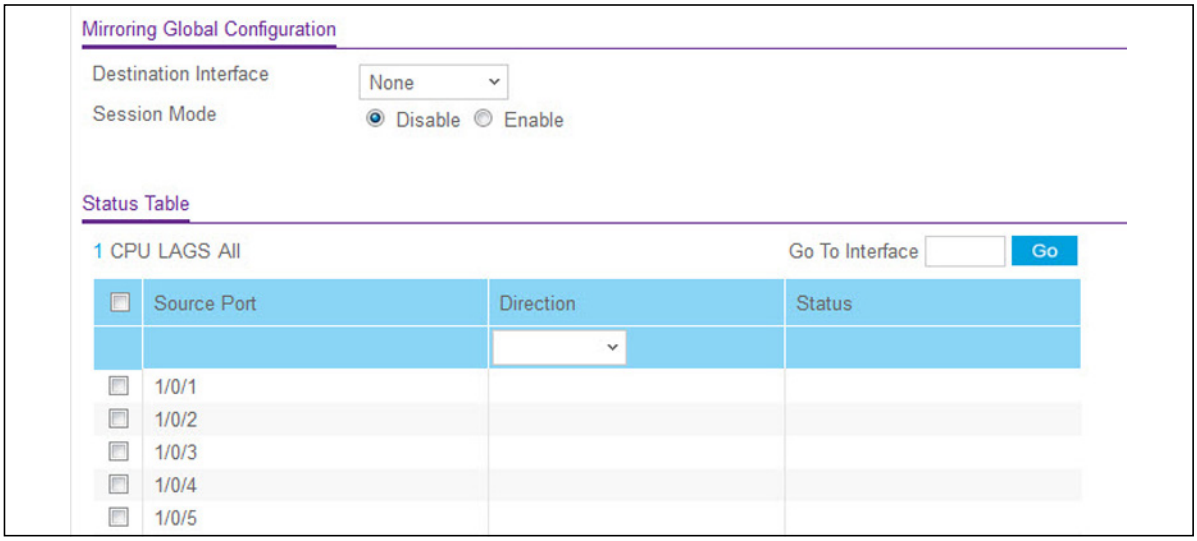
Multiple Port Mirroring

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 > Multiple Port Mirroring**.



To configure Port Mirroring:

1. In the **Destination Interface** field, specify the port to which port traffic is to be copied. You can configure only one destination port on the system. It acts as a probe port and will receive all the traffic from configured mirrored port(s). If the value is not configured, it will be shown as None. The default value is None.
2. 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.

   The default mode is Disable.
3. Select the option next to a port to configure it as a source port.
4. 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.
5. In the **Direction** field, specify the direction of the Traffic to be mirrored from the configured mirrored port(s). If the value is not configured, it is shown as blank. The default value is blank. Direction options are:
   - Tx and Rx—Monitors transmitted and received packets.
   - Tx Only—Monitors transmitted packets only.
   - Rx Only—Monitors received packets only.
6. Click **Apply** to apply the settings to the system. If the port is configured as a source port, the **Mirroring Port** field value is Mirrored.
7. To delete a mirrored port, select the option 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.

Note: In case of an error dialog having multiple error messages, resolve them to get the remaining set of errors, if any.

Field	Description
Status	A non-configurable field indicating 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 515
- *Advanced* on page 516

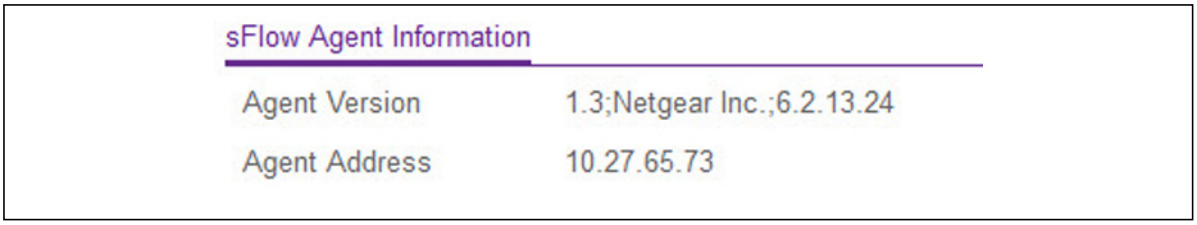
Basic

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

- *sFlow Agent Information* on page 515

sFlow Agent Information

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



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: • MIB Version: '1.3', the version of this MIB. • Organization: NETGEAR Inc. • Revision: 1.0
Agent Address	The IP address associated with this agent.

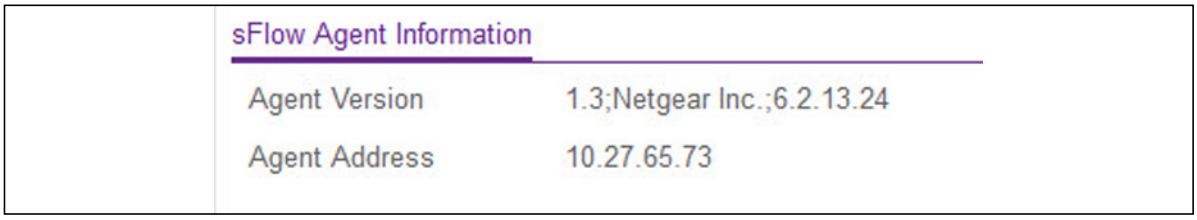
Click **Update** to update the page with the latest information on the switch.

Advanced

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

sFlow Agent

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

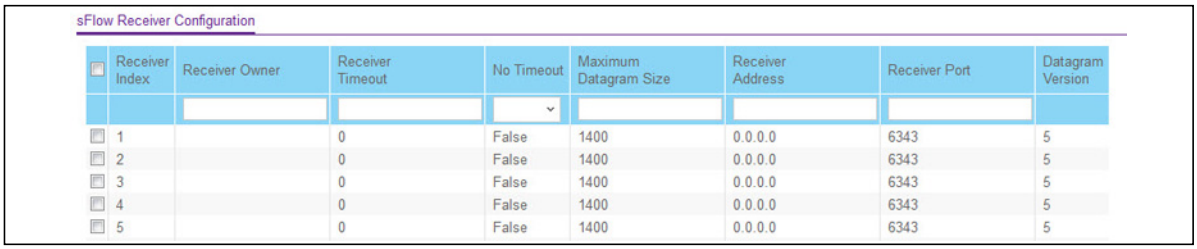


Field	Description
Agent Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version;Organization;Software Revision where: • MIB Version: '1.3', the version of this MIB. • Organization: NETGEAR Inc. • Revision: 1.0
Agent Address	The IP address associated with this agent.

Click **Update** to update the page with the latest information on the switch.

sFlow Receiver Configuration

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



1. **Receiver Owner** - 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.

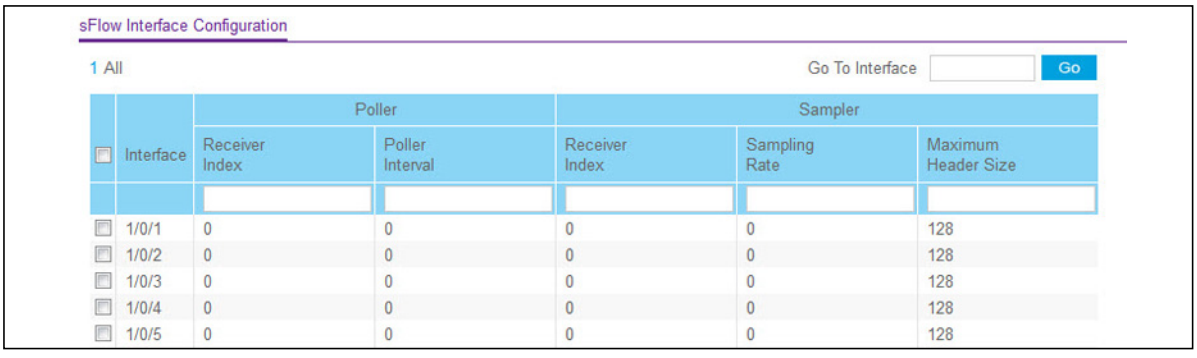
2. **Receiver Timeout** - The time (in seconds) remaining before the sampler is released and stops sampling. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. Valid range is (0 to 2147483647). A value of zero sets the selected receiver configuration to its default values.
3. Use **No Timeout** to select True or False from the menu to set the no timeout sampling for the receiver. Sampling will not be stopped until 'No Timeout' selected entry is True. The default value is False.
4. **Maximum Datagram Size** - 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. **Receiver Address** - The IP address of the sFlow collector. If set to 0.0.0.0 no sFlow datagrams will be sent.
6. **Receiver Port** - 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**.



1. **Interface** displays the interface for this flow poller and sampler. This Agent will support Physical ports only.
2. Use **Poller 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 seconds.
4. Use **Sampler 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.

8 Maintenance

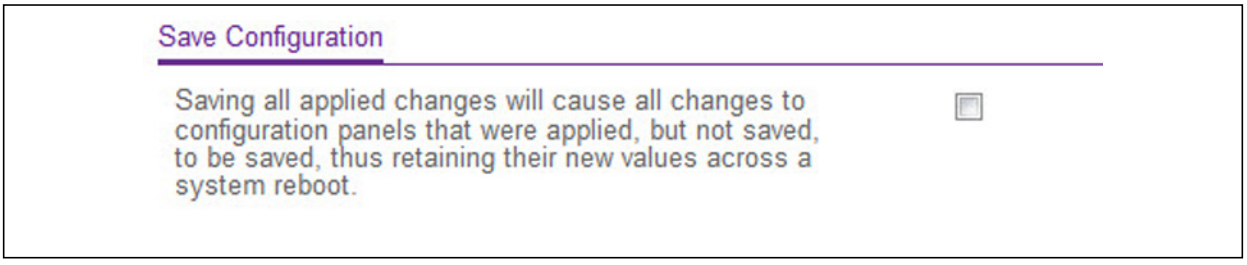
Use the features available from the Maintenance tab to help you manage the switch. The Maintenance tab contains links to the following features:

Save Configuration

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

Save Configuration

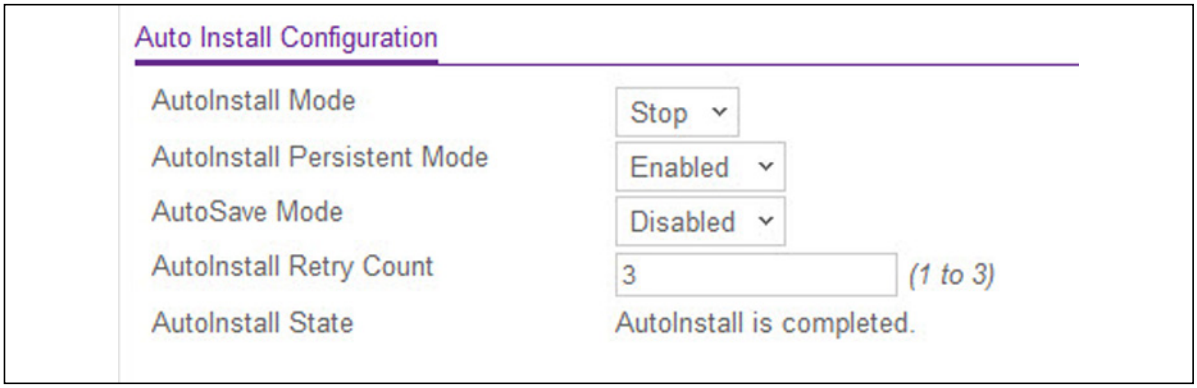
To access the Save Configuration page, click **Maintenance** > **Save Config**> **Save Configuration**.



1. Select the check box and click the **Apply** button to have configuration changes you have made saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

Auto Install Configuration

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



1. Use **Auto Install** to select the start/stop auto install mode on the switch.
2. Use **AutoInstall Persistent Mode** to enable/disable AutoInstall persistent mode.
3. Use **AutoSave Mode** to select Enabled/Disabled 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.
4. Use **AutoInstall 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.

Field	Description
AutoInstall State	Displays the current status of the AutoInstall process.

Reset

The **Reset** menu contains links to the following options:

- *Device Reboot* on page 520
- *Power Cycle* on page 521
- *Factory Default* on page 521
- *Password Reset* on page 522

Device Reboot

Use the Device Reboot page to reboot M6100 Chassis switch.

To access the Device Reboot page, click **Maintenance** > **Reset** > **Device Reboot**.

To reboot the switch:

1. In the **Reboot Unit No**. field, select the unit to reset. When multiple units are connected in a chassis, select **All** to reset all the units in the stack (in other words, the whole chassis) or select the unit number to reset only the specific unit.
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.

Power Cycle

Use the Power Cycle page to reboot the blade if it is not responding. To access the Power Cycle page, click **Maintenance** > **Reset** > **Power Cycle**. The following page is displayed.

➢ **To reboot the switch:**

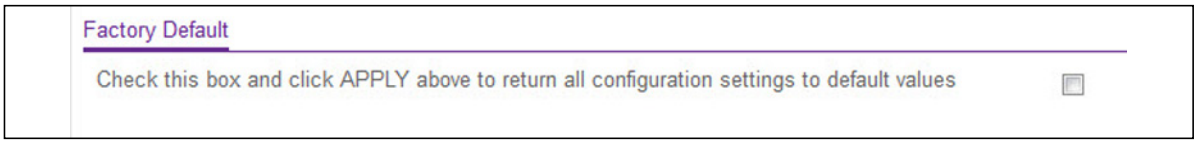
1. Select the slot from the list.
2. Click **Apply** to do the hardware switch reboot.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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

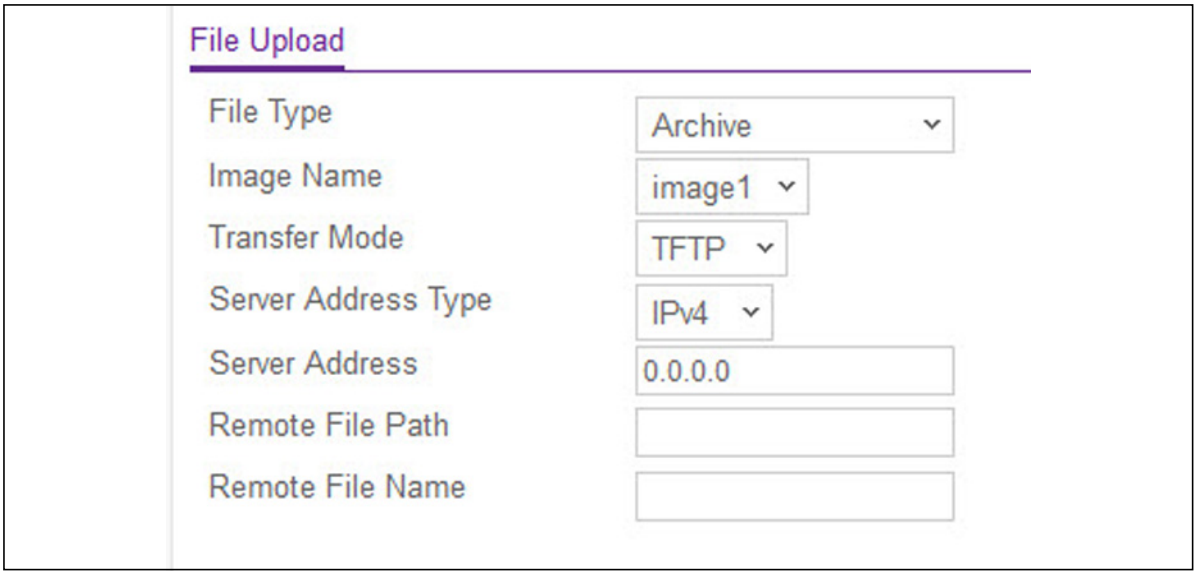
Use the File Upload page to upload configuration (ASCII), log (ASCII), and image (binary) files from the switch to the TFTP server.

The Upload menu contains links to the following options:

- *File Upload* on page 523
- *HTTP File Upload* on page 524
- *USB File Upload* on page 525

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.
   - **CLI Banner** - Specify CLI Banner when you want to retrieve the CLI banner file.
   - **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 trouble-shooting.
   - **Crash Logs** - Specify Crash Log to retrieve the crash logs.

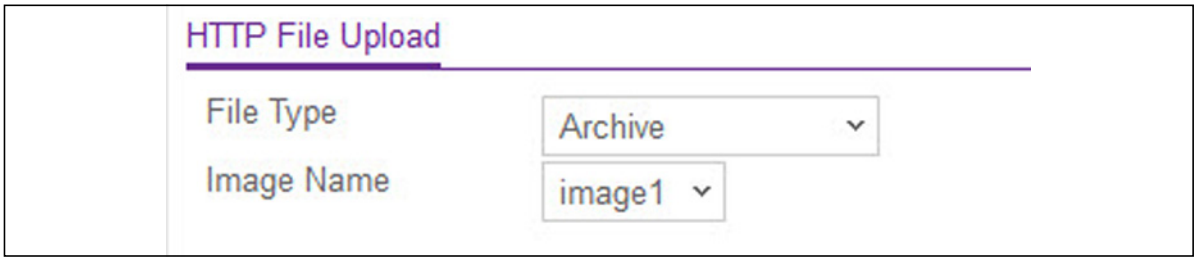
   The factory default is Archive.
2. The **Image Name** field is only visible when the selected File Type is Archive. If you are uploading a switch image (Archive), use the **Image Name** list to select the software image on the switch to upload to the management system:
   - **image1** - Select image1 to upload image1.
   - **image2** - Select image2 to upload image2
3. 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
- **FTP** - File Transfer Protocol

4. Use **Server Address Type** to specify either IPv4, IPv6 or DNS to indicate the format of the Server Address field. The factory default is IPv4.
5. 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.
6. Use **Remote File Path** to enter the path where you want to upload the file. File path may include alphabetic, numeric, forward slash, dot or underscore characters only. You may enter up to 160 characters. The factory default is blank.
7. 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.
8. Use **Local File Name** to specify the local script file name you want to upload. This field is visible only when File Type is Script File.
9. 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.
10. 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.
11. 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:
   - **Image Name** - Select one of the images from the list:
     - **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.
   - **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.
- **Crash Logs** - Specify Crash Logs to retrieve the system crash logs.

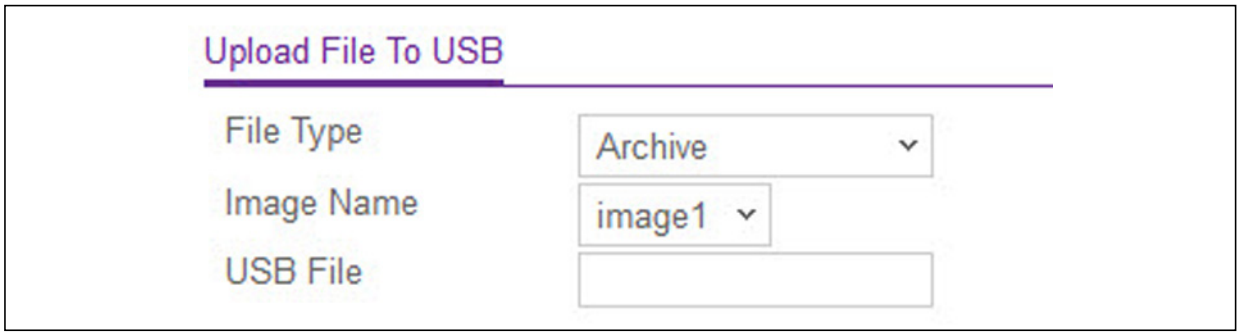
The factory default is Archive.

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:
   - **Text Configuration** to specify configuration in text mode when you want to retrieve the stored configuration. The factory default is **Archive**.
2. Use **Image Name** to select one of the images from the list:
   - **Image1** - Specify the code image1 when you want to retrieve.
   - **Image2** - Specify the code image2 when you want to retrieve.
3. 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.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

Download File To Switch

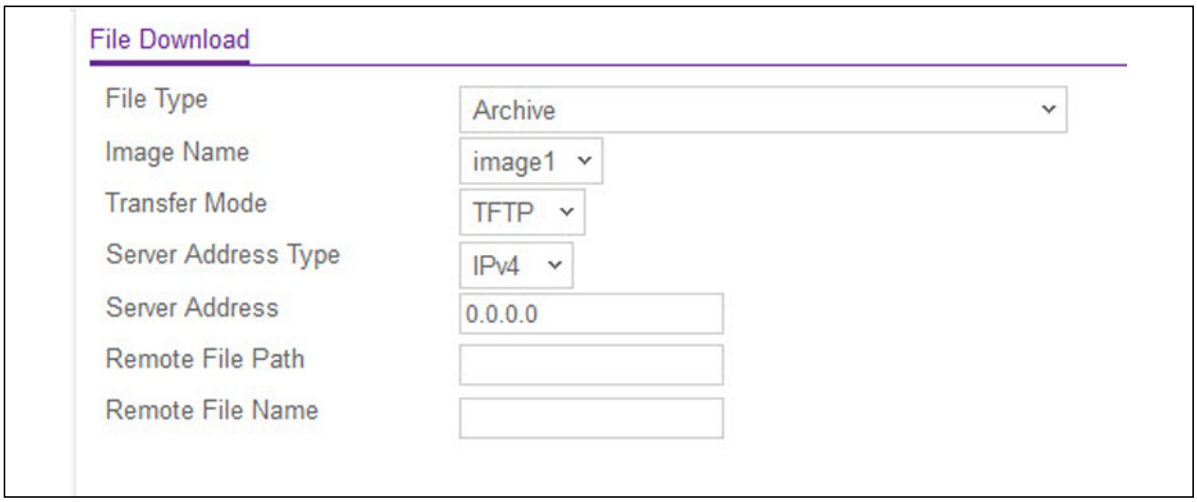
The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.

The Download menu contains links to the following options:

- *File Download* on page 526
- *HTTP File Download* on page 528
- *USB File Download* on page 530

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.
   - **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).
- Use **IAS Users** to specify the Internal Authentication Server Users Database File.

The factory default is Archive.

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 **Image Name** to select one of the images from the list:
   - **Image1** - Specify the code image1 when you want to retrieve.
   - **Image2** - Specify the code image2 when you want to retrieve.

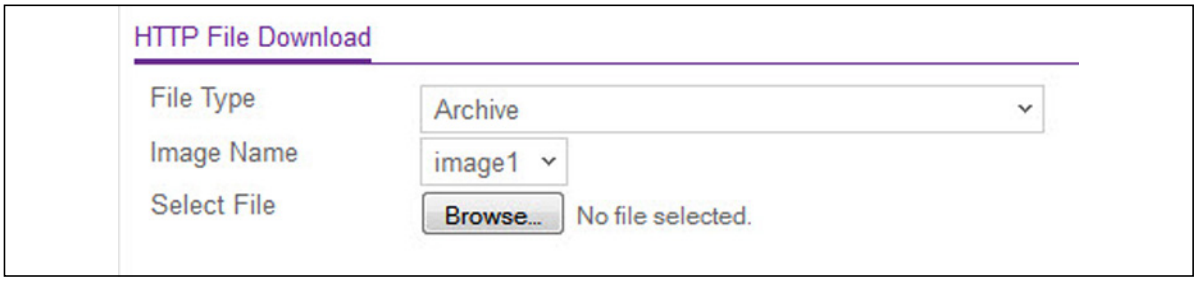
   The Image Name field is visible only when File Type **Archive** is selected.
3. Use **Transfer Mode** to specify what protocol to use to transfer the file:
   - **TFTP** - Trivial File Transfer Protocol
   - **SFTP** - Secure File Transfer Program
   - **SCP** - Secure Copy
   - **FTP** - File Transfer Protocol
4. Use **Server Address Type** to specify either IPv4, IPv6 or DNS to indicate the format of the TFTP/SFTP/SCP Server Address field. The factory default is IPv4.
5. Use **Server Address** to enter the IP address of the TFTP server in accordance with the format indicated by the Server Address Type, for example an IP address in the x.x.x.x format. The factory default is the IPv4 address 0.0.0.0.
6. Use **Remote File Path** to enter the path of the file which you want to download. The file path cannot include the following symbols: ' \:*?”<>| '. Up to 160 characters can be entered. The factory default is blank.

7. Use **Remote File Name** to enter the name of the file you want to download from the server. The file path cannot include the following symbols: ' \:*?”<>| '. You may enter up to 32 characters. The factory default is blank.
8. 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.
9. 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.
10. The last row of the table is used to display information about the progress of the file transfer. It is displayed only after the process starts. The screen will refresh automatically until the file transfer completes.
11. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
12. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

HTTP File Download

Use the HTTP File Download page to download files of various types to the switch using an HTTP session (for example, via your Web browser).

To display this page, click **Maintenance** > **Download** > **HTTP File Download**.



To download a file to the switch by using HTTP:

1. Use **File Type** to specify what type of file you want to transfer:
   - **Archive** - Specify archive (STK) code when you want to upgrade the operational flash:
     - **Image1** - Specify the code image1 you want to download.
     - **Image2** - Specify the code image2 you want to download.
   - **CLI Banner** - Specify CLI Banner when you want a banner to be displayed before the login prompt.
   - **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).
- Use **IAS Users** to specify the Internal Authentication Server Users Database File.

The factory default is Archive.

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 **Image Name** to select one of the images from the list:
   - **Image1** - Specify the code image1 when you want to retrieve.
   - **Image2** - Specify the code image2 when you want to retrieve.
3. 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.
4. Click **BROWSE** to open a file upload window to locate the file you want to download. The factory default is blank.
5. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
6. Click the **Apply** button to initiate the file download.

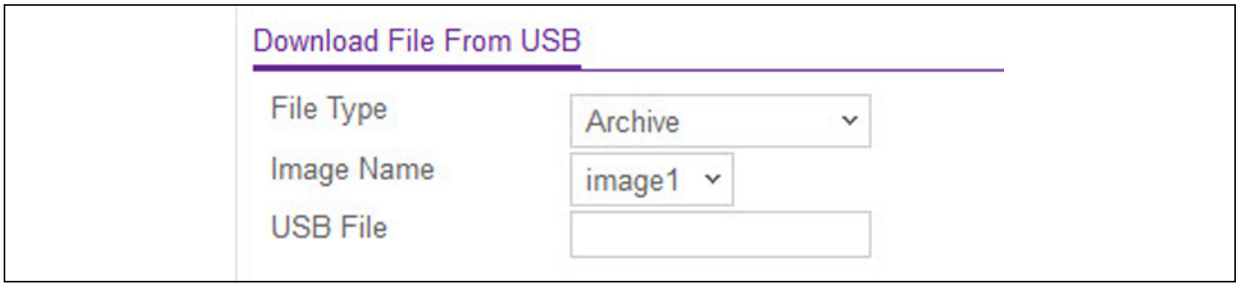
Note: After a file transfer is started, please wait until the page refreshes. When the page refreshes, the *Select File* option will be blanked out. This indicates that the file transfer is done.

7. **Download Status** - Displays the status during transfer file to the switch.

USB File Download

Use this menu to download a file to the switch from a USB device.

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



1. Use **File Type** to specify what type of file you want to download:
   - **Archive** - Specify archive (STK) code when you want to download to the operational flash.
   - **Text Configuration** to specify configuration in text mode when you want to update the switch's configuration (Startup-config). If the file has errors, the update will be stopped. The factory default is **Archive**.
2. Use **Image Name** to select one of the images from the list:
   - **Image1** - Select image1 to download to image1.
   - **Image2** - Select image2 to download to image2.

   This field is visible only when File Type **Archive** is selected.
3. Use **USB File** to give a name along with path for the file you want to download. You may enter up to 32 characters. The factory default is blank.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Download Status displays the status of the file transfer to the switch. The last row of the table is used to display information about the progress of the file transfer. It is displayed only after the process starts. The screen will refresh automatically until the file transfer completes.

File Management

The system maintains two versions of the M6100 Chassis switch software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded during subsequent switch restarts. This feature reduces switch down time when upgrading or downgrading the M6100 Chassis switch software.

The **File Management** menu contains links to the following options:

- *Copy* on page 531

- *Dual Image Configuration* on page 531

Copy

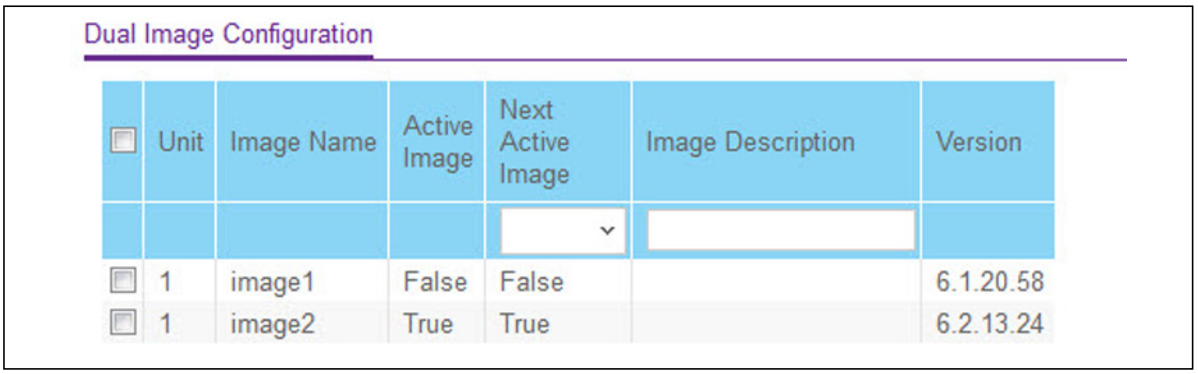
To display the Copy page, click **Maintenance** > **File Management** > **Copy**.

1. Use **Source Image** to select the image1 or image2 as source image, the image you want to copy from, when copy occurs.
2. Use **Chassis Member** to select the destination unit to which you are going to copy from the supervisor.
3. Use **Destination Image** to select the image1 or image2 as destination image, where you want to copy the source image to, when copy occurs.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

Dual Image Configuration

The Dual Image feature allows the 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**.



To configure Dual Image settings:

1. Use **Unit** to select the unit whose code image you want to activate, update, or delete.
2. Use **Next Active Image** to make the selected image the next active image for subsequent reboots.
3. Use **Image Description** to specify the description for the image that you have selected.
4. Click **Delete** to delete the selected image from permanent storage on the switch.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

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 532
- *Ping IPv6* on page 534
- *Traceroute IPv4* on page 535
- *Traceroute IPv6* on page 537
- *Full Memory Dump* on page 538

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 a specified number of ping requests and the results will be displayed.

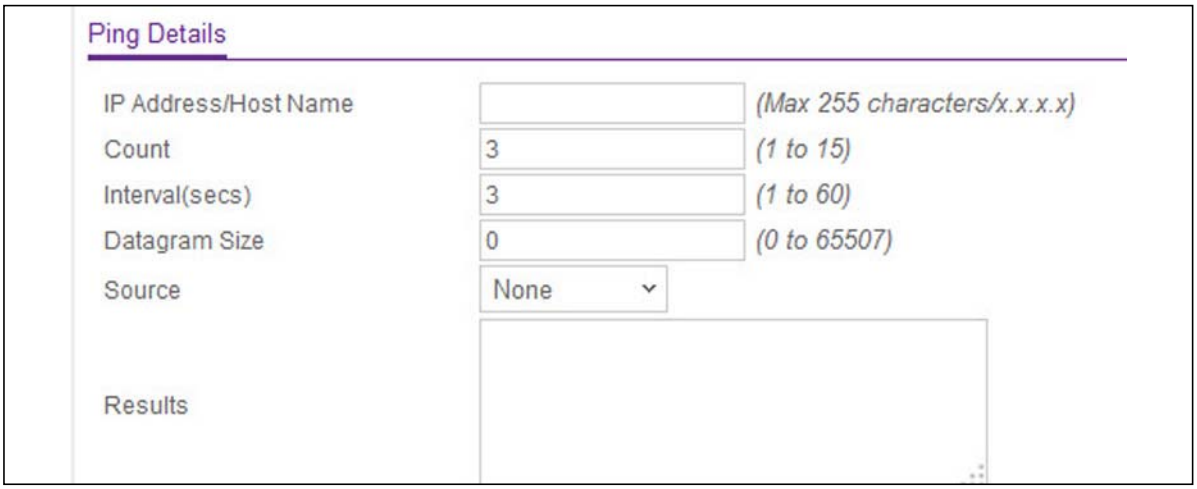
If a reply to the ping is not received, you will see:

```
Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec
```

If a reply to the ping is received, you will see:

```
Reply From a.b.c.d: icmp_seq = 0. time= xyz usec.
Reply From a.b.c.d: icmp_seq = 1. time= abc usec.
Reply From a.b.c.d: icmp_seq = 2. time= 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**.



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.
2. Enter the **Count,** the number of echo requests you want to send. The initial value is the default value. The default value is 3. The range is 1 to 15.
3. Enter the **Interval** between ping packets in seconds. The initial value is the default value. The default value is 3 seconds. The range is 1 to 60.
4. Enter the **Datagram Size** of ping packet. The initial value is the default value. The default value is 0 bytes. The range is 0 to 65507.
5. Enter the **Source** IP address or interface to use when sending the echo request packets. If source is not required, select None as the source option. Possible values are:
   - None—The source address of the ping packet would be the address of the default outgoing interface.
   - IP Address—The source IP address to use when sending the Echo request packets. This field is shown when **IP Address** is selected as the source option.
   - Interface—The interface to use when sending the Echo request packets. This field is shown when **Interface** is selected as the source option.

Note: Values configured in the fields above are not saved to the switch. As a result, refreshing the page sets these fields to the default values.

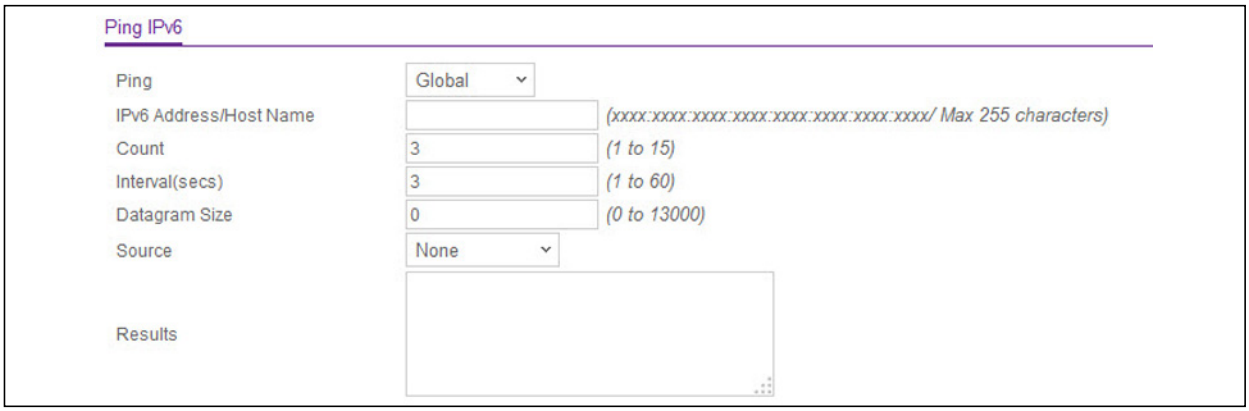
6. Click **Apply** to send the ping to the specified address. The switch sends the number of pings specified in the **Count** field, and the results are displayed below the configurable data in the **Results** area.
7. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.

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 a specified number of ping requests and the results will be displayed below the configurable data. The output will be:

```
Send count=n, Receive count=n from (IPv6 Address). Average round trip
time = n ms.
```

To access the Ping IPv6 page, click **Maintenance** > **Troubleshooting** > **Ping IPv6**.



1. Select the **Ping** type from the list. Possible values are:
   - Global—Ping a global IPv6 address.
   - Link Local—Ping a link-local IPv6 address over the specified interface. This field is shown when Interface is selected as the ping option.
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 format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. The maximum number of characters is 255.
3. Use **Count** to enter the number of echo requests you want to send. The range is 1 to 15. The default value is 3.
4. Enter the **Interval** in seconds between ping packets. The range is 1 to 60. The default value is 3.
5. Use **Datagram Size** to enter the datagram size. The valid range is 0 to 13000. The default value is 0 bytes.
6. Enter the **Source** IP address or interface to use when sending the echo request packets. If source is not required, select None as the source option. Possible values are:

- None—The source address of the ping packet would be the address of the default outgoing interface.
- IPv6 Address—The source IPv6 address to use when sending the Echo request packets. This field is shown when **IPv6 Address** is selected as the source option.
- Interface—The interface to use when sending the Echo request packets. This field is shown when **Interface** is selected as the source option.

Note: Values configured in the fields above are not saved to the switch. As a result, refreshing the page sets these fields to the default values.

7. Click **Apply** to send the ping to the specified IPv6 address or hostname. The switch sends the number of pings specified in the **Count** field, and the results are displayed below the configurable data in the **Results** area.
8. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

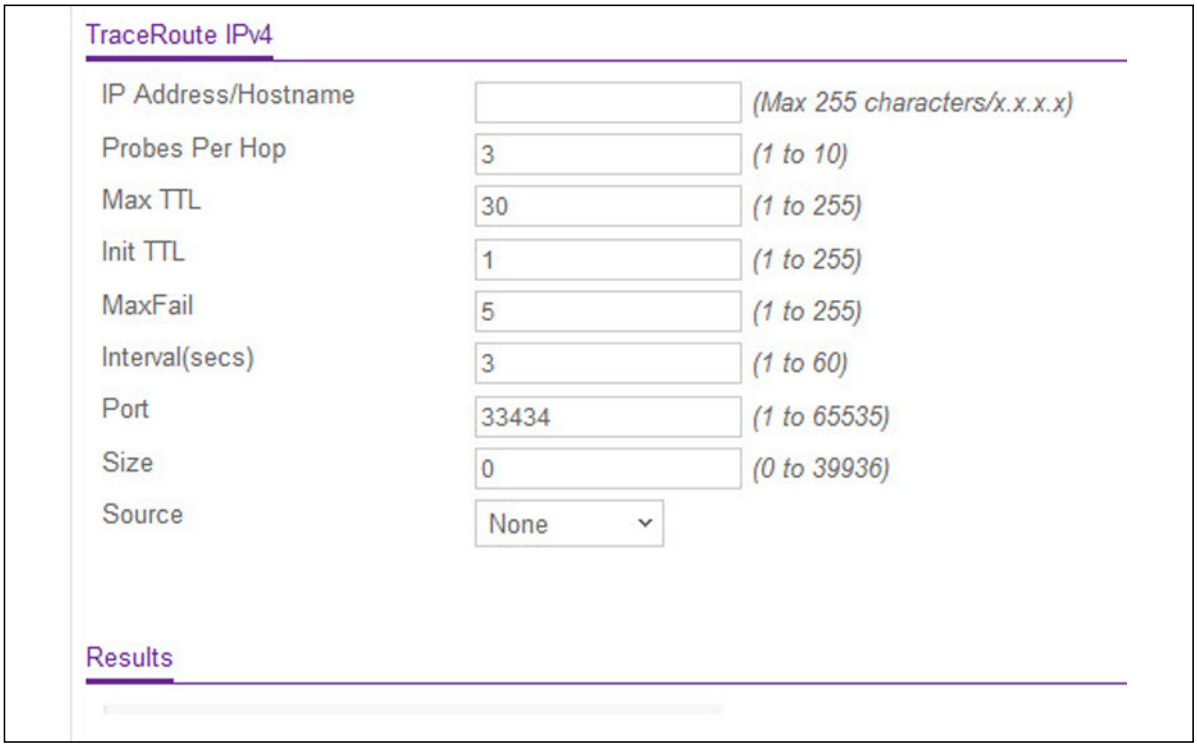
Traceroute IPv4

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 e.f.g.h 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 = j Last TTL = k Test attempt = m Test Success = n.
```

To display the Traceroute IPv4 page, click **Maintenance** > **Troubleshooting** > **Traceroute IPv4**.



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 a path. The default value is blank.
2. Enter the number of **Probes Per Hop.** The default value is 3. The range is 1 to 10.
3. Enter the **Maximum TTL** for the destination. The default value is 30. The range is 1 to 255.
4. Enter the **Initial TTL** to be used. The default value is 1. The range is 1 to 255.
5. Enter the **Maximum Failures** allowed in the session. The default value is 5. The range is 1 to 255.
6. **Interval (secs)** - Enter the Time between probes in seconds. The default value is 3. The range is 1 to 60.
7. Enter the UDP Destination **Port** in probe packets. The default value is 33434. The range is 1- 65535.
8. Enter the **Size** of the probe packets. The default value is 0. The range is 0 to 39936.
9. Enter the **Source** IP address or interface to use when sending the echo request packets. If source is not required, select None as the source option. Possible values are:
   - None—The source address of the ping packet would be the address of the default outgoing interface.
   - IP Address—The source IP address to use when sending the Echo request packets. This field is shown when **IP Address** is selected as the source option.
   - Interface—The interface to use when sending the Echo request packets. This field is shown when **Interface** is selected as the source option.

Note: Values configured in the fields above are not saved to the switch. As a result, refreshing the page sets these fields to the default values.

10. **Results** - Displays the traceroute IPv4 result after the switch sends a traceroute request to the specified IP address or hostname.
11. Click **Apply** to sends a traceroute request to the specified IP address or hostname. The results are displayed below the configurable data in the TraceRoute Results area.
12. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.

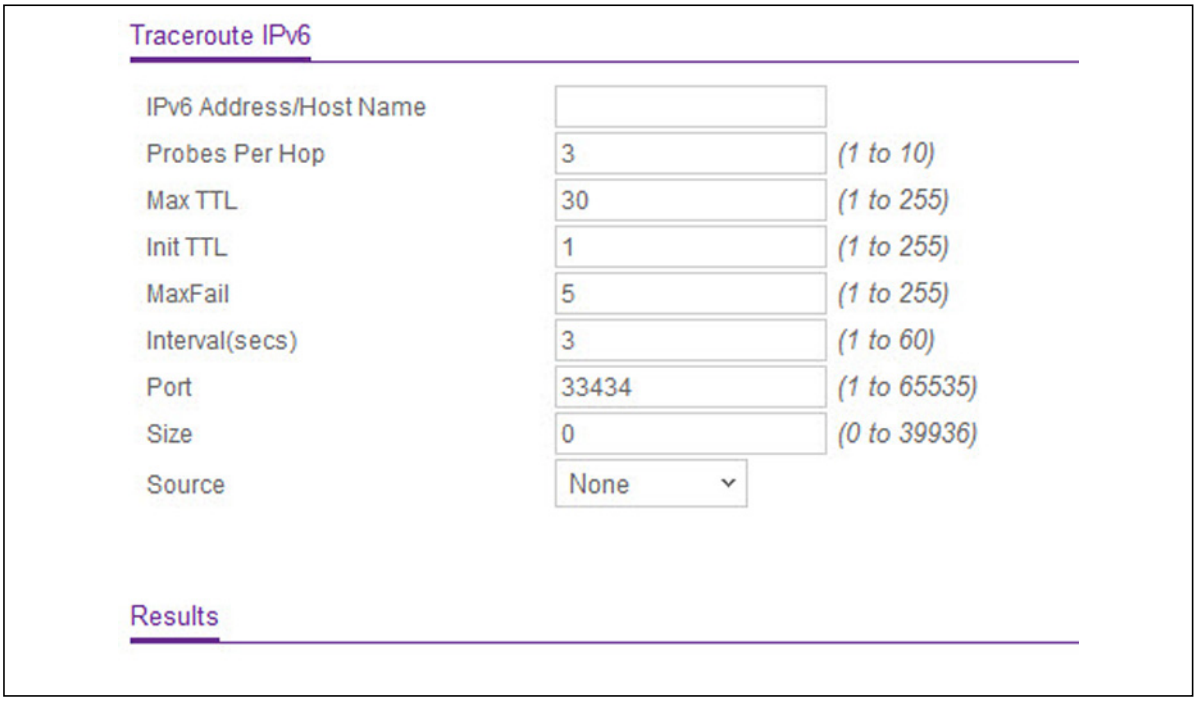
Traceroute IPv6

Use this screen to tell the switch to send a TraceRoute request to a specified IPv6 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 a 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 = p Last TTL = q Test attempt = r Test Success = s.
```

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. Enter the **Probes Per Hop**. The default value is 3. The range is 1 to 10.
3. Enter the **Maximum TTL** for the destination. The default value is 30. The range is 1 to 255. The MaxTTL you enter is not retained across a power cycle.
4. Enter the **Initial TTL** to be used. The default value is 1. The range is 1 to 255. The InitTTL you enter is not retained across a power cycle.
5. Enter the **Maximum Failures** allowed in the session. The default value is 5. The range is 1 to 255. The MaxFail you enter is not retained across a power cycle.
6. **Interval (secs)** - Enter the Time between probes in seconds. The default value is 3. The range is 1 to 60. The Interval you enter is not retained across a power cycle.
7. Enter the UDP Destination **Port** in probe packets. The default value is 33434. The range is 1- 65535. The port you enter is not retained across a power cycle.
8. Enter the **Size** of the probe packets. The default value is 0. The range is 0 to 39936. The Size you enter is not retained across a power cycle.
9. Enter the **Source** IP address or interface to use when sending the echo request packets. If source is not required, select None as the source option. Possible values are:
   - None—The source address of the ping packet would be the address of the default outgoing interface.
   - IP Address—The source IP address to use when sending the Echo request packets. This field is shown when **IP Address** is selected as the source option.
   - Interface—The interface to use when sending the Echo request packets. This field is shown when **Interface** is selected as the source option.

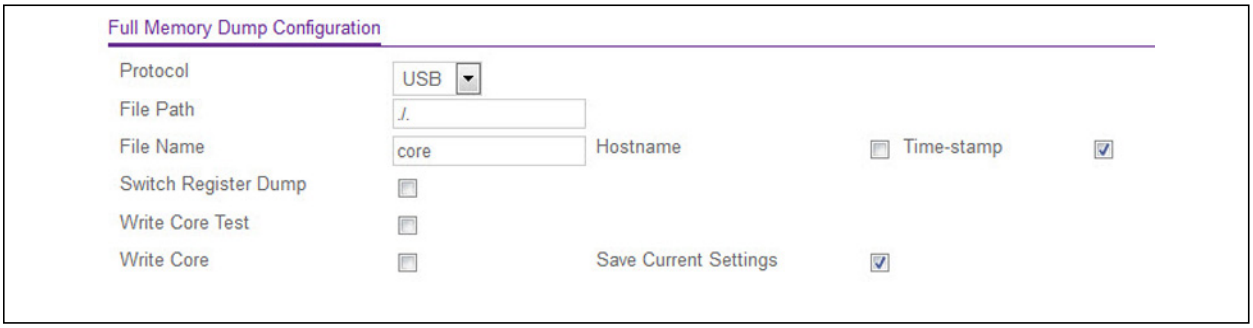
Note: Values configured in the fields above are not saved to the switch. As a result, refreshing the page sets these fields to the default values.

10. **Results** - Displays the traceroute IPv6 result after the switch sends a traceroute request to the specified IP address or hostname.
11. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
12. Click **Apply** to initiate the traceroute. The results display in the TraceRoute area.

Full Memory Dump

Use this screen to configure full memory dump in order to retrieve the core dump for troubleshooting.

To display the Full Memory Dump Configuration page, click **Maintenance** > **Troubleshooting** > **Full Memory Dump**.



1. From the **Protocol** menu, select the protocol used to store the core dump file. Possible values are:
   - **None**—Disable core dump.
   - **TFTP**—Set TFTP protocol.
   - **NFS**—Set NFS protocol.
   - **USB**—Set USB protocol.
2. In the **File Path** field, enter the path to store the core dump file.
3. In the **File Name** field, enter the core dump filename.
4. Select the **Hostname** option to append the hostname to the core dump filename.
5. Select the **Time-stamp** option to append a time-stamp to the core dump filename.
6. Select the **Switch Register Dump** option to dump the switch chip register in case of an exception.
7. Select the **Write Core Test** option to test the core dump setup.
8. Select the **Write Core** option to create a core dump and store it to the previously configured external server. Executing this procedure causes a reload of the device.
9. Select the **Save Current Settings** option to save the current settings of the system.

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.

9 Help

Use the features available from the Help tab to connect to online resources for assistance. The Help tab contains a link to *Online Help* .

Registration

The first time you log onto the switch, you will be given the option of registering with NETGEAR. Registration confirms your e-mail alerts will work, lowers technical support resolution time and ensures your shipping address accuracy. We'd also like to incorporate your feedback into future product development.

NETGEAR will never sell or rent your e-mail address and you may opt out of communications at any time.

1. To register with NETGEAR, click REGISTER NOW.

Online Help

The Online Help includes the following pages:

- *Support* on page 540
- *User Guide* on page 541

Support

Use the Support page to connect to the Online Support site at netgear.com.

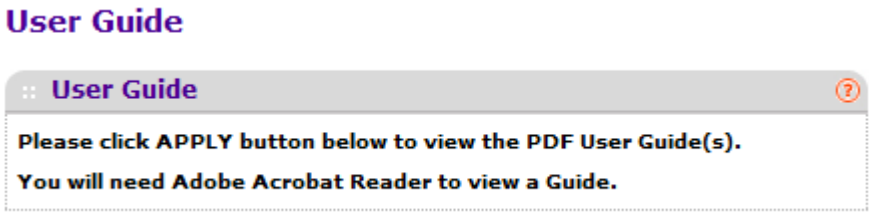
To access the Support page, click **Help** > **Online Help > Support**.

To connect to the NETGEAR support site for M6100 Chassis switch, click **Apply**.

User Guide

Use the User Guide page to access the *Documentation Templates* (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**.

Default Settings

A

This appendix describes the default settings for many of the NETGEAR M6100 Managed Chassis software features.

Table 162. Default Settings

Feature	Default
IP address	169.254.100.100
Subnet mask	255.255.0.0
Default gateway	0.0.0.0
Protocol	DHCP
Management VLAN ID	1
Minimum password length	Eight characters
IPv6 management mode	None
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 162. Default Settings (continued)

Feature	Default
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)	Disabled
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	Enabled
MAC Table Address Aging	300 seconds (Dynamic Addresses)
DHCP Layer 2 Relay	Disabled

Table 162. Default Settings (continued)

Feature	Default
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 RSTP
Optional STP Features	Disabled
STP Bridge Priority	32768
Multiple Spanning Tree	Disabled
Link Aggregation	No Link Aggregation Groups (LAGs) configured
LACP System Priority	1
Routing Mode	Disabled
IP Helper and UDP Relay	Disabled
Tunnel and Loopback Interfaces	None
DiffServ	Enabled
Auto VoIP	Disabled
Auto VoIP Traffic Class	6
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)

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 3-115.
- 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 3-115), 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.

M6100 Chassis switch 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.

M6100 Managed Chassis 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 M6100 Managed Chassis 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:

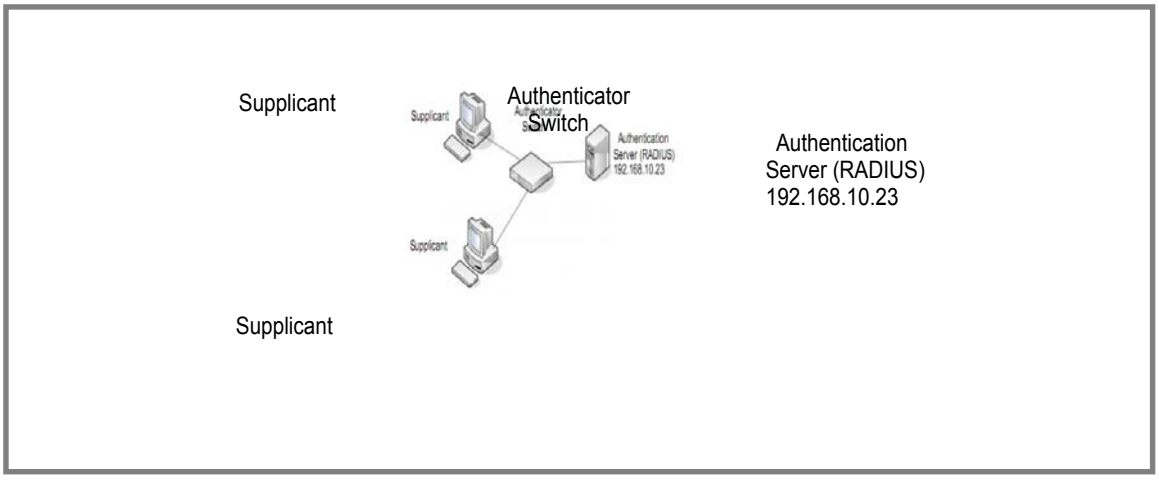
1. **Authenticator**: A Port that enforces authentication before allowing access to services available via that Port.
2. **Supplicant**: A Port that attempts to access services offered by the Authenticator.

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.

M6100 Managed Chassis 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 287).

   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 M6100 Chassis switch 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.

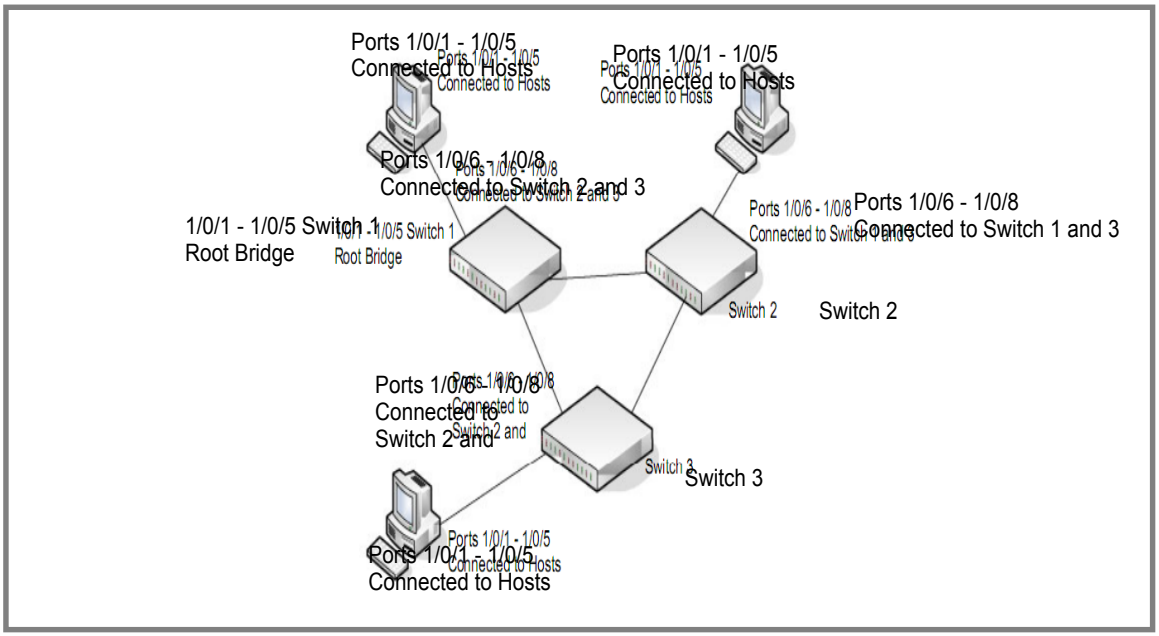
With this allocation we ensure that every VLAN is assigned to one and only one MSTI. The CIST is also an instance of spanning tree with a MSTID of 0.

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 M6100 switch. The example network has three different M6100 Chassis switch 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

C

NETGEAR wireless routers, gateways, APs

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Products bearing the CE marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

If it is a VueZone product intended for outdoor use, remove the indoor use only statement. (Always remove this writer note.)

For indoor use only. Valid in all EU member states, EFTA states, and Switzerland.

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 M6100 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 and Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
  Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
  Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

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.

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.

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.

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.

Interference Reduction Table

The table below shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

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