User Manual
Version 11.0.0

Contents

1. Getting Started

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

- *Available Publications and Online Help*
- *Understanding the User Interfaces*
- *Web Management Interface Overview*
- *Use a Web Browser to Access the Switch and Log In*
- *Using SNMP*

Note: For more information about the topics covered in this manual, visit the support website at *.com*.

1.1.1.1.1.**Note:** Firmware updates with new features and bug fixes are made available from time to time at *.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

Available Publications and Online Help

A number of publications are available for your managed switch at *downloadcenter..com*, including the following publications:

- *Chassis Hardware Installation Guide.*
- *Switch Module Installation Guide.*
- *Software Setup Manual.*
- *User Manual* (this document). You can also access this document online when you are logged in to the switch. Select **Help** > **Online Help > User Guide**.
- *Command Line Interface Manual.*

  Refer to the *Command Line Interface Manual* for information about the command structure. This provides information about the CLI commands used to configure the switch. It provides CLI descriptions, syntax, and default values.
- *Software Administration Manual.*

When you log into the web management interface, online help is available. See *Online Help* on page 19.

Understanding the User Interfaces

The managed 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 managed switch software. The method you use to manage the system depends on your network size and requirements, and on your preference.

The Series Managed Switch User Manual (this book) describes how to use the web-based interface to manage and monitor the system.

1.1. Web Management Interface Overview

Your managed switch contains an embedded web server and management software for managing and monitoring switch functions. The managed 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.

Software Requirements to Use 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

1.2. Use a Web Browser to Access the Switch and Log In

You can use a web browser to access the switch and log in. You must be able to ping the IP address of the managed switch management interface from your administrative system for web access to be available.

To use browser-based access to log in to the switch:

1. Prepare your computer with a static IP address in the 192.168.10.0 subnet, for example, 192.168.10.101.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

   The default IP address of the switch is 192.168.10.12.

   The Login screen displays.
5. Enter the user name and password.

   The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.

The web management interface menu displays.

Web Interface Buttons and User-Defined Fields

The following table shows the command buttons that are used throughout the screens in the web interface:

Table1. Web interface command buttons

Button	Function
Add	Clicking the **Add** button 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 the **Cancel** button cancels the configuration on the screen and resets the data on the screen to the previous values of the switch.
Delete	Clicking the **Delete** button removes the selected item.
Update	Clicking the **Update** button refreshes the screen with the latest information from the device.
Logout	Clicking the **Logout** button ends the session.

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

User-Defined Field Invalid Characters	
\	<
/	>
*	|
?	

1.2.1. Interface Naming Conventions

The managed switch supports physical and logical interfaces. Interfaces are identified by their type and the interface number. The physical ports are gigabit interfaces and are numbered on the front panel. You configure the logical interfaces by using the software.

The following table describes the naming convention for all interfaces available on the switch.

Table2. Naming conventions for interfaces

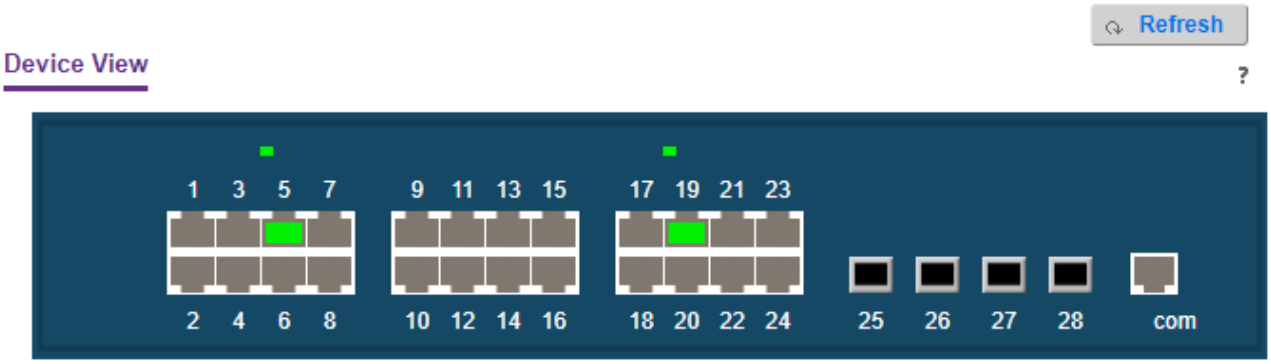
Interface	Description	Example
Physical	The physical ports are Gigabit Ethernet interfaces and are numbered sequentially starting from one.	0/1, 0/2, 0/3, and so on
Link aggregation group (LAG)	LAG interfaces are logical interfaces that are used only for bridging functions.	LAG 1, LAG 2, lAG 3, and so 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

1.2.2. Web Management Interface 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, tables, and feature components.

System > Device View.

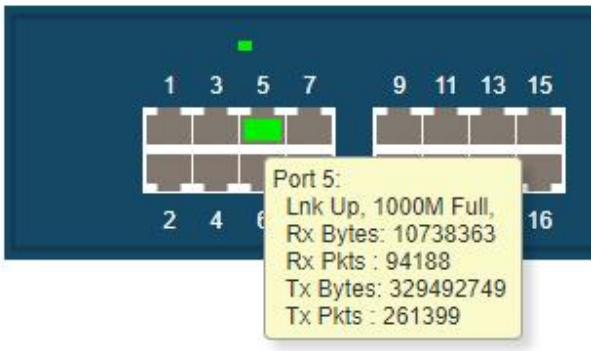
The port coloring indicates whether a port is currently active. Green indicates that the port is enabled; grey indicates that an error occurred on the port, or that the link is disabled.



Click a port to see a menu that displays statistics and configuration options.

You can click a menu option to access the screen that contains the configuration or monitoring options.

If you click the graphic, but do not click a specific port, the main menu displays. This menu contains the same options as the navigation tabs at the top of the screen.



1.3. Using SNMP

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

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

SNMP is enabled by default. The System Information screen, which is the screen that displays when you log in, displays the information that you need to configure an SNMP manager to access the switch.

Any user can connect to the switch using the SNMP v3 protocol, but for authentication and encryption, the switch supports only one user, which is **admin**; therefore, only one profile can be created or modified.

To configure authentication and encryption settings for the SNMP v3 admin profile:

Select **System** > **SNMP** > **SNMP v3** > **User Configuration**.

The User Configuration screen displays.

1. To enable authentication, select an **Authentication Protocol** option, which is either **MD5** or **SHA**.
2. To enable encryption, select the **DES** option in the **Encryption Protocol** list Then enter an encryption code of eight or more alphanumeric characters in the **Encryption Key** field.
3. Click the **APPLY** button.

   Your settings are saved.

To access configuration information for SNMP V1 or SNMP V2, select **System** > **SNMP** > **SNMPv1/v2** and select the screen that contains the information to configure

2. Configure System Information

This chapter covers the following topics:

- *Initial Setup*
- *Configure DHCP Server Settings*
- *Configure Basic PoE*
- *Configure SNMP*
- *LLDP Overview*
- *Configure ISDP*
- *Timer Schedule*

2.1. Initial Setup

When you log in to a switch that has its factory settings, the Initial Setup screen displays.

To do the initial system configuration:

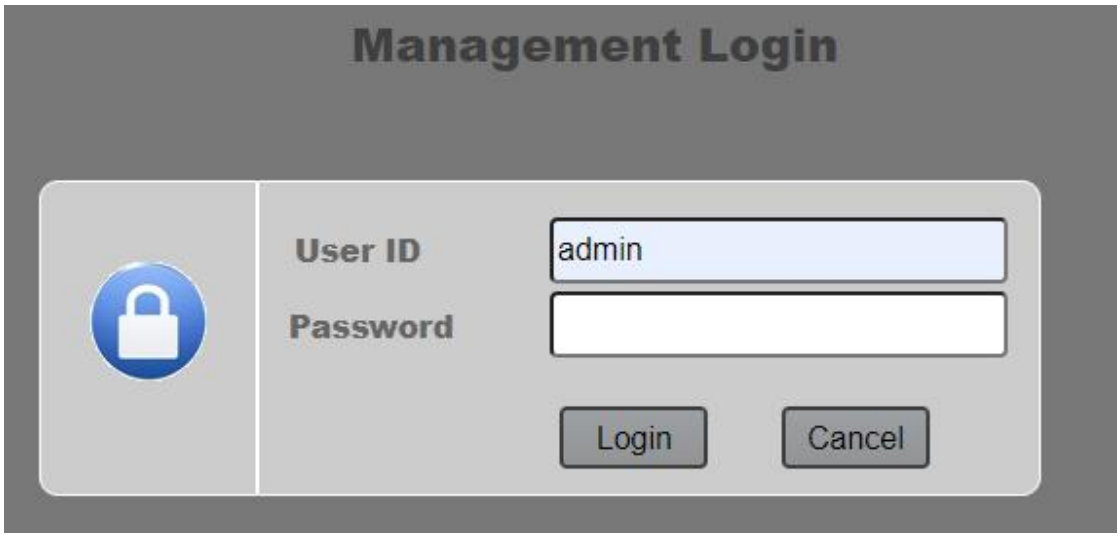
1. Prepare your computer with a static IP address in the 192.168.10.0 subnet, for example, 192.168.10.101.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

   The default IP address of the switch is 192.168.10.12.

   The Login screen displays.
5. Enter the user name and password.

   The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.

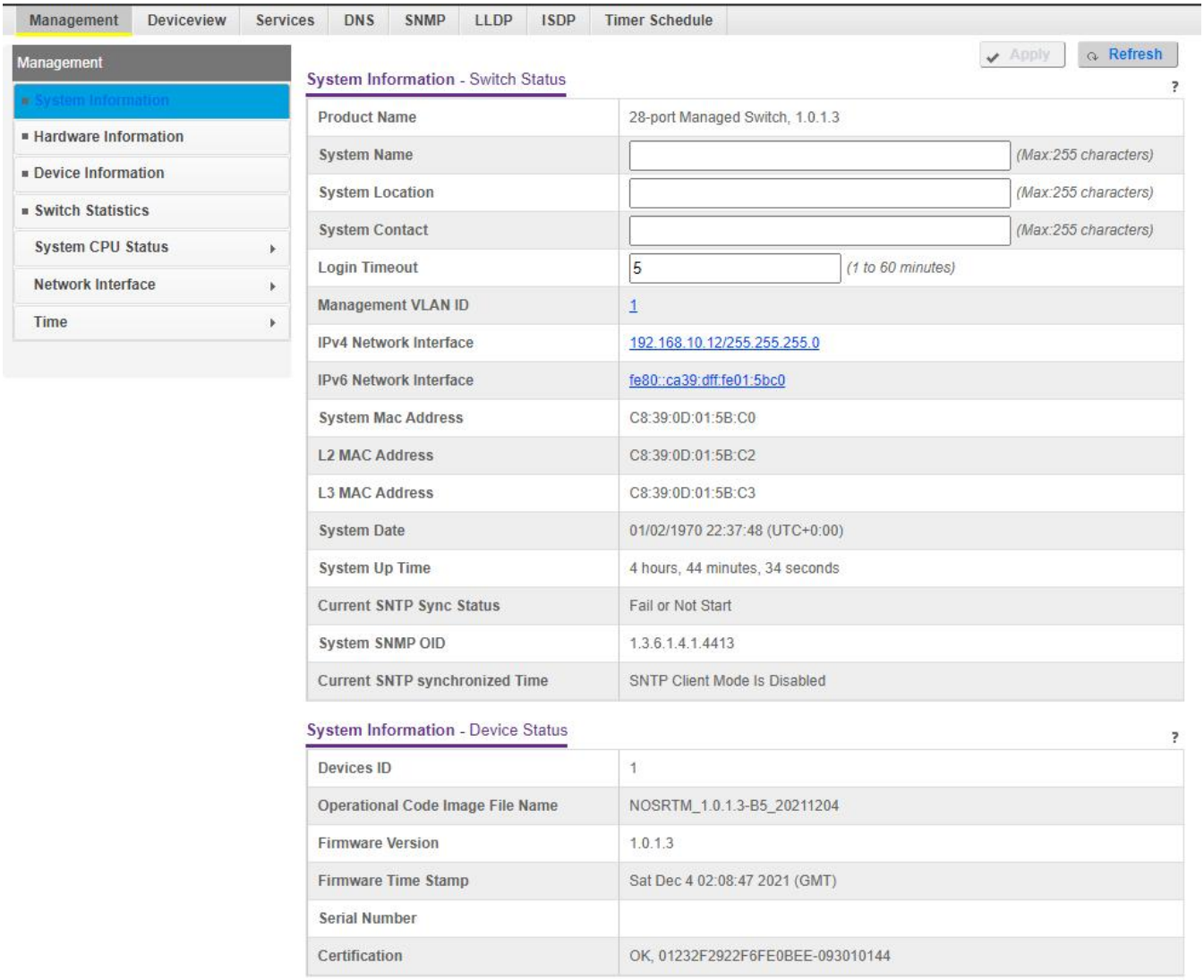
   The web management interface menu displays.



2.1.1. View or Define System Information

When you log in, the System Information screen displays. You can configure and view general device information.

System > **Management** > System information.



1. In the **System Name** field, type the name to identify this switch.

   You can use a name up to 255 characters in length. The factory default is blank.

2. In the **System Location** field, type the location of the switch.

   You can use a location up to 255 characters in length. The factory default is blank.

3. Enter the **System Contact**, the name of the contact person for this switch.

   You can use a contact name up to 255 characters in length. The factory default is blank.

4. Click the **Apply** button.

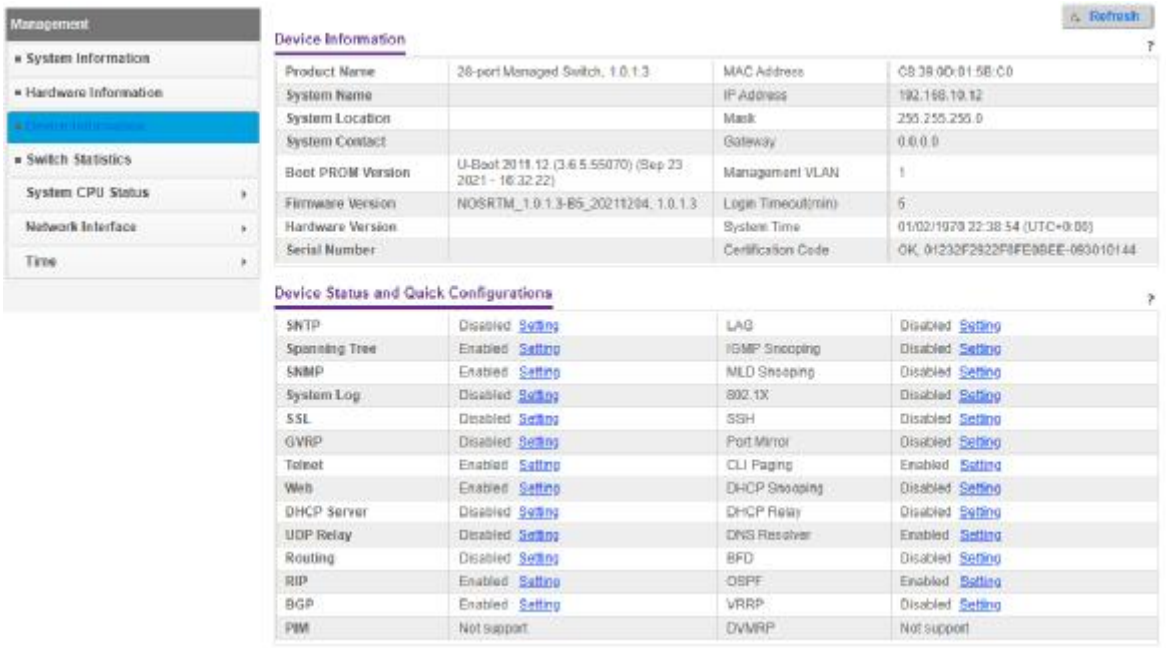
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

Table3. System Information

Field	Description
Product Name	The product name of this switch.
IPv4 Management VLAN Interface	The IPv4 address and mask assigned to the management VLAN interface.
IPv6 Management VLAN Interface	The IPv6 prefix and prefix length assigned to the management VLAN interface.
Management VLAN ID	The management VLAN ID of the switch. Click the displayed Management VLAN ID value to jump to the configuration screen.
IPv4 Service Port Network Interface	The IPv4 address and mask assigned to the service port interface.
IPv6 Service Port Network Interface	The IPv6 prefix and prefix length assigned to the service port 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	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.
Service Port MAC Address	The MAC address used for out-of-band connectivity.
L2 MAC Address	The MAC address used for communications on the Layer 2 network segment.
L2 MAC Address	The MAC address used for communications on the Layer 3 network segment.
Supported Java Plugin Version	The supported version of Java plug-in.
Current SNTP Synchronized Time	The SNTP synchronized time.

2.1.2. View the Device Status

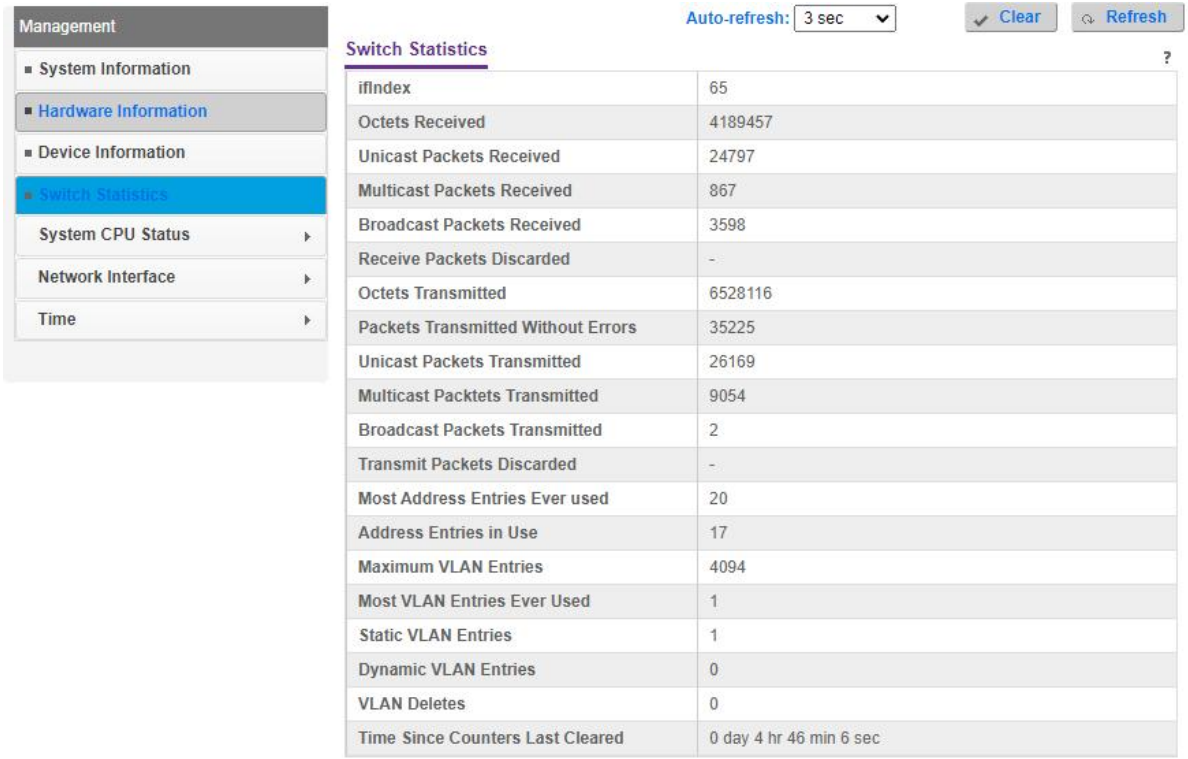
System > **Management** >Device Information



To refresh the screen

2.1.3. View Switch Statistics

System > **Management** >Switch Statistics.



To clear all the counters, resetting all switch summary and detailed statistics to default values, click the **Clear** button. The discarded packets count cannot be cleared.

The following table describes Switch Statistics information.

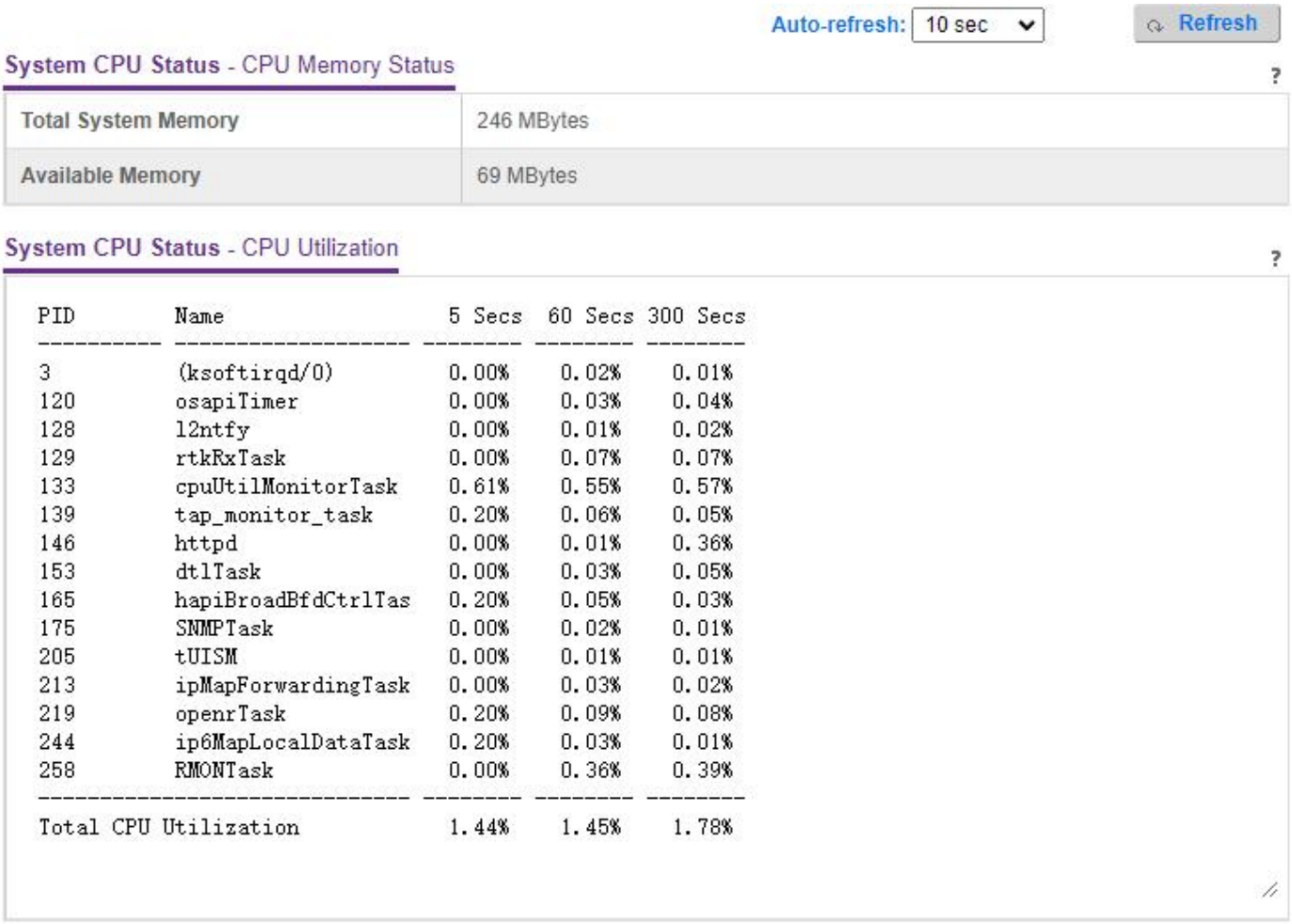
Table4. Switch Statistics information

Field	Description
ifIndex	The ifIndex of the interface table entry associated with the processor of this switch.
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Errors	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. This does not include multicast packets.
Receive Packets Discarded	The number of inbound packets that were discarded even though no errors were 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 are 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 are 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 are transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets that were discarded even though no errors were 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 learned by this switch since the most recent reboot.
Address Entries in Use	The number of learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that were active on this switch since the last reboot.

Static VLAN Entries	The number of presently active VLAN entries on this switch that were created statically.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that were created by GVRP registration.
VLAN Deletes	The number of VLANs on this switch that were created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

2.1.4. View the System CPU Status

System > **Management** > **System CPU Status**.



You can view the CPU Utilization information, which contains the memory information, task-related information, and percentage of CPU utilization per task.

The following table describes CPU Memory Status information.

Table5. 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.

2.1.5. Configure the CPU Thresholds

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

System > **Management** > **System CPU Status** > **CPU Threshold**

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.

To refresh the screen, click the **Refresh** button.

System > Management > Management Interfaces > IPv4 Management VLAN Configuration.

1. Specify the **Management VLAN ID** of the switch.

   The management VLAN is used for management of the switch. It can be configured to any value in the range of 1–4093.

Table6. IPv4 Management VLAN Configuration

Field	Description
MAC Address	The MAC address assigned to the VLAN routing interface.
Routing Interface Status	Indicates whether the link status is up or down.
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.

2. Select a Service Port Configuration Protocol radio button:
   - **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. Specify the **IP Address** of the interface.

   The factory default value is 192.168.10.12.
4. Specify the IP **Subnet Mask** for the interface.

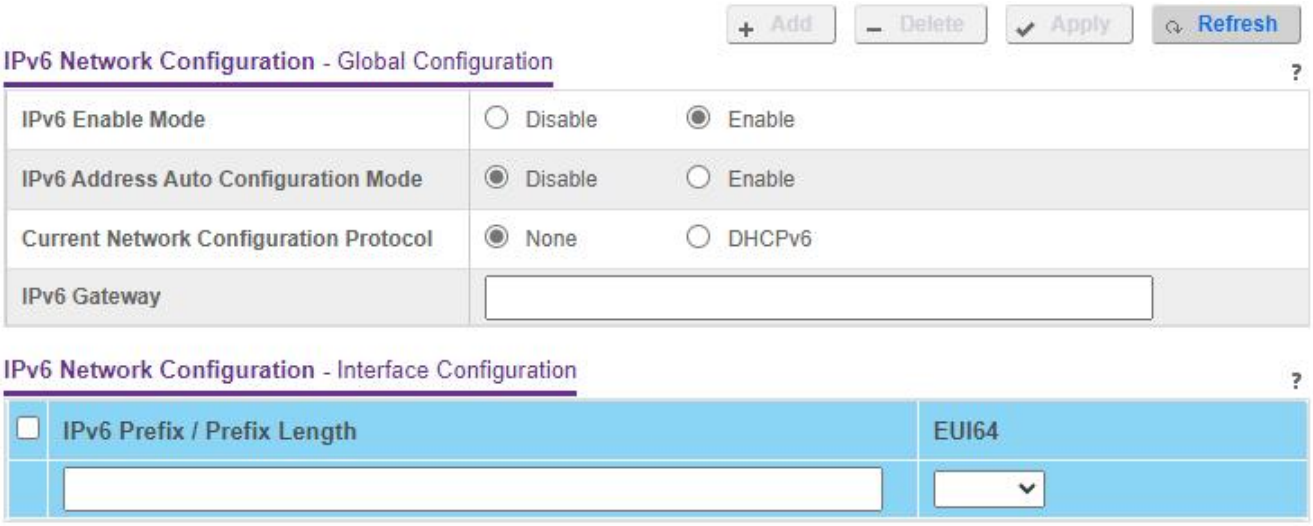
   The factory default value is 255.255.0.0.
5. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.1.6. Configure the IPv6 Service Port

You can 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:
System > Management > Management Interfaces > IPv6 Service Port Configuration.



1. Select the IPv6 mode **Enable** or **Disable** radio button.

   This specifies the IPv6 administrative mode on the service port.

2. Select the Service Port Configuration Protocol **None** or **DHCP** radio button.

   This specifies whether the device acquires network information from a DHCPv6 server. Selecting **None** disables the DHCPv6 client on the service port.

3. Select the IPv6 Stateless Address AutoConfig mode **Enable** or **Disable** radio button:
   - **Enable**. The service port can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of router advertisement messages.
   - **Disable**. The service port does not use the native IPv6 address autoconfiguration feature to acquire an IPv6 address.

   This sets the IPv6 stateless address autoconfiguration mode on the service port.

4. The **DHCPv6 Client DUID** field displays the client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.
5. To configure the IPv6 gateway, select the **Change IPv6 Gateway** check box.

   The IPv6 gateway is the default gateway for the IPv6 service port interface.

6. Use the **IPv6 Gateway** field to specify the default gateway for the IPv6 service port interface.

   The **Add/Delete IPv6 Address** table lists the manually configured static IPv6 addresses on the service port interface.

7. Specify the following:
   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.
8. Click the **Add** button.

The IPv6 address is added to the service port interface,

9. To delete the selected IPv6 address, click the **Delete** button.
10. Click the **Apply** button.

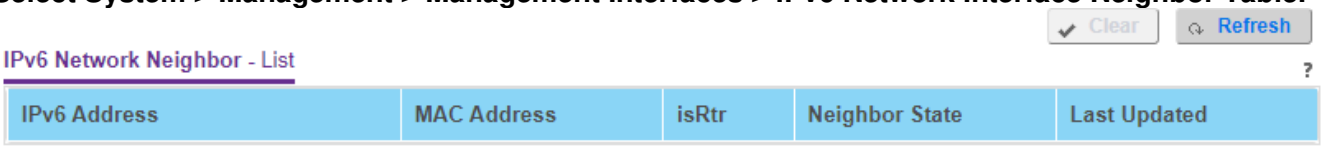
    The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen, click the **Update** button.

2.1.7. View the IPv6 Network Interface Neighbor Table

To view the IPv6 Network Neighbor Table:

Select System > Management > Management Interfaces > IPv6 Network Interface Neighbor Table.



The following table displays IPv6 Network Interface Neighbor Table information.

Table7. IPv6 Network Interface Neighbor Table information

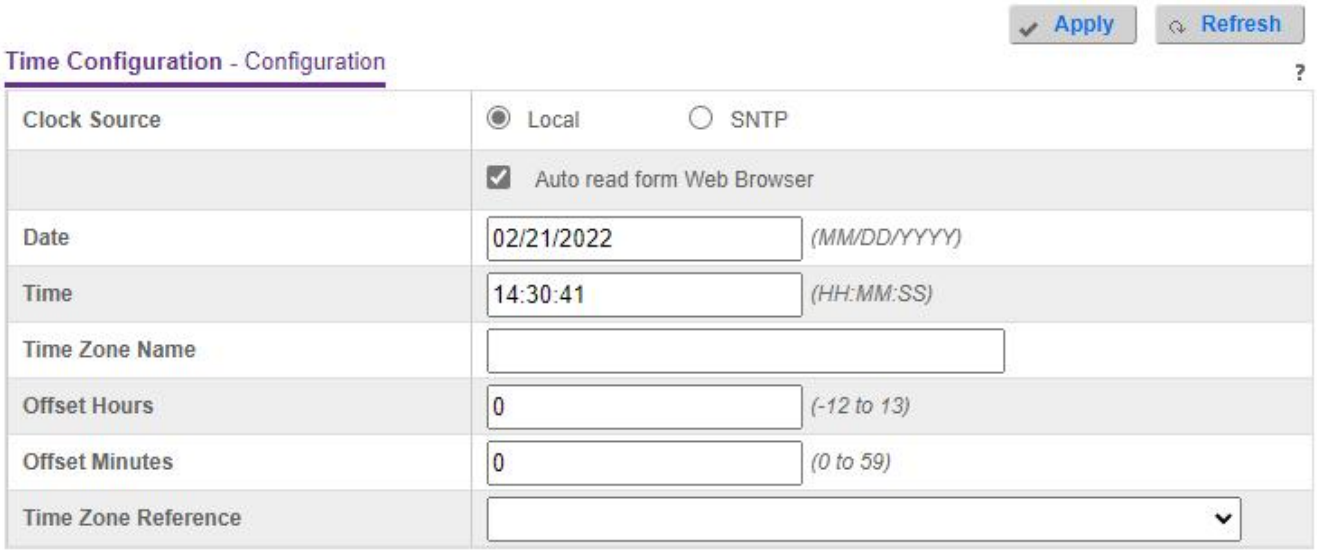
Field	Description
IPv6 address	The IPv6 address of a neighbor switch visible to the network interface.
MAC address	The MAC address of a neighbor switch.
IsRtr	**true (1)** if the neighbor machine is a router, **false (2)** otherwise.
Neighbor State	The state of the neighboring switch: • **reachable (1)**. The neighbor is reachable by this switch. • **stale (2)**. Information about the neighbor is scheduled for deletion. • **delay (3)**. No information was received from neighbor during delay period. • **probe (4)**. The switch is attempting to probe for this neighbor. • **unknown (6)**. Unknown status.
Last Updated	The last sysUpTime that this neighbor was updated.

2.2. Time

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 through the Internet.

2.2.1. Configure the Time Setting

To configure the time setting:
System > Management > Time > Time Configuration.



1. Select the Clock Source **Local** or **SNTP** radio button.

   The default is SNTP. The local clock can be set to SNTP only if the following two conditions are met:

   - The SNTP server is configured.
   - The SNTP last attempt status is successful.

2. In the **Date** field, 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 the **Apply** button.

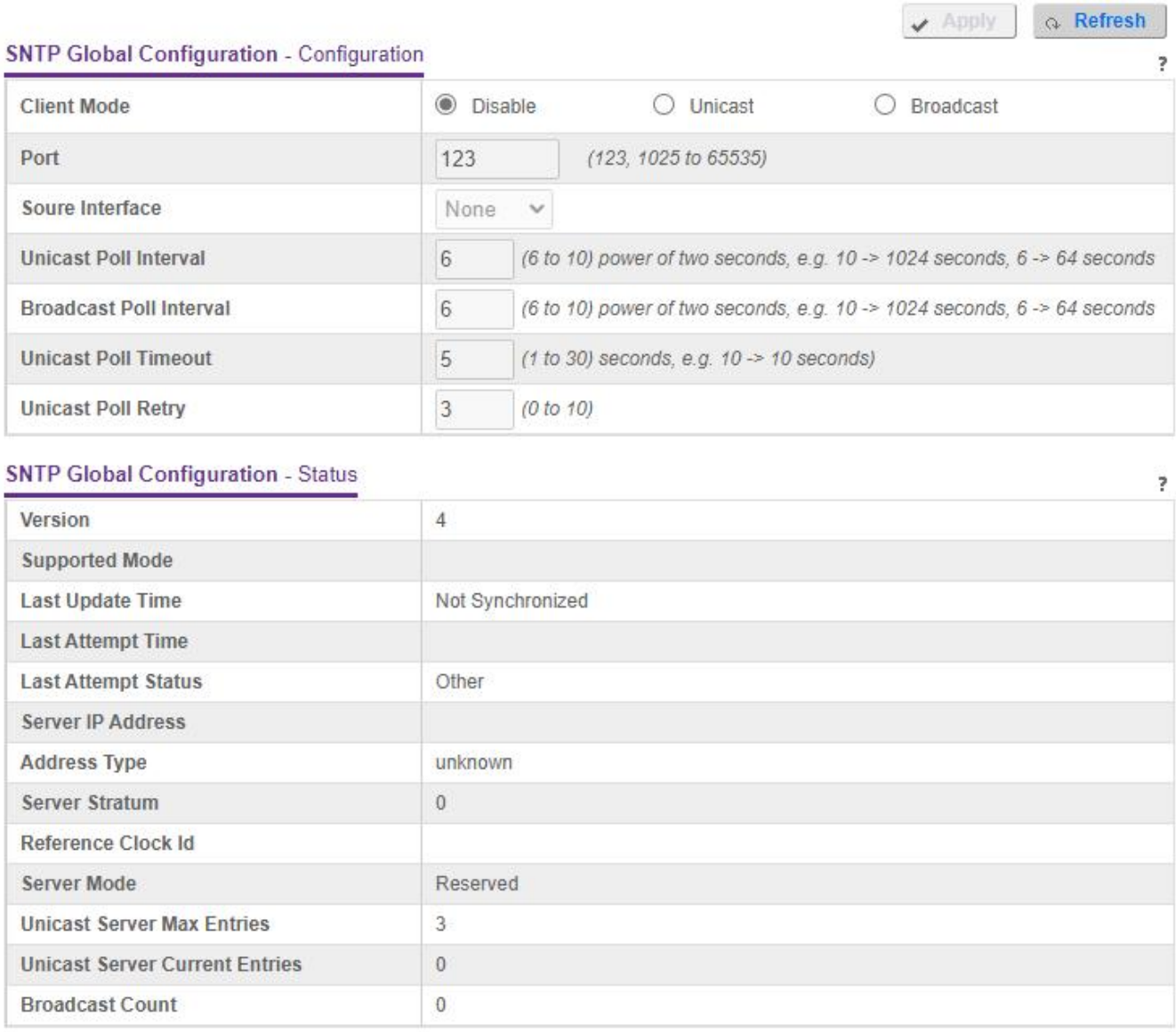
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen, click the **Update** button.

2.2.2. Configure the SNTP Global Settings

To configure the SNTP global settings:
System > Management > Time > Time Configuration > SNTP Global Configuration.

When you select the **SNTP** option as the **Clock Source**, the SNTP Global Configuration section is displayed below the Time Configuration section of the screen.



1. Select a **Client mode** radio button to specify the mode of operation of the SNTP client:
   - **Disable**. SNTP is not operational. No SNTP requests are sent from the client and no received SNTP messages are processed.
   - **Unicast**. SNTP operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.
   - **Broadcast**. SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has Internet wide scope.

The default value is Unicast.

2. In the **Port** field, specify the local UDP port that the SNTP client receives server packets on.

   The allowed range is 1025 to 65535 and the value 123. The default value is 123. When the default value is configured, the actual client port value used in SNTP packets is assigned by the operating system.

3. Select the **Source Interface** to use for the SNTP client.

   Possible values are as follows:

   - None
   - VLAN 1
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Tunnel interface
   - Service port

   By default VLAN 1 is used as the source interface.

4. Specify the **Unicast Poll Interval**.

   This is the number of seconds between unicast poll requests expressed as a power of two when configured in unicast mode. The allowed range is 6 to 10. The default value is 6.

5. Specify the **Broadcast Poll Interval**.

   This is the number of seconds between broadcast poll requests expressed as a power of 2 when configured in broadcast mode. Broadcasts received prior to the expiry of this interval are discarded. The allowed range is 6 to 10. The default value is 6.

6. Specify the **Unicast Poll Timeout**.

   This is the number of seconds to wait for an SNTP response when configured in unicast mode. The allowed range is 1 to 30. The default value is 5.

7. Specify the **Unicast Poll Retry**.

   This is the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode. The allowed range is 0 to 10. The default value is 1.

8. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen, click the **Update** button.

2.2.3. View SNTP Global Status

When you select the **SNTP** option as the **Clock Source**, the SNTP global status is displayed below the SNTP Global Configuration section of the screen.

To view SNTP global status:
System > Management > Time > Time Configuration > SNTP Global Status

When you select the **SNTP** option as the **Clock Source**, the SNTP Global Status is displayed below the SNTP Global Configuration section.

The following table displays the nonconfigurable SNTP Global Status information.

Table8. SNTP Global Status

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

Unicast Server Current Entries	The number of current valid unicast server entries configured for this client.
Broadcast Count	The number of unsolicited broadcast SNTP messages that were received and processed by the SNTP client since the last reboot.

2.2.4. Configure an SNTP Server

SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. 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, through 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 that the original request was sent by the client.
- **T2**. Time that the original request was received by the server.
- **T3**. Time that the server sent a reply.
- **T4**. Time that the client received the server's reply.

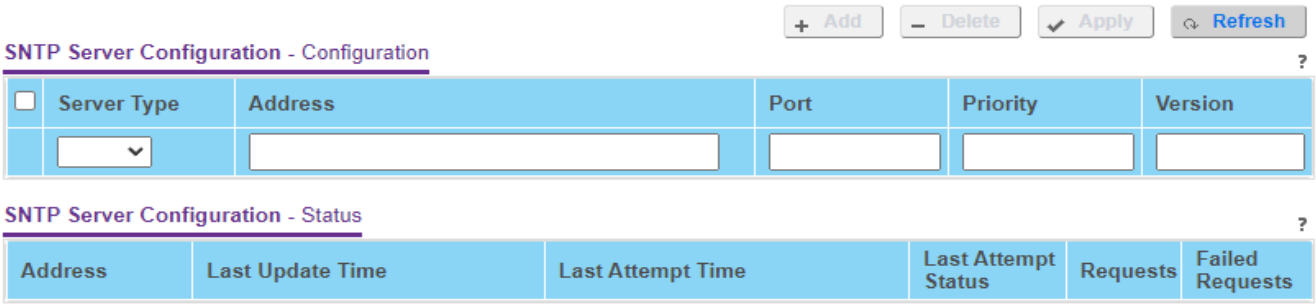
The device can poll unicast server types for the server time.

Polling for unicast information is used for polling a server for which the IP address is known. SNTP servers that were 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 screen.

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

You can view and modify information for adding and modifying Simple Network Time Protocol SNTP servers.

To configure the SNTP server settings:
System > Management > Time > SNTP Server Configuration.



1. In the **Server Type** list, select the address type of the configured SNTP server address.

   Possible values are as follows:

   - 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 host name of an SNTP server. Unicast SNTP requests are sent to this address. If this address is a DNS host name, then that host name is 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 are sent.

   The client continues sending requests to different servers until a successful response is received, or all servers are exhausted. The priority indicates the order in which to query the servers. A server entry with a precedence of 1 is 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 follows 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 the **Add** button.

   The SNTP server entry is added. 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.
9. To remove an SNTP server entry, select the check box next to the configured server to remove, and then click the **Delete** button.

   The entry is removed, and the device is updated.

10. Click the **Apply** button.

    The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen, click the **Update** button.

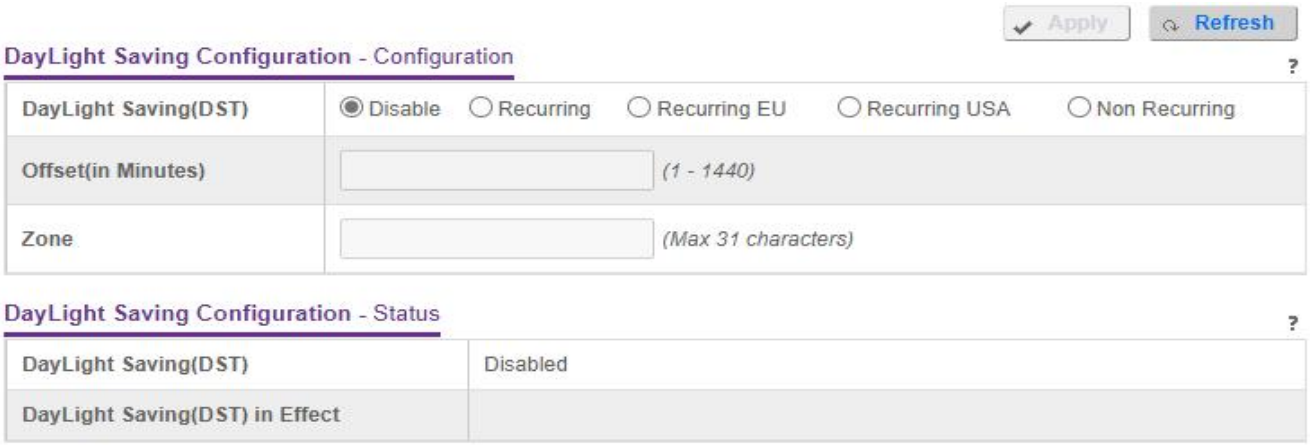
The SNTP Server Status table displays status information about the SNTP servers configured on your switch. The following table displays SNTP Server Status information.

Table9. SNTP Server Status

Field	Description
Address	All the existing server addresses. If no server configuration exists, a message saying No SNTP server exists flashes on the screen.
Last Update Time	The local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	The local date and time (UTC) that this SNTP server was last queried.
Last Attempt Status	The status of the last S9 NTP request to this server. If no packet was 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 through the leap indicator field on the SNTP message. • **Server Kiss Of Death**. The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Requests	The number of SNTP requests made to this server since last agent reboot.
Failed Requests	The number of failed SNTP requests made to this server since last reboot.

2.2.5. Configure Daylight Saving Time Settings

To configure the Daylight Saving Time settings:
System > Management > Time > Daylight Saving Configuration.



1. Select Daylight Saving (DST) radio button:
   - **Disable**. Disable daylight saving time.
   - **Recurring**. Enable Recurring daylight saving time.
   - **Recurring EU**. Enable recurring EU daylight saving time.
   - **Recurring USA**. Enable recurring USA daylight saving time.
   - **Non Recurring**. Configure non-recurring daylight saving time.
2. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.2.6. Recurring EU or Recurring USA.

The fields in the following tables are visible only when DayLight Saving is **Recurring** or

Table10. DayLight Saving - Recurring

Field	Description
Begins At	These fields are used to configure the start values of the date and time. • **Week**. Configure the start week. • **Day**. Configure the start day. • **Month**. Configure the start month. • **Hours**. Configure the start hours. • **Minutes**. Configure the start minutes.

Ends At	These fields are used to configure the end values of date and time. • **Week**. Configure the end week. • **Day**. Configure the end day. • **Month**. Configure the end month. • **Hours**. Configure the end hours. • **Minutes**. Configure the end minutes.
Offset	Configure recurring offset in minutes. The valid range is 1–1440 minutes.
Zone	Configure the time zone.

The fields in the following table are visible only when DayLight Saving is **Non Recurring**.

Table11. DayLight Saving - Non Recurring

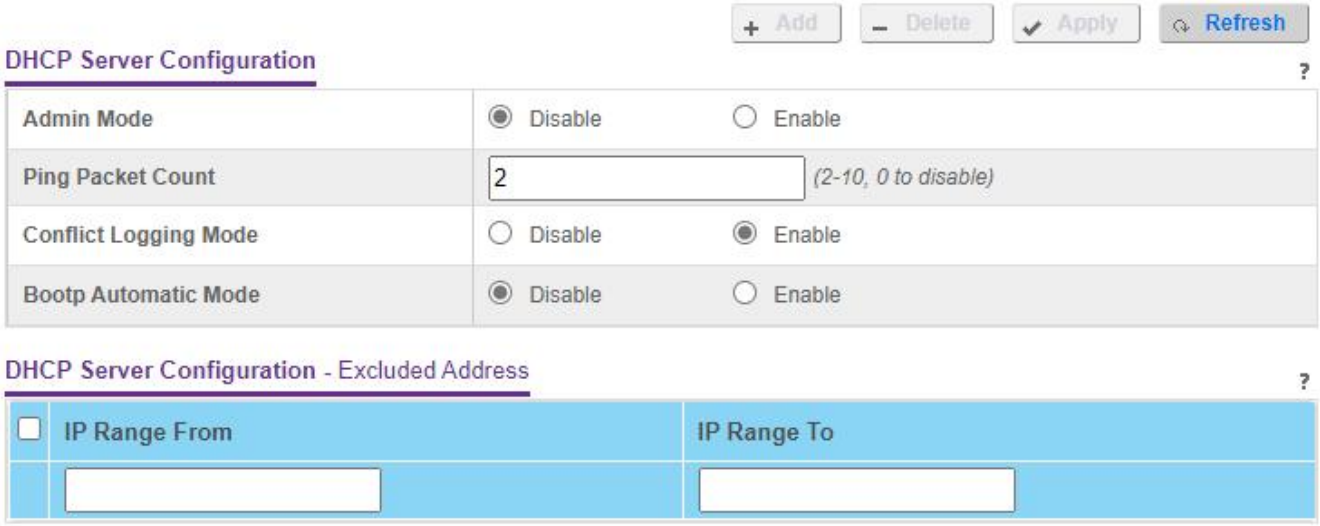
Field	Description
Begins At	These fields are used to configure the start values of the date and time. • **Week**. Configure the start week. • **Day**. Configure the start day. • **Month**. Configure the start month. • **Hours**. Configure the start hours. • **Minutes**. Configure the start minutes.
Ends At	These fields are used to configure the end values of date and time. • **Week**. Configure the end week. • **Day**. Configure the end day. • **Month**. Configure the end month. • **Hours**. Configure the end hours. • **Minutes**. Configure the end minutes.
Offset	Configure the non-recurring offset in minutes. The valid range is 1–1440 minutes.
Zone	Configure the time zone.

2.3. Configure DHCP Server Settings

You can configure settings for DHCP server, DHCP pools, DHCP bindings, and DHCP relay. You can also view DHCP statistics and conflicts.

2.3.1. Configure DHCP Server

To configure a DHCP server:
System > Services > DHCP Server > DHCP Server Configuration.



1. Select the Admin Mode **Disable** or **Enable** radio button.

   This specifies whether the DHCP service is enabled or disabled. The 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.

   The default value is 2. Valid range is 0, 2 to 10. Setting the value to 0 disables the function.

3. Select the Conflict Logging mode **Disable** or **Enable** radio button.

   This specifies whether conflict logging on a DHCP server is to be enabled or disabled. The default value is Enable.

4. Select the BootP Automatic mode **Disable** or **Enable** radio button.

   This specifies whether BootP for dynamic pools is to be enabled or disabled. The default value is Disable.

5. To exclude addresses, do the following:
   a. In the **IP Range From** field, enter the lowest address in the range or a single address to be excluded.
   b. In the **IP Range To** field, to exclude a range, enter the highest address in the range. To exclude a single address, enter the same IP address as specified in the **IP Range From** field, or leave it as 0.0.0.0.

6. Click the **Add** button.

   The exclude addresses are added to the switch

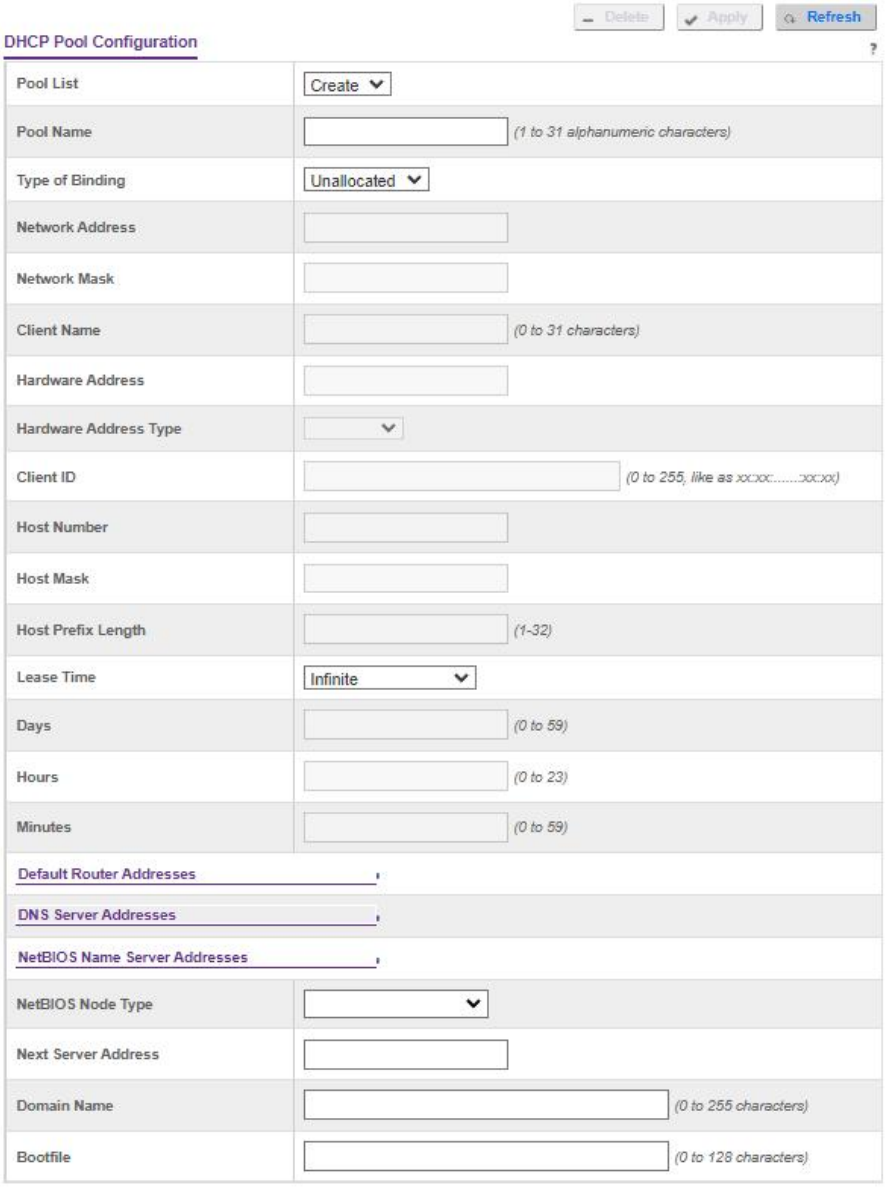
7. To delete the exclude address from the switch, click the **Delete** button.

8. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.3.2. Configure the DHCP Pool

To configure the DHCP pool:
System > Services > DHCP Server > DHCP Pool Configuration.



1. Click the **Add** button.

   The pool configuration is added.

2. To delete the pool, click the **Delete** button.

   This field is not visible to a user with read-only permission.

3. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the DHCP Pool Configuration fields.

Table12. DHCP Pool Configuration

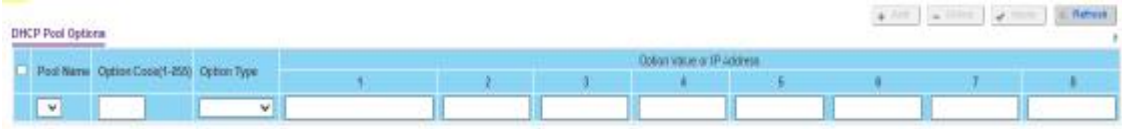
Field	Description
Pool Name*	For a user with read/write permission, this field shows names of all the existing pools along with an additional option **Create**. When the user selects **Create**, another text box **Pool Name**, appears where the user can enter a name for the pool to be created. For a user with read-only permission, this field shows names of the existing pools only.
Pool Name	The name of the pool to be created. This field appears when the user with read-write permission selects **Create** in the Pool Name list*. **Pool Name** can be up to 31 characters in length.
Type of Binding	The type of binding for the pool: • Unallocated • Dynamic • Manual
Network Address	The subnet address for a DHCP address of a dynamic pool.
Network Mask	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	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. The valid range is 0 to 32.
Client Name	The client name for DHCP manual pool.
Hardware Address	The MAC address of the hardware platform of the DHCP client.
Hardware Address Type	The protocol of the hardware platform of the DHCP client. Valid types are Ethernet and ieee802. The default value is Ethernet.
Client ID	The client identifier for DHCP manual pool.
Host Number	The IP address for a manual binding to a DHCP client. The host can be set only if f Client Identifier or Hardware Address is specified. Deleting Host would delete the client name, client ID, and hardware address for the manual pool, and set the pool type to Unallocated.

Table13. DHCP Pool Configuration (continued)

Field	Description
Host Mask	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	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. The 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. The default value is Specified Duration.
Days	The number of days of the lease period. This field appears only if the user specified **Specified Duration** as the Lease time. The default value is 1. The valid range is 0 to 59.
Hours	The number of hours of the lease period. This field appears only if the user specified **Specified Duration** as the Lease time. The valid range is 0 to 22.
Minutes	The number of minutes of the lease period. This field appears only if you specified **Specified Duration** as the lease time. The valid range is 0 to 86399.
Default Router Addresses	The list of **Default Router Addresses** for the pool. Click the arrow beside the field name to expand the screen and display a table where you can specify up to eight default router addresses in order of preference.
DNS Server Addresses	The list of **DNS Server Addresses** for the pool. Click the arrow beside the field name to expand the screen and display a table where you can specify up to eight DNS Server Addresses in order of preference.
NetBIOS Name Server Addresses	The list of **NetBIOS Name Server Addresses** for the pool. Click the arrow beside the field name to expand the screen and display a table where you can specify up to eight NetBIOS name server addresses in order of preference.
NetBIOS Node Type	The NetBIOS node type for DHCP clients: • b-node Broadcast • p-node Peer-to-Peer • m-node Mixed • h-node Hybrid
Next Server Address	The **Next Server Address** for the pool.
Domain Name	The domain name for a DHCP client. **Domain Name** can be up to 255 characters in length.
Bootfile	The name of the default boot image for a DHCP client. File Name can be up to 128 characters in length.

2.3.3. Configure DHCP Pool Options

To configure DHCP Pool options:
System > Services > DHCP Server> DHCP Pool Options.

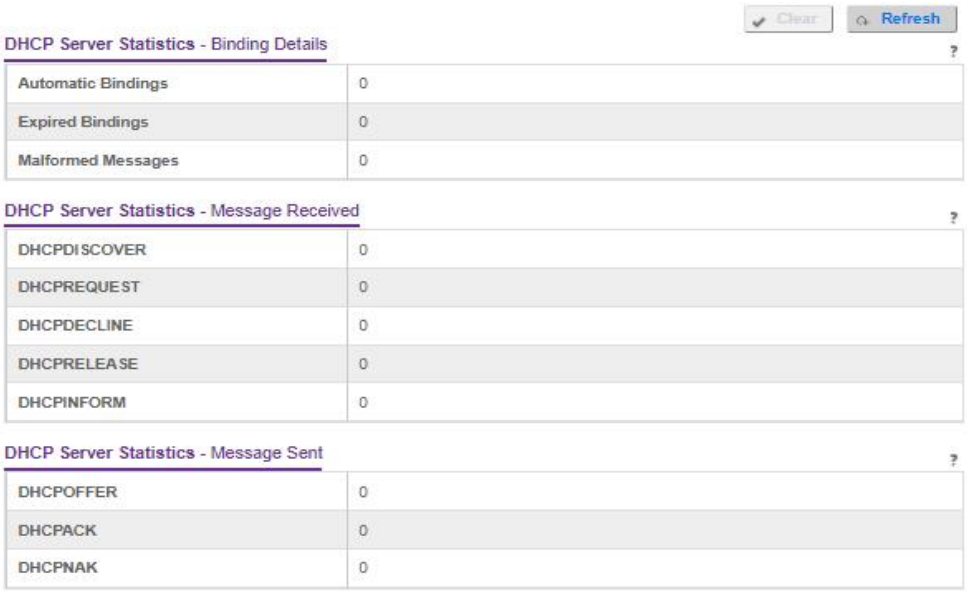


1. In **Pool Name** list, select the pool name.
2. **Option Code** specifies the Option Code configured for the selected Pool.
3. Use **Option Type** to specify the Option Type against the Option Code configured for the selected pool:
   - ASCII
   - Hex
   - IP Address
4. **Option Value** specifies the value against the Option Code configured for the selected pool.
5. Click the **Add** button.

   The Option Code is added for the selected pool.
6. To delete the Option Code for the selected pool, click the **Delete** button.

2.3.4. View DHCP Server Statistics

To view the DHCP server statistics:
System > Services > DHCP Server > DHCP Server Statistics.



The following table describes the DHCP Server Statistics fields.

Table14. DHCP Server Statistics

Field	Description
Automatic Bindings	The number of automatic bindings on the DHCP Server.
Expired Bindings	The number of expired bindings on the DHCP Server.
Malformed Messages	The number of the malformed messages.
DHCPDISCOVER	The number of DHCPDISCOVER messages received by the DHCP Server.
DHCPREQUEST	The number of DHCPREQUEST messages received by the DHCP Server.
DHCPDECLINE	The number of DHCPDECLINE messages received by the DHCP Server.
DHCPRELEASE	The number of DHCPRELEASE messages received by the DHCP Server.
DHCPINFORM	The number of DHCPINFORM messages received by the DHCP Server.
DHCPOFFER	The number of DHCPOFFER messages sent by the DHCP Server.
DHCPACK	The number of DHCPACK messages sent by the DHCP Server.
DHCPNAK	The number of DHCPNAK messages sent by the DHCP Server.

2.3.5. View DHCP Bindings Information

To view the DHCP bindings:
System > Services > DHCP Server > DHCP Bindings Information.

1. To display DHCP Bindings Information, select one of the following radio buttons:
   - **All Dynamic Bindings**. Specify all dynamic bindings to be deleted.
   - **Specific Dynamic Binding**. Specify specific dynamic binding to be deleted.

The following table describes the DHCP Bindings Information fields.

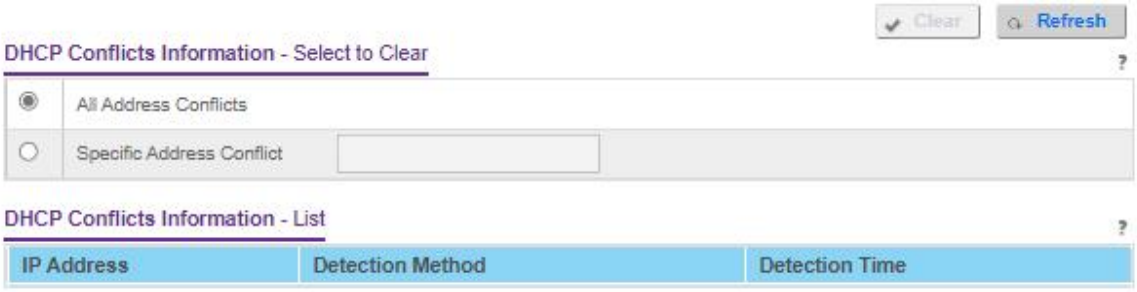
Table 34. DHCP Bindings Information

Field	Description
IP Address	The client's IP address.
Hardware Address	The client's hardware address.
Lease Time Left	The Lease Time Left in Days, Hours and Minutes dd:hh:mm format.
Type	The Type of Binding: Dynamic or Manual.

2.3.6. View DHCP Conflicts

You can view information on hosts with address conflicts, such as when the same IP address is assigned to two or more devices on the network.

To view the DHCP conflicts:
System > Services > DHCP Server > DHCP Conflicts Information.



1. To display DHCP conflicts information, select one of the following radio buttons:
   - **All Address Conflicts**. Specify all address conflicts to be deleted.
   - **Specific Address Conflict**. Specify a specific dynamic binding to be deleted.

The following table describes the DHCP Conflicts Information fields.

Table15. DHCP Conflicts Information

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

2.3.7. Configure the DHCP Relay

To configure DHCP relay:

System > Services > DHCP Relay.

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. Select the Admin mode **Disable** or **Enable** radio button.

   When you select Enable, DHCP requests are 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 is compared to the time stamp in the client's request packets, which represents the time since the client was powered up. Packets are forwarded only when the time stamp exceeds the minimum wait time. The range is (0 to 100).

4. Select the Circuit ID Option mode **Disable** or **Enable** radio button.

   If you select **Enable**, Relay Agent options are added to requests before they are forwarded to the server and removed from replies before they are forwarded to clients.

The following table describes the DHCP Relay Statistics fields.

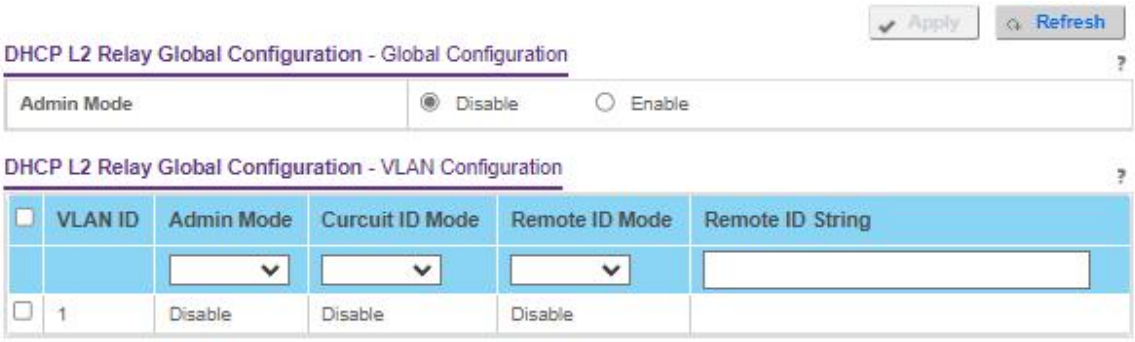
Table16. DHCP Relay Status

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.

2.4. DHCP L2 Relay

2.4.1. Configure Global DHCP L2 Relay Settings

To configure global DHCP L2 Relay settings:
System > Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration.



1. Select the Admin mode **Disable** or **Enable** radio button.

   For global configuration, this enables or disables the DHCP L2 Relay on the switch. The default is Disable.

2. For VLAN configuration, **VLAN ID** shows the VLAN ID configured on the switch.
   a. Use **Admin mode** to enable or disable the DHCP L2 Relay on the selected VLAN.
   b. Use **Circuit ID mode** to enable or disable the Circuit ID suboption of DHCP Option-82.
   c. Use **Remote ID String** to specify the Remote ID when Remote ID mode is enabled.
3. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

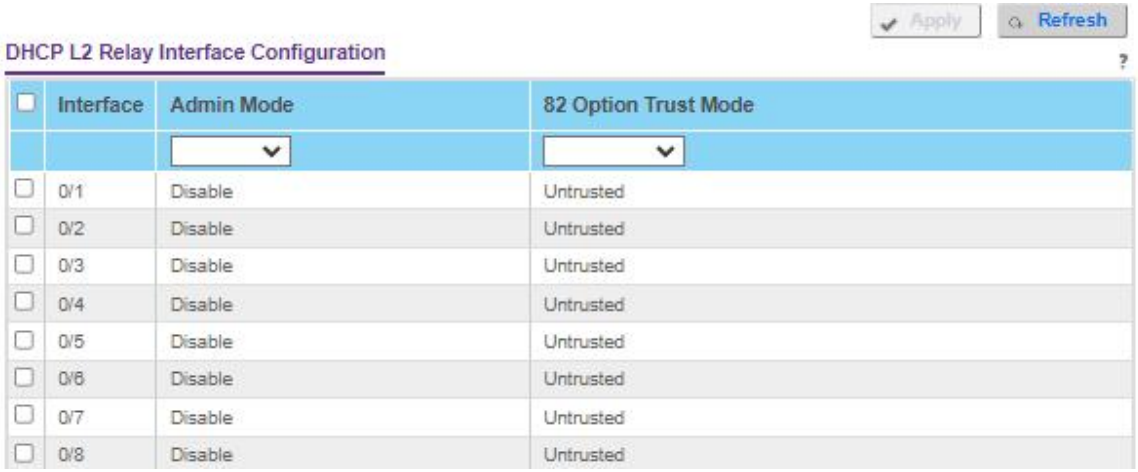
- Pagination Navigation Menu
  - Rows per page. Select how many table entries are displayed per screen. Possible values are 20, 50, 100, 200, and All.

  Note: If you select All, the browser might be slow to display the information.

  - < Display the previous page of the table data entries.
  - > Display the next page of the table data entries.

2.4.2. Configure a DHCP L2 Relay Interface

To configure DHCP L2 Relay:
System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration.



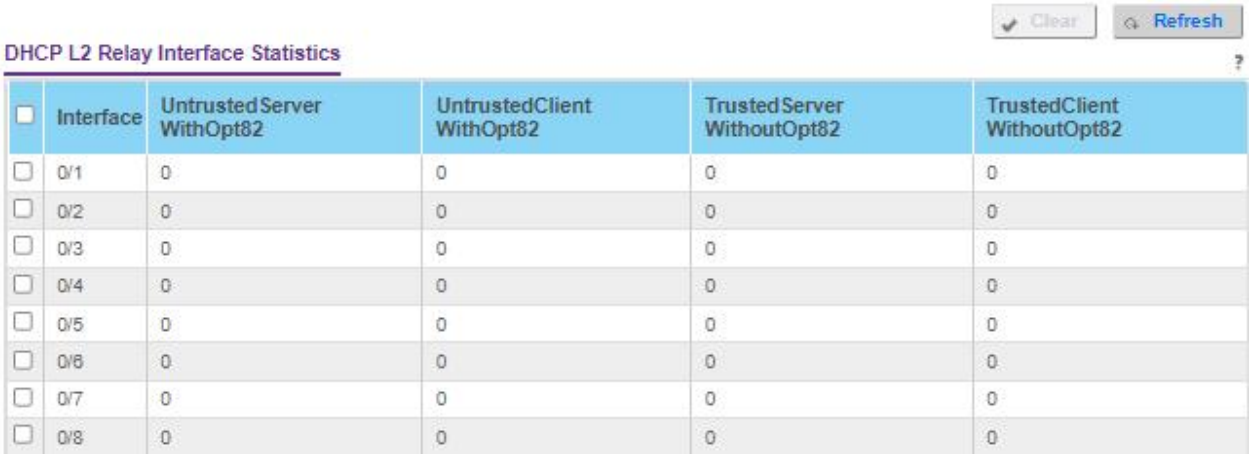
1. Use **Admin mode** to enable or disable the DHCP L2 Relay on the selected interface.

   The 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.

2.4.3. View DHCP L2 Relay Interface Statistics

To view the DHCP L2 Relay Interface Statistics:
System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Statistics.



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

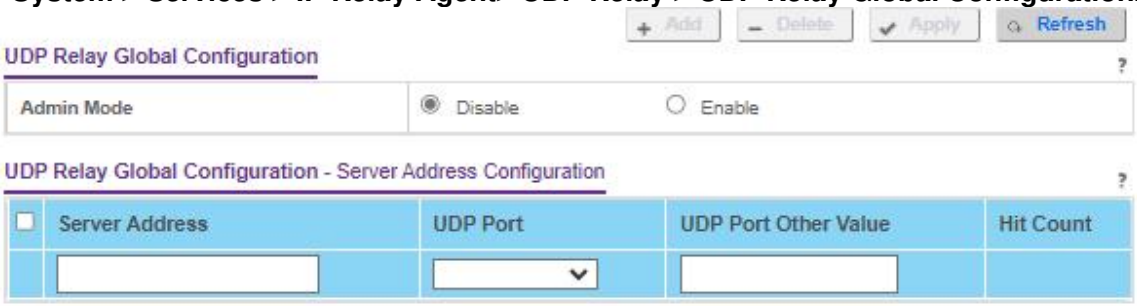
Table17. DHCP L2 Relay Interface Statistics

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.

2.4.4. Configure UDP Relay Global Settings

To configure UDP relay global settings:
System > Services > IP Relay Agent> UDP Relay > UDP Relay Global Configuration.



1. Select the Admin mode **Disable** or **Enable** radio button.

   This enables or disables 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 you to enter your 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 the **Add** button.

   This creates an entry in UDP Relay Table with the specified configuration.
6. To remove all entries or a specified one from UDP Relay Table, click the **Delete** button.
7. Click the **Apply** button.

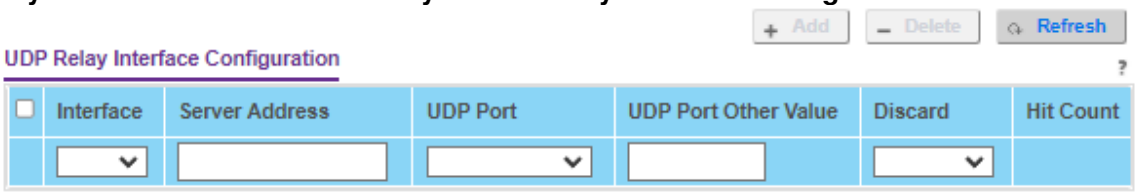
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

The **Hit Count** field displays the number of UDP packets hitting the UDP port.

To refresh the screen, click the **Update** button.

2.4.5. Configure UDP Relay Interface Settings

To configure UDP Relay Interface settings:
System > Services > UDP Relay > UDP Relay Interface Configuration.



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 the **Add** button.

   This creates an entry in UDP Relay Table with the specified configuration.
7. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To remove all entries or a specified one from UDP Relay Interface Configuration Table, click the **Delete** button.

The **Hit Count** field displays the number of UDP packets hitting the UDP port.

To refresh the screen, click the **Update** button.

2.4.6. Enable or Disable DHCPv6 Server

You can 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 enable or disable DHCP service:
System > Services > DHCPv6 Server > DHCPv6 Server Configuration.

1. Select the Admin mode **Disable** or **Enable** radio button.

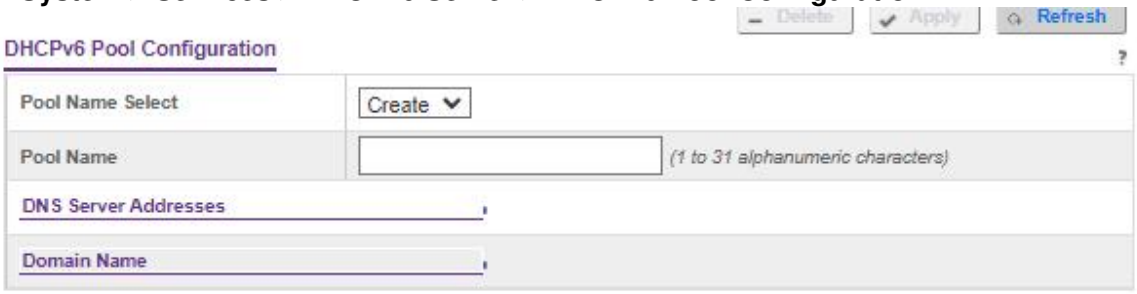
   This specifies whether the DHCPv6 Service administrative mode is enabled or disabled The default value is Disable.
2. Use the **DHCPv6 Server DUID** field to specify the DHCP Unique Identifier (DUID) of the DHCPv6 server.
3. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.4.7. Configure the DHCPv6 Pool

You can 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 configure DHCPv6 pool settings:
System > Services > DHCPv6 Server > DHCPv6 Pool Configuration.



The **Pool Name** field shows the names of all the existing pools and the **Create** option.

Note: If you are logged in as a user with read-only permission, the **Pool Name** field displays only the existing pool names. To create a pool, you must log in with the admin user name, which has read/write permissions.

1. To create a pool, select **Create**, and enter a unique name that identifies the DHCPv6 server pool to be created.

   The name can be up to 31 alphanumeric characters in length.

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.

   To delete the selected pool on the switch, click the **Delete** button.

4. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.4.8. Configure the DHCPv6 Prefix Delegation

To configure the DHCPv6 Prefix delegation settings:
System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration.

1. Select from the list of configured **Pool Names**.
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 the **Add** button.

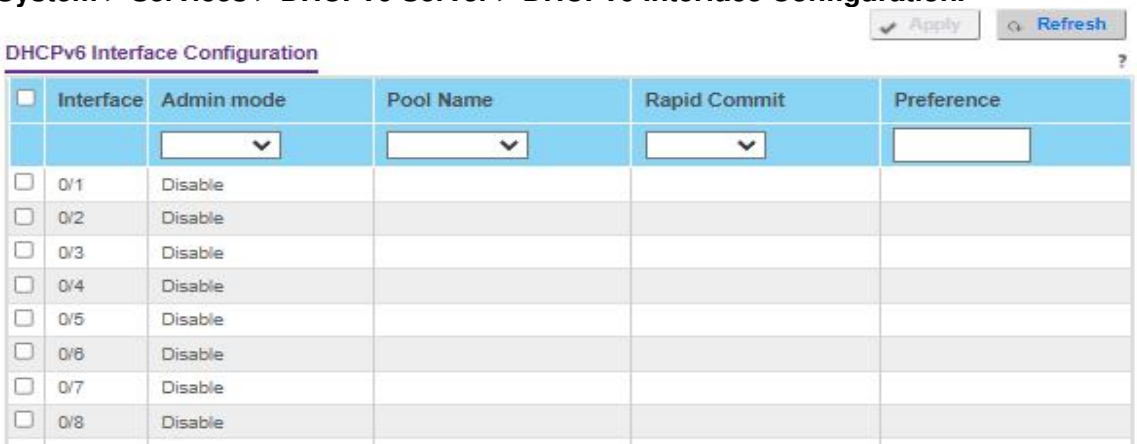
   The delegated prefix is added for the selected pool.
8. To delete the delegated prefix for the selected pool, click the **Delete** button.
9. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.4.9. Configure DHCPv6 Interface Settings

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

To configure DHCPv6 Interface settings:
System > Services > DHCPv6 Server > DHCPv6 Interface Configuration.



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 the **Go** button. The entry corresponding to the specified interface is 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.

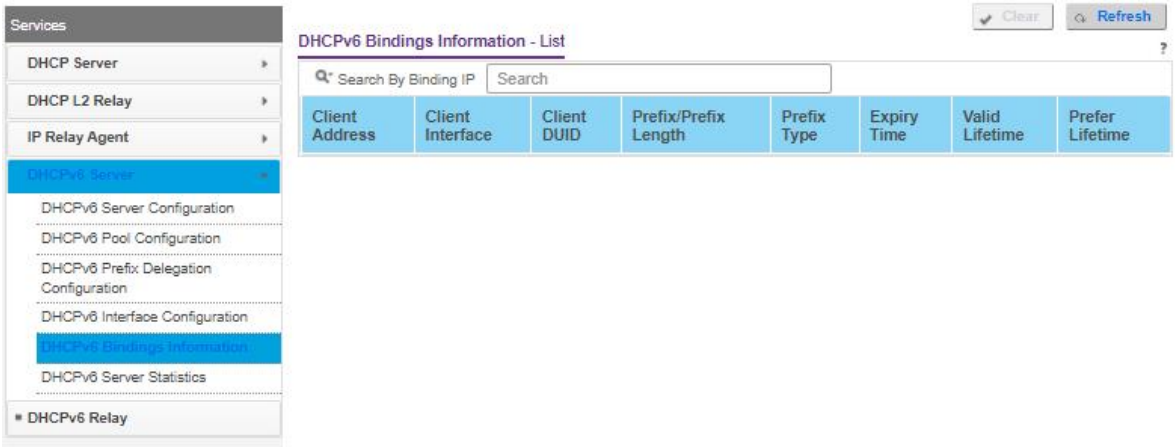
6. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.4.10. View DHCPv6 Bindings Information

You can 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 view DHCPv6 bindings information:
System > Services > DHCPv6 Server > DHCPv6 Bindings Information.



To refresh the screen, click the **Update** button.

The following table describes the nonconfigurable fields that are displayed.

Table18. DHCPv6 Binding 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.

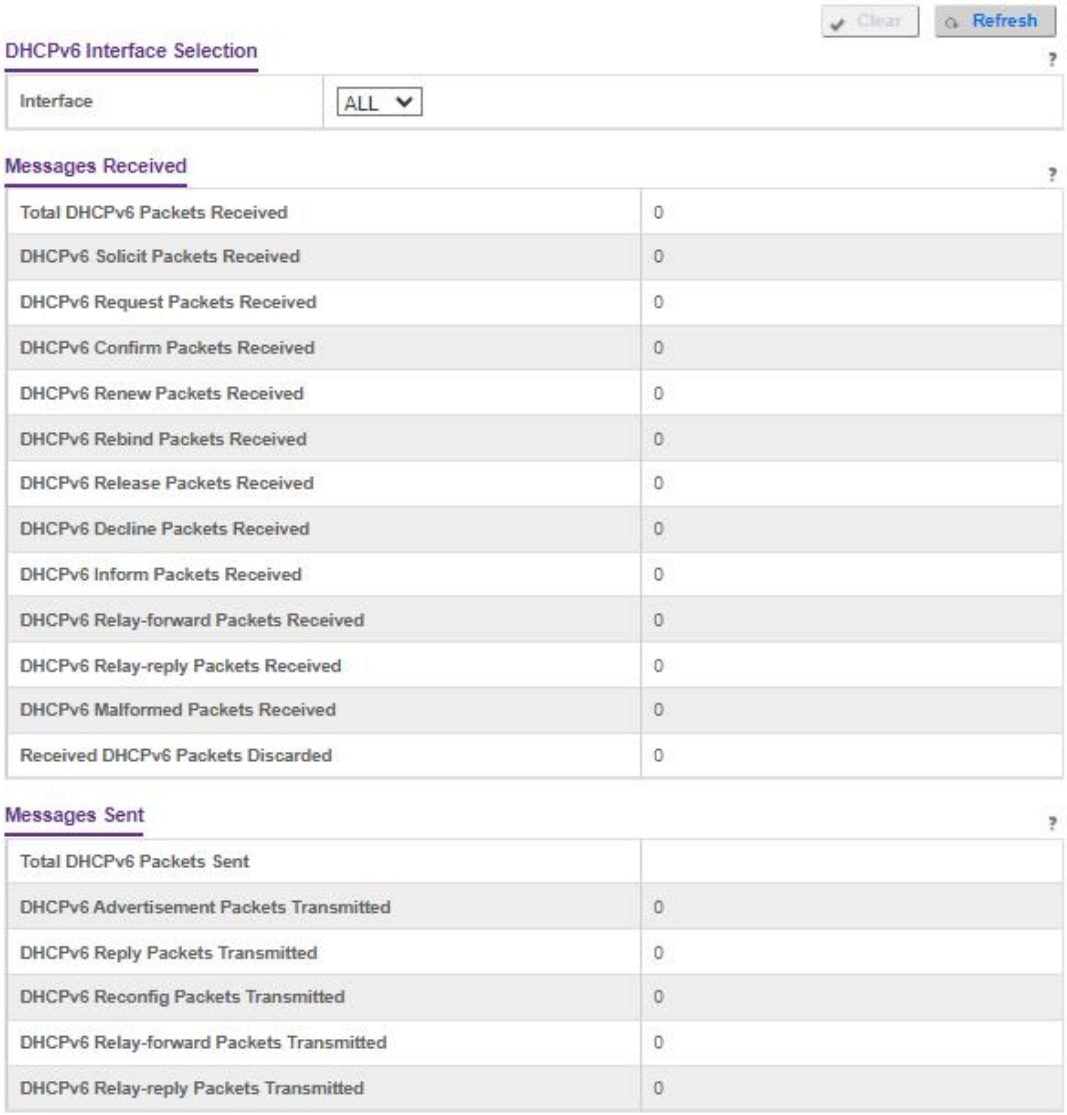
Table19. DHCPv6 Binding Information (continued)

Field	Description
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.

2.4.11. View DHCPv6 Server Statistics

You can view 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 screen indicate the various counts that accumulated since they were last cleared.

To view DHCPv6 server statistics:
System > Services > DHCPv6 Server > DHCPv6 Server Statistics.



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 is shown for all interfaces.

To reset the DHCPv6 counters for one or more interface, select each interface with the statistics to reset and click the **Clear** button.

To refresh the screen, click the **Update** button.

The following table describes the nonconfigurable fields that are displayed.

Table20. DHCPv6 Server Statistics

Field	Description
Messages Received	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 DHCP v6 client to a DHCP v6 server include solicit, request, confirm, renew, rebind, release, decline, and information-request messages. Additionally, a DHCP v6 relay agent can forward relay-forward messages to a DHCP v6 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.

Table21. DHCPv6 Server Statistics (continued)

Field	Description
DHCPv6 Request Packets Received	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 DHCP v6 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 DHCP v6 relay-reply messages received on the interface. This type of message is sent by a server to a DHCP v6 relay agent and contains the message for the relay agent to deliver to the client.
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	The number of Packets Discarded.
Messages Sent	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.

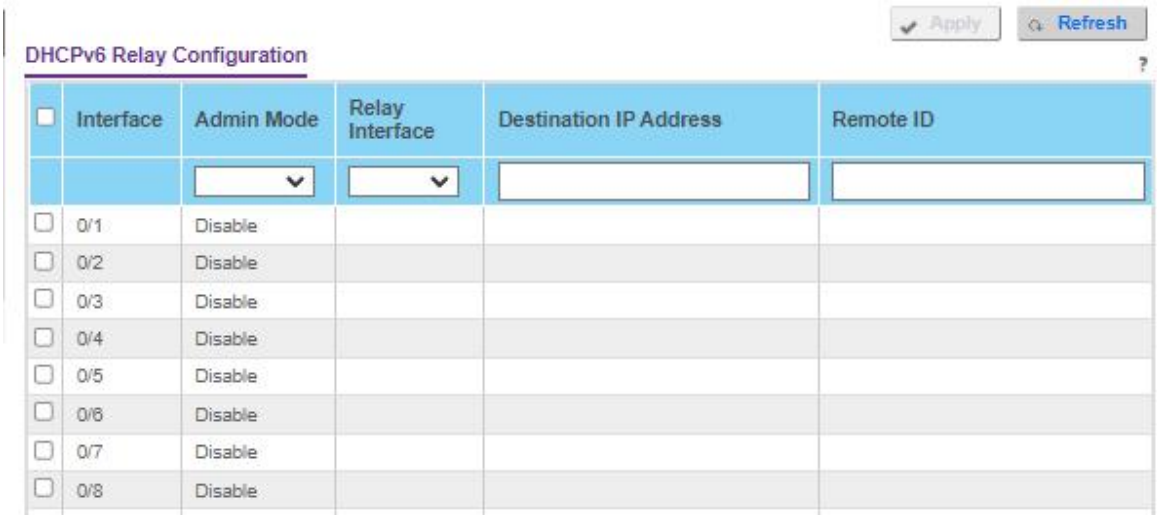
DHCPv6 Advertisement Packets Transmitted	The number of DHCPv6 Advertise messages sent by the interface. This type of message is sent by a server to a DHCPv6 client in response to a Solicit message and indicates that it is available for service.
DHCPv6 Reply Packets Transmitted	The number of DHCPv6 Reply messages sent from the interface to a DHCPv6 client in response to a solicit, request, renew, rebind, information-request, confirm, release, or decline message.

Table22. DHCPv6 Server Statistics (continued)

Field	Description
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.

2.4.12. Configure DHCPv6 Relay for an Interface

To configure DHCPv6 Relay for an interface:
System > Services > DHCPv6 Relay.



1. Select the Interface with the information to view or configure. You can either:
   - 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 is selected.
   - 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** list, 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 is derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

6. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

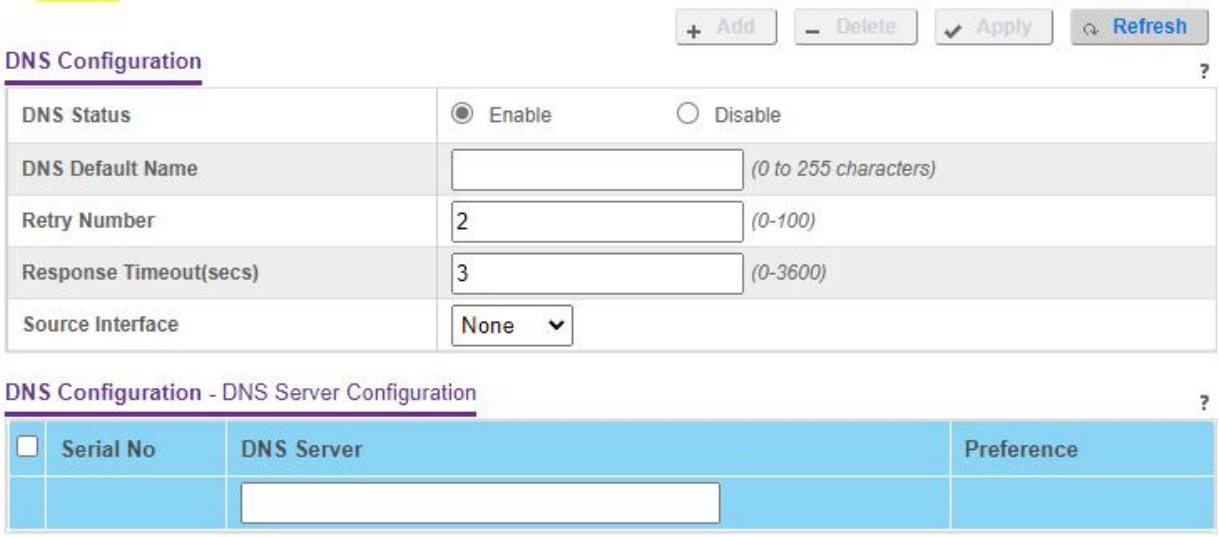
2.5. Configure DNS Settings

You can configure information about DNS servers that the network uses and how the switch operates as a DNS client.

2.5.1. Configure Global DNS Settings

You can configure global DNS settings and DNS server information.

To configure the global DNS settings:
System > Management > DNS > DNS Configuration.



1. Select the DNS Status **Disable** or **Enable** radio button:
   - **Enable**. Allow the switch to send DNS queries to a DNS server to resolve a DNS domain name. The 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 host name, this field is provides the domain name (for example, if default domain name is .com and the user enters test, then test is changed to test..com to resolve the name). The length of the name must not be longer than 255 characters.
3. Use **Retry Number** to specify the number of times to retry sending DNS queries to the 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 time-out ranges from 0 to 3600. The default value is 3.
5. Specify the **Source Interface** to use for DNS.

   Possible values are as follows:

   - None
   - VLAN 1
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Tunnel interface
   - Service port

   By default VLAN 1 is used as the source interface.
6. 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** field and click the **Add** button.

   The server appears in the list. You can specify up to eight DNS servers. The precedence is set in the order created.
7. To remove a DNS server from the list, select its check box and click the **Delete** button.

   If you click the **Delete** button without selecting a DNS server, all the DNS servers are deleted.
8. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen, click the **Update** button.

The following table displays DNS Server Configuration information.

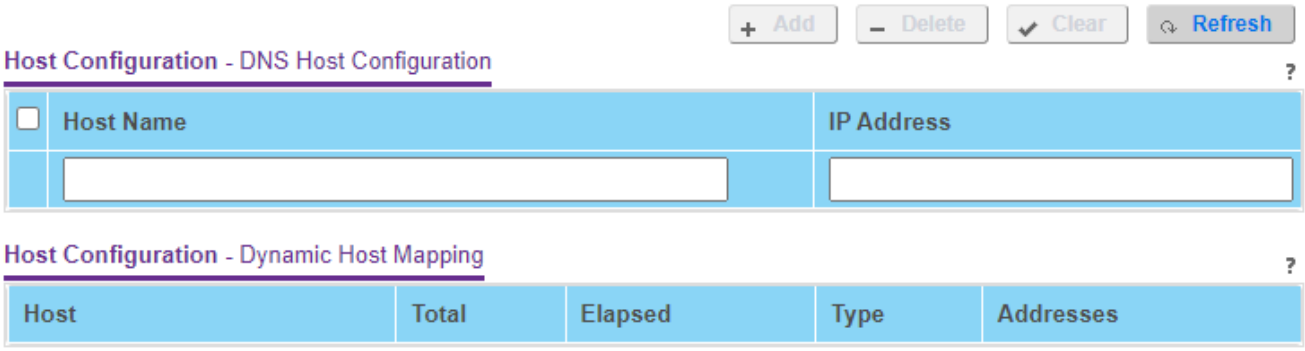
Table23. DNS Server Configuration

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 in which they were entered.

2.5.2. Add a Static Entry to the Local DNS Table

You can manually map host names to IP addresses or to view dynamic DNS mappings.

To add a static entry to the local DNS table:
System > Management > DNS > Host Configuration.



1. In the **Host Name (1 to 255 characters)** field, specify the static host name to add.

   Its length cannot exceed 255 characters and it is a mandatory field.

2. In the **IP Address** field, enter the IP address in standard IPv4 dot notation to associate with the host name.
3. Click the **Add** button.

   The entry appears in the list on the screen.

4. To remove an entry from the static DNS table, select its check box and click the **Delete** button.

To clear all the dynamic host name entries from the list, click the **Clear** button.

To refresh the screen, click the **Update** button.

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

Table24. DNS Dynamic Host Mapping

Field	Description
Host	Lists the host name that 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.

2.5.3. Configure the Switch Database Management Template Preference

A Switch Database Management (SDM) template is a description of the maximum resources a switch or router can use for various features. Different SDM templates allow different

combinations of scaling factors, enabling different allocations of resources depending on how the device is used. In other words, SDM templates enable you to reallocate system resources to support a different mix of features based on your network requirements.

Note: If you attach a unit to a stack and its template does not match the stack's template, then the new unit automatically reboots using the template used by the other stacking members. To avoid the automatic reboot, first set the template to the SDM template used by existing members of the stack. Then power off the new unit, attach it to the stack, and power it on.

You can configure SDM template preferences for the switch.

To configure the SDM Template Preference settings:
System > Management > DNS > SDM Template Preference.

1. Use **SDM Next Template ID** to configure the next active template.

   It is active only after the next reboot. To revert to the default template after the next reboot, use the Default option. Possible values are as follows:

   - 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.

Table25. SDM Template Preference Summary

Field	Description
SDM Current Template ID	The current active SDM template. Possible values are as follows: • Dual IPv4 and IPv6 • IPv4-routing Default • IPv4 Data Center

SDM Template	Identifies the template. The possible values are as follows: • 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.
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.

2.6. Configure SNMP

You can configure SNMP settings for SNMP V1/V2 and SNMPv3.

2.7. Configure the SNMP V1/V2 Community

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. You can change the defaults or to add other communities. Only the communities that you define can 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.

Note: If you want to use SNMP v3, use the User Accounts menu.

To configure the SNMP V1/V2 community:
System > SNMP > SNMP V1/V2 > Community Configuration.

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 can 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) is 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 can 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) is 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. In the **Access mode** menu, select **Read-Write** or **Read-Only**.

   This specifies the access level for this community.

5. Use **Status** to specify the status of this community by selecting **Enable** or **Disable**.

   If you select enable, the Community Name must be unique among all valid Community Names or the set request are rejected. If you select disable, the Community Name becomes invalid.

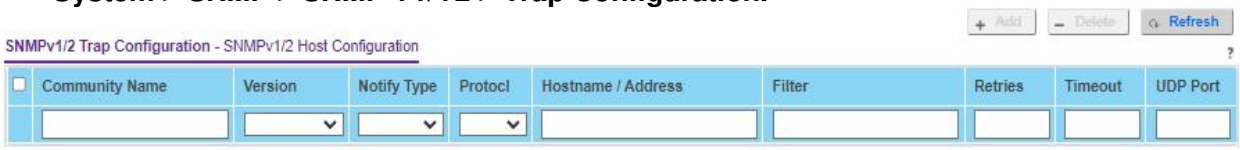
6. Click the **Add** button.

   This adds the selected community to the switch.

7. To delete the selected Community Name, click the **Delete** button.

2.7.1. Configure SNMP V1/V2 Trap Settings

To configure the SNMP V1/V2 trap settings:
System > SNMP > SNMP V1/V2 > Trap Configuration.



1. In the **Source Interface** list, select the source interface to use for SNMP Trap receiver.

Possible values are as follows:

- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port

VLAN 1 is used as source interface by default.

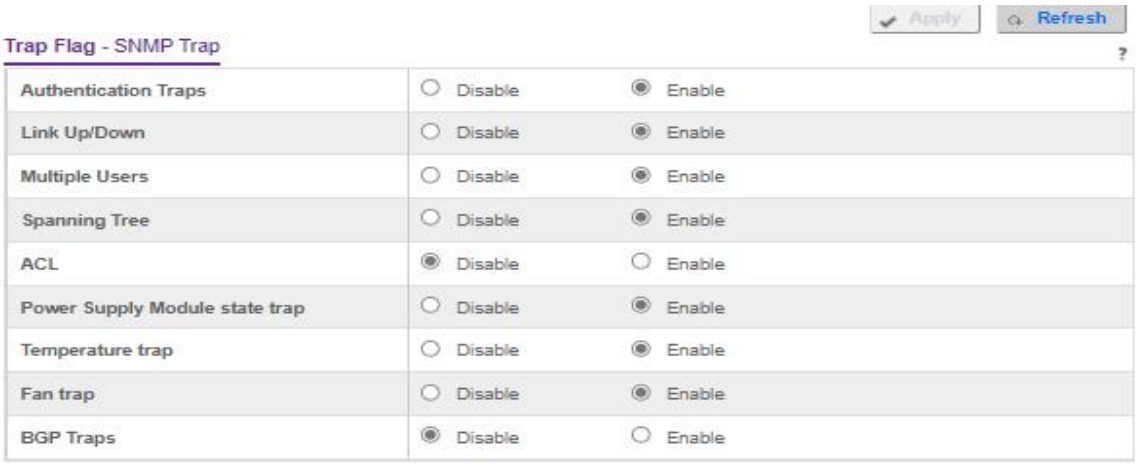
2. To add a host that receives SNMP traps, do the following steps:
   a. **Community Name**. Enter the community string for the SNMP trap packet to be sent to the trap manager. This name can be up to 16 characters and is case-sensitive.
   b. **Version**. Select the trap version to be used by the receiver:
      - **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. Select **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 the IPv6 address in xxxx:xxxx:xxxx:xxxxx:xxxx:xxxx:xxxx:xxxx to receive SNMP traps from this device. The length of the address cannot exceed 39 characters.
   e. **Status**. Select the receiver's status:
      - **Enable**. Send traps to the receiver
      - **Disable**. Do not send traps to the receiver.
   f. Click the **Add** button.
3. To modify information about an existing SNMP recipient, select the check box for the recipient, and change the desired fields.
4. To delete a recipient, select the check box for the recipient and click the **Delete** button.
5. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.7.2. Configure SNMP V1/V2 Trap Flags

You can 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 configure the trap flags:
System > SNMP > SNMP V1/V2 > Trap Flags.



1. Select the Authentication **Disable** or **Enable** radio button.

   This enables or disables activation of authentication failure traps. The factory default is Enable.

2. Select the Link Up/Down **Disable** or **Enable** radio button

   This enables or disables activation of link status traps.The factory default is Enable.

3. Select the Multiple Users **Disable** or **Enable** radio button

   This enables or disables activation of multiple user traps.The factory default is Enable. This trap is triggered when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).

4. Select the Spanning Tree **Disable** or **Enable** radio button.

   This enables or disables activation of spanning tree traps. The factory default is Enable.

5. Select the ACL **Disable** or **Enable** radio button.

   This enables or disables activation of ACL traps. The factory default is Disable.

6. Select the PoE **Disable** or **Enable** radio button.

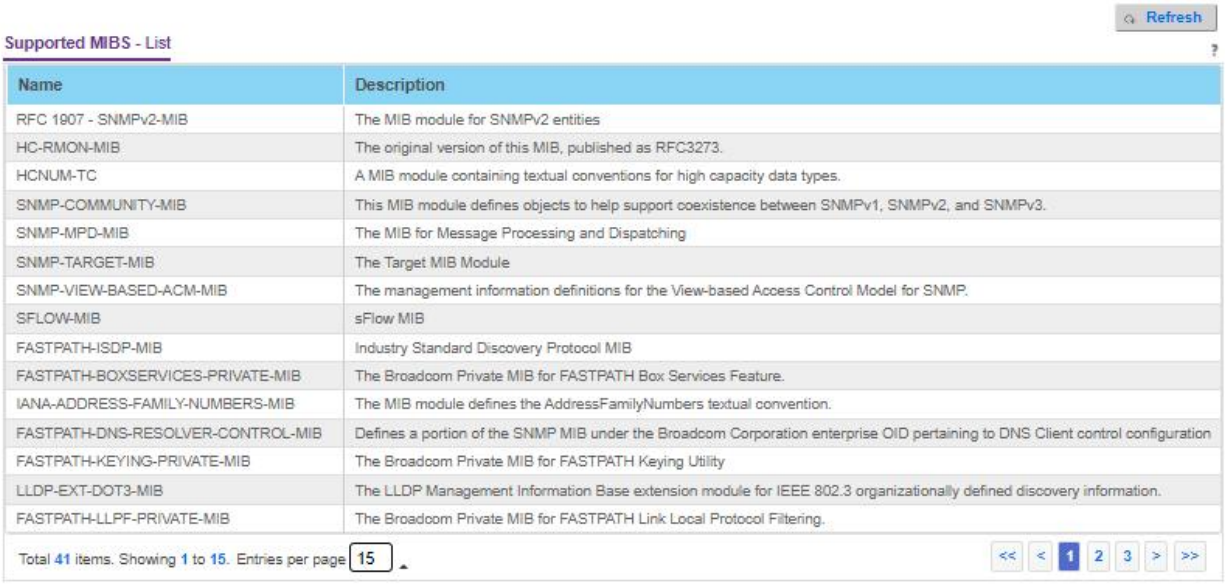
   This enables or disables activation of PoE traps. The factory default is Enable. Indicates whether PoE traps are sent.

7. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.7.3. View the Supported MIBs

To view all the MIBs supported by the switch:
System > SNMP > SNMP V1/V2 >Supported MIBs.



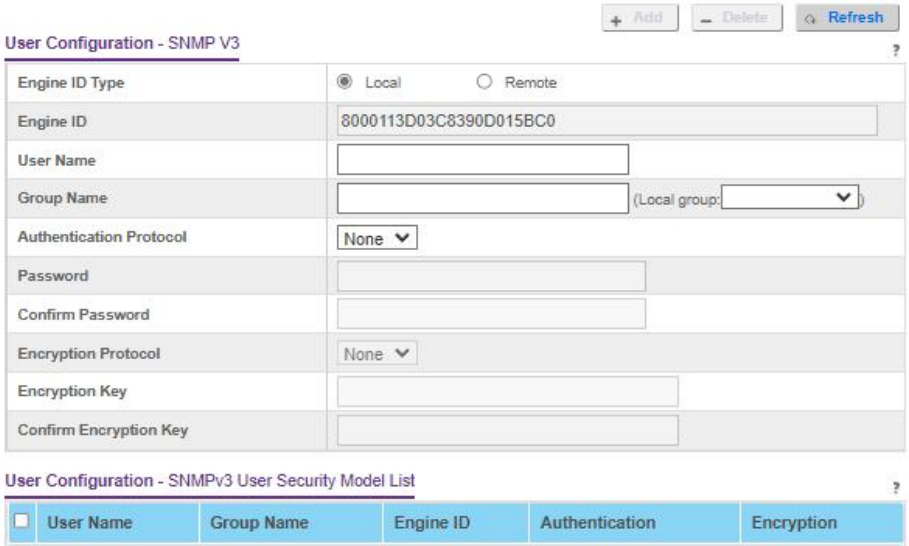
The following table describes the SNMP Supported MIBs Status fields.

Table26. SNMP Supported MIBs

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

2.7.4. Configure SNMP V3 Users

To configure SNMPv3 settings for the user account:
System > SNMP > SNMP V3 > User Configuration.



1. In the **User Name** list, select the user account to be configured.

   The **SNMP v3 Access mode** field indicates the SNMPv3 access privileges for the user account. The admin account has read/write access, and all other accounts are assigned read-only access.

2. Select an **Authentication Protocol** radio button.

   The valid Authentication Protocols are None, MD5 or SHA:

   - If you select **None**, the user cannot access the SNMP data from an SNMP browser.
   - If you select **MD5** or **SHA**, the user login password are used as the SNMPv3 authentication password, and you must therefore specify a password, and it must be eight characters long.

   This specifies the SNMPv3 Authentication Protocol setting for the selected user account.

3. Select a **Encryption Protocol** radio button.

   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.

   This specifies the SNMPv3 Encryption Protocol setting for the selected user account.

4. If you selected **DES** in the **Encryption Protocol** field, enter the encryption key in the **SNMPv3 Encryption Key** field.

   If you did not select DES, this field is ignored. Valid keys are 0 to 15 characters long. You must select the **Apply** check box to change the Encryption Protocol and Encryption Key.

5. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

2.8. LLDP Overview

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.

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:

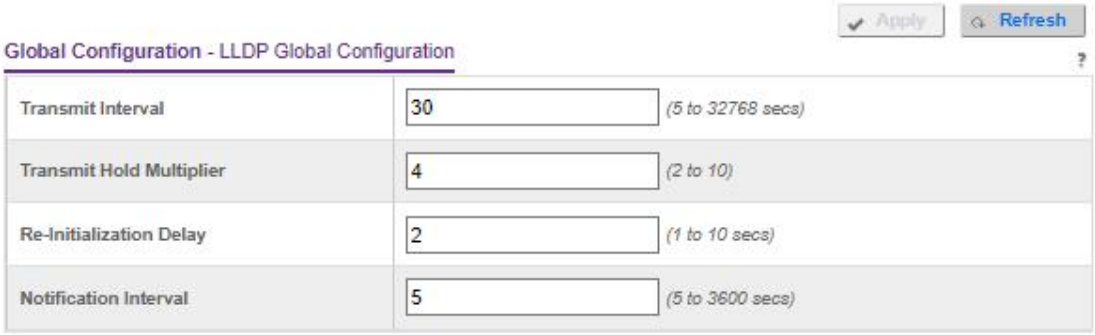
- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority, and DiffServ settings), enabling plug and play networking.

- 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).

2.8.1. Configure LLDP Global Settings

You can specify LLDP parameters that are applied to the switch.

To configure global LLDP settings:
System > LLDP > Global Configuration.



1. In the **Transmit Interval** field, enter the interval in seconds to transmit LLDP frames.

   The range is from 5 to 32768 secs. The default value is 30 seconds.

2. In the **Transmit Hold Multiplier** field, enter the multiplier on Transmit Interval to assign TTL.

   The range is from 2 to 10 secs. The default value is 4.

3. In the **Re-Initialization Delay** field, enter the delay before re-initialization.

   The range is from 1 to 10 secs. The default value is 2 seconds.

4. In the **Notification Interval** field, enter the interval in seconds for transmission of notifications.

   The range is from 5 to 3600 secs. The default value is 5 seconds.

5. Click the **Apply** button.

   The updated configuration is sent to the switch. The changes take effect immediately but are not retained across a power cycle unless a save is performed.

2.8.2. Configure the LLDP Interface

To configure the LLDP interface:
System > LLDP > Interface Configuration.

1. Use **Go To Port** to enter the Port in unit/slot/port format and click the **Go** button.

   The entry corresponding to the specified Port, is selected.

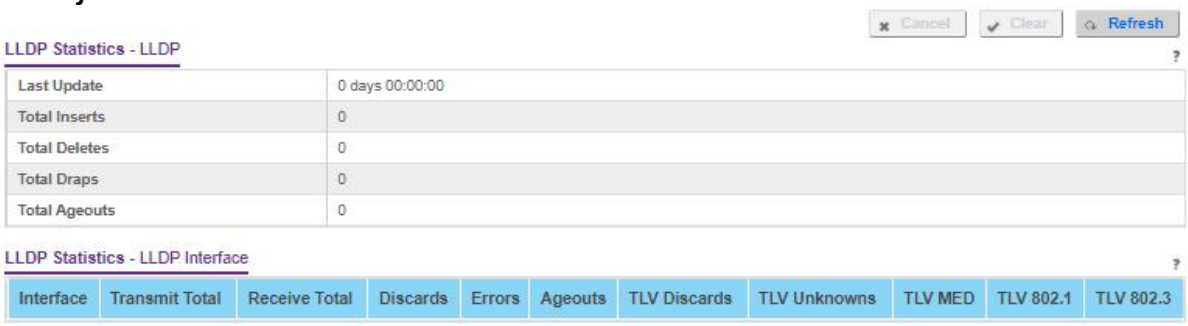
2. Use **Port** to specify the list of ports on which LLDP - 802.1AB can be configured.

The **Link Status** field indicates whether the link is up or down.

3. Use **Transmit** to specify the LLDP - 802.1AB transmit mode for the selected interface.
4. Use **Receive** to specify the LLDP - 802.1AB receive mode for the selected interface.
5. Use **Notify** to specify the LLDP - 802.1AB notification mode for the selected interface.
6. 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.
7. Use **Transmit Management Information** to specify whether management address is transmitted in LLDP frames for the selected interface.

2.8.3. View LLDP Statistics

To view LLDP statistics:
System > LLDP > Statistics.



The following table describes the LLDP Statistics fields.

Table27. LLDP Statistics

Field	Description
Last Update	The time when an entry was created, modified or deleted in the tables associated with the remote system.
Total Inserts	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) was inserted into tables associated with the remote systems.
Total Deletes	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) was deleted from tables associated with the remote systems.
Total Drops	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.

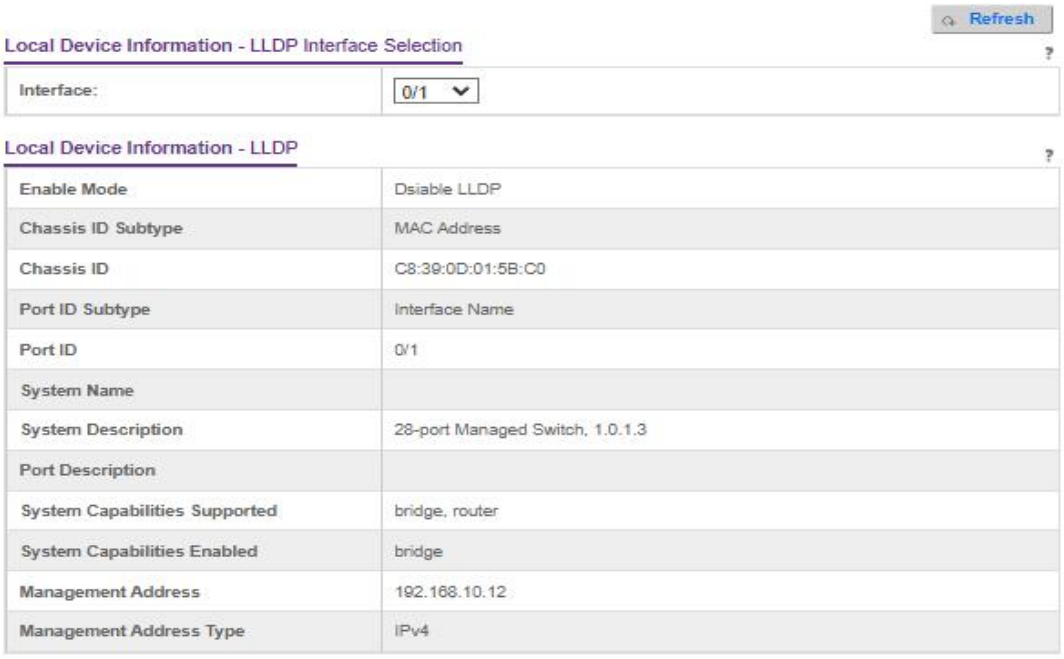
Total Age outs	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) was deleted from tables associated with the remote systems because the information timeliness interval has expired.
Interface	The unit/slot/port for the interfaces.
Transmit Total	The number of LLDP frames transmitted by the LLDP agent on the corresponding port.

Table28. LLDP Statistics (continued)

Field	Description
Receive Total	The number of valid LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
Discards	The number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.
Errors	The number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Age outs	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) was deleted from tables associated with the remote entries because information timeliness interval expired.
TLV Discards	The number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.
TLV Unknowns	The number of LLDP TLVs received on the local ports which were not recognized by the LLDP agent on the corresponding port.
TLV MED	The total number of LLDP-MED TLVs received on the local ports.
TLV 802.1	The total number of LLDP TLVs received on the local ports which are of type 802.1.
TLV 802.3	The total number of LLDP TLVs received on the local ports which are of type 802.3.

2.8.4. View LLDP Local Device Information

To view LLDP local device information:
System > LLDP > Local Device Information.



1. In **Interface** list, select the ports on which LLDP - 802.1AB frames can be transmitted.

The following table describes the LLDP Local Device Information fields.

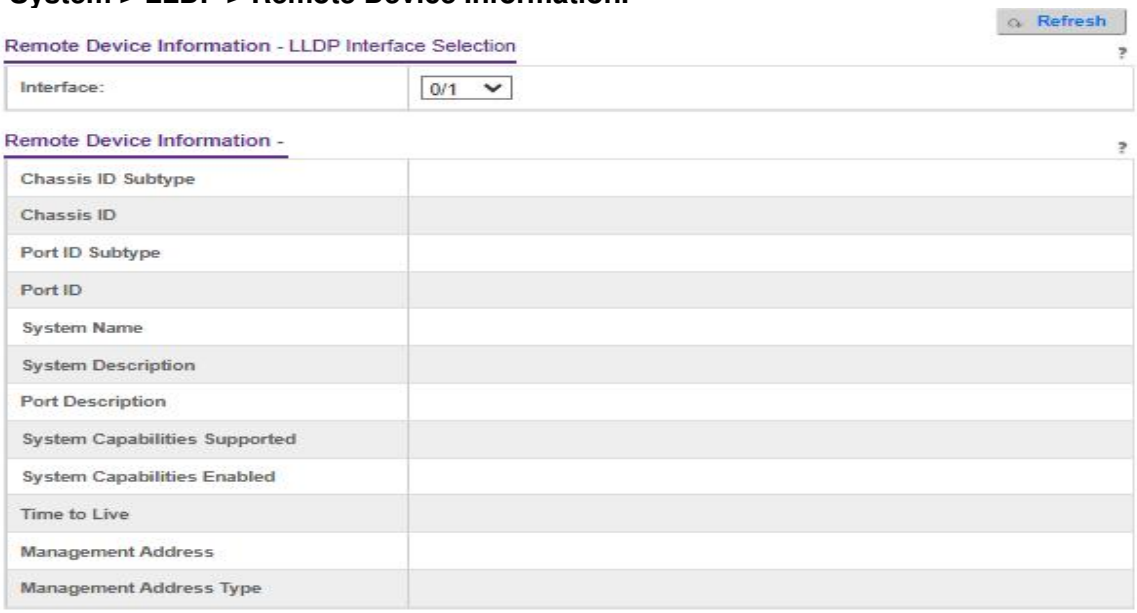
Table29. LLDP Local Device Information

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

2.8.5. View LLDP Remote Device Information

You can view information on remote devices connected to the port.

To view LLDP remote device information:
System > LLDP > Remote Device Information.



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

The following table describes the LLDP Remote Device Information fields.

Table30. LLDP Remote Device Information

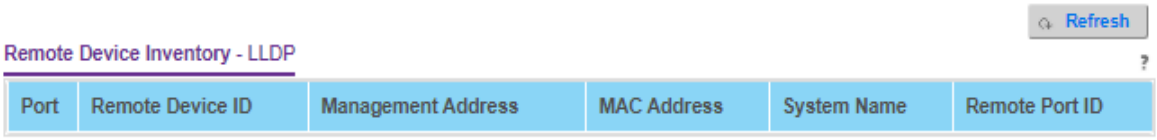
Field	Description
Remote ID	The remote ID.
Chassis ID	The chassis component associated with the remote system.
Chassis ID Subtype	The source of the chassis identifier.
Port ID	The port component associated with the remote system.
Port ID Subtype	The source of port identifier.
System Name	The system name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

Table31. LLDP Remote Device Information (continued)

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

2.8.6. View LLDP Remote Device Inventory

To view LLDP remote device inventory:
System > LLDP > LLDP > Remote Device Inventory.



The following table describes the LLDP Remote Device Inventory fields.

Table32. LLDP Remote Device Inventory

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

2.8.7. Configure LLDP-MED Global Settings

You can specify LLDP-MED parameters that are applied to the switch.

To configure LLDP-MED global settings:
System > LLDP > LLDP-MED > Global Configuration.

1. In the **Fast Start Repeat Count** field, enter the number of LLDP PDUs that are transmitted when the protocol is enabled.

   The range is from (1 to 10). Default value of fast repeat count is 3.

   The **Device Class** field 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 and so on], Class II Media [Conference Bridge and so on], Class III Communication [IP Telephone and so on]). The fourth device is Network Connectivity Device, which is typically a LAN Switch/Router, IEEE 802.1 Bridge, IEEE 802.11 Wireless Access Point and so on

2.8.8. Configure LLDP-MED Interface

To configure LLDP-MED Interface
System > LLDP > LLDP-MED > Interface Configuration.

The **Link Status** field displays the link status of the port (up or down).

The **Operational Status** field displays whether the LLDP-MED TLVs are transferred on this interface.

1. Use **Go To Port** to enter the Port in unit/slot/port format and click the **Go** button.

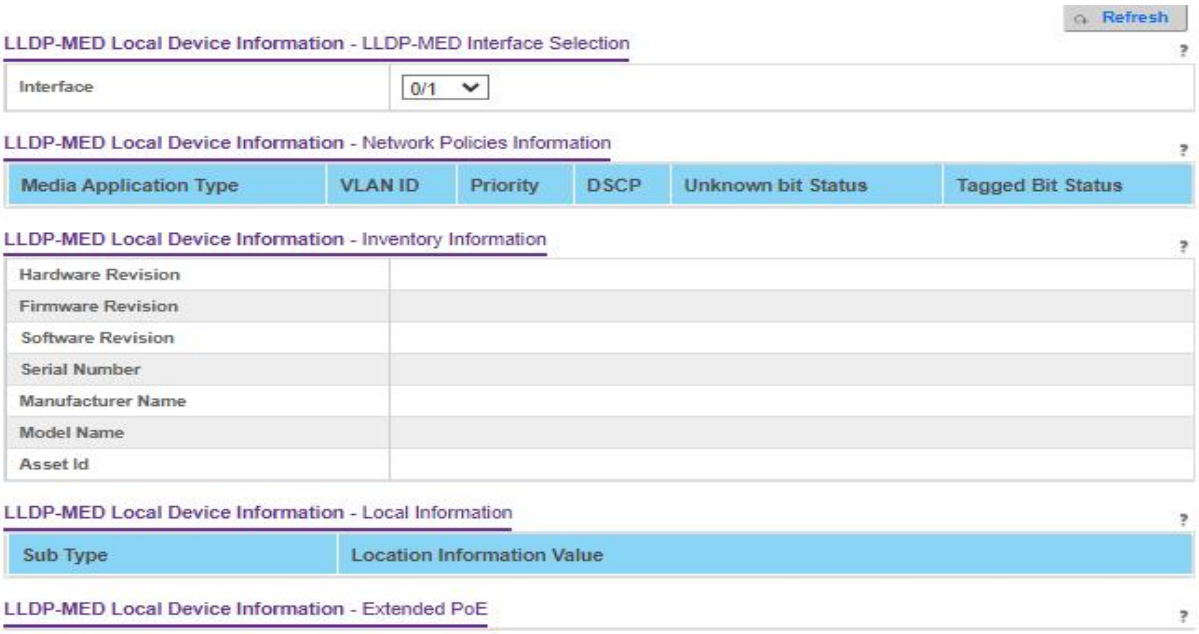
   The entry corresponding to the specified Port, is selected.

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 is 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.

2.8.9. View LLDP-MED Local Device Information

To view LLDP-MED local device information:
System > LLDP > LLDP-MED > Local Device Information.



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.

Table33. LDP-MED Local Device Information

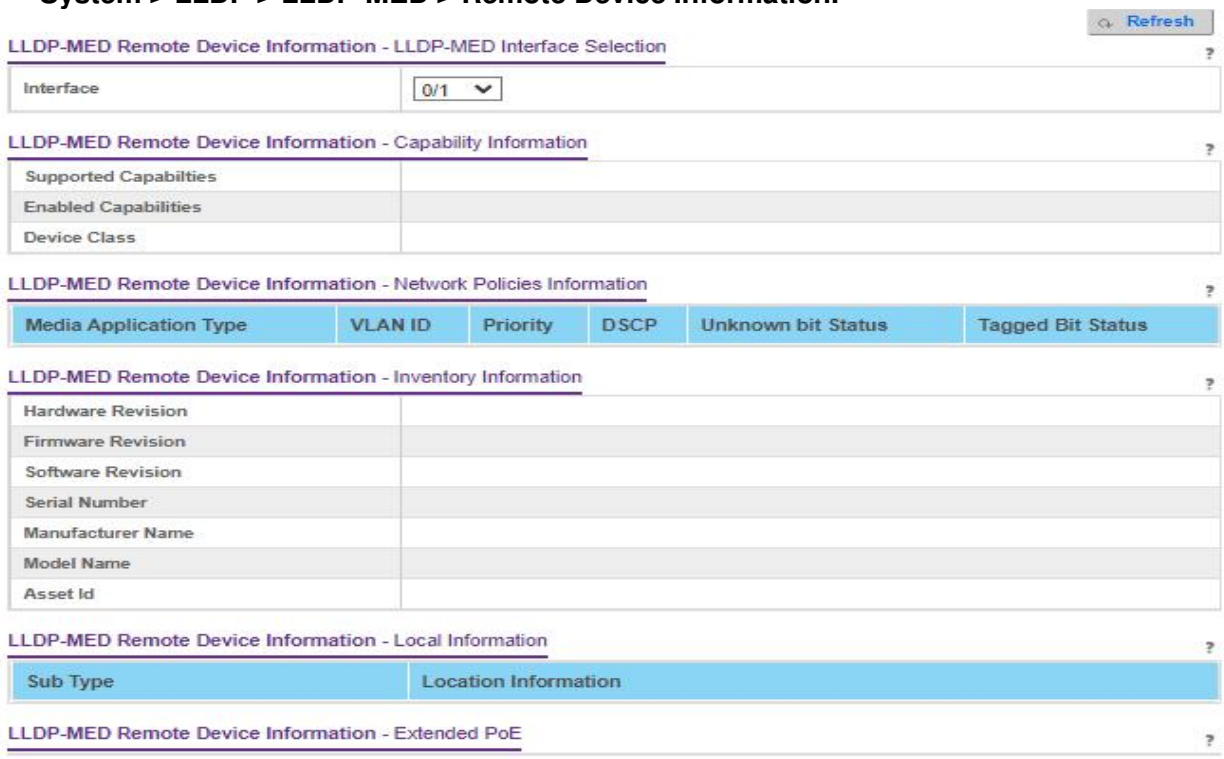
Field	Description
Network Policy Information: Specifies if network policy TLV is present in the LLDP frames.	
Media Application Type	The application type. Types of application types are **unknown**, **voicesignaling**, **guestvoice**, **guestvoicesignalling**, **softphonevoice**, **videoconferencing**, **streammingvideo**, **vidoesignalling**. Each application type that is received has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port can receive one or many such application types. If a network policy TLV was transmitted, only then would this information be displayed
Inventory: Specifies if inventory TLV is present in LLDP frames	
Hardware Revision	Specifies hardware version.

Table34. LDP-MED Local Device Information (continued)

Field	Description
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	The location information as a string for given type of location ID.

2.8.10. View LLDP-MED Remote Device Information

To view LLDP-MED remote device information:
System > LLDP > LLDP-MED > Remote Device Information.



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

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

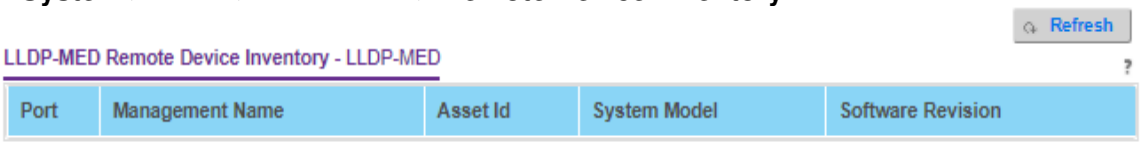
Table35. LLDP-MED Remote Device Information

Field	Description
Capability Information: 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	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 can receive one or many such application types. If a network policy TLV was received on this port, only then would this information be displayed.
VLAN Id	The VLAN ID associated with a particular policy type.
Priority	The priority associated with a particular policy type.
DSCP	The DSCP associated with a particular policy type.
Unknown Bit Status	The unknown bit associated with a particular policy type.
Tagged Bit Status	The tagged bit associated with a particular policy type.
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	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	The remote ports PSE power value in tenths of watts.

Source	The remote ports PSE power source.
Priority	The remote ports PSE power priority.
Extended POE PD: Specifies if extended PD TLV is received in LLDP frame on this port.	
Required	The remote port's PD power requirement.
Source	The remote port's PD power source.
Priority	The remote port's PD power priority.

2.8.11. View LLDP-MED Remote Device Inventory

To view LLDP-MED remote device inventory:
System > LLDP > LLDP-MED > Remote Device Inventory.



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

Table36. LLDP-MED Remote Device Inventory

Field	Definition
Port	The list of all the ports on which LLDP-MED is enabled.
Management Address	The advertised management address of the remote system.
MAC Address	The MAC address associated with the remote system.

Table37. LLDP-MED Remote Device Inventory (continued)

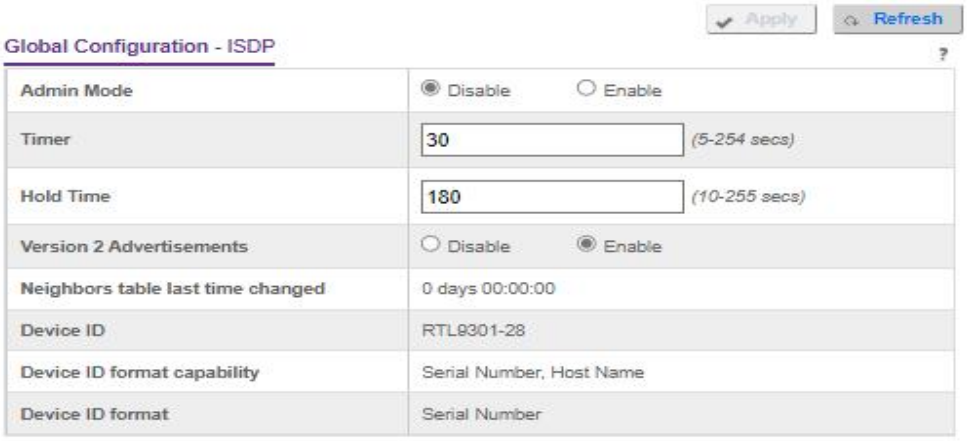
Field	Definition
System Model	Specifies model name of the remote device.
Software Revision	Specifies Software version of the remote device.

2.9. Configure ISDP

You can configure ISDP global and interface settings.

2.9.1. Configure ISDP Basic Global Settings

To configure ISDP basic global settings:
System > ISDP > Basic > Global Configuration.



1. Select the Admin mode **Disable** or **Enable** radio button.

   This specifies whether the ISDP Service is 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. The 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 must store information sent in the ISDP packet before discarding it. The range 10 to 255 seconds. The default value is 180 seconds.

4. Select the Version 2 Advertisements **Disable** or **Enable** radio button.

   This enables or disables the sending of ISDP version 2 packets from the device. The default value is Enabled.

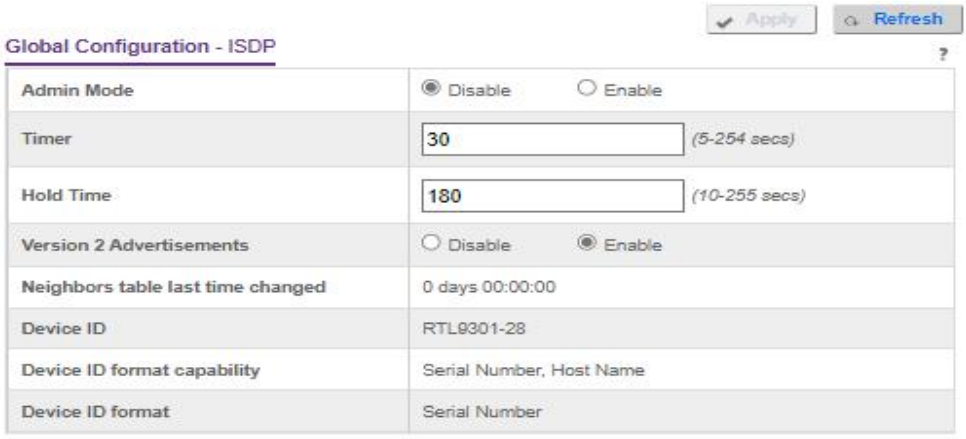
The following table describes the ISDP Basic Global Configuration fields.

Table38. ISDP Basic Global Configuration

Field	Description
Neighbors table last time changed	Specifies if
Device ID	The device ID of this switch.
Device ID Format Capability	The device ID format capability.
Device ID Format	The device ID format.

2.9.2. Configure ISDP Global Settings

To configure ISDP global settings:
System > ISDP > Advanced > Global Configuration.



1. Select the Admin mode **Disable** or **Enable** radio button.

   This specifies whether the ISDP Service is enabled or disabled. The default value is Enable.

2. In the **Timer** field, specify the period of time between sending new ISDP packets.

   The range is 5 to 254 seconds. The default value is 30 seconds.

3. In the **Hold Time** field, specify the hold time for ISDP packets that the switch transmits.

   The hold time specifies how long a receiving device must store information sent in the ISDP packet before discarding it. The range 10 to 255 seconds. The default value is 180 seconds.

4. Select the Version 2 Advertisements **Disable** or **Enable** radio button.

   This enables or disables the sending of ISDP version 2 packets from the device. The default value is Enable.

The following table describes the ISDP Advanced Global Configuration fields.

Table39. ISDP Advanced Global Configuration

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

2.9.3. Configure an ISDP Interface

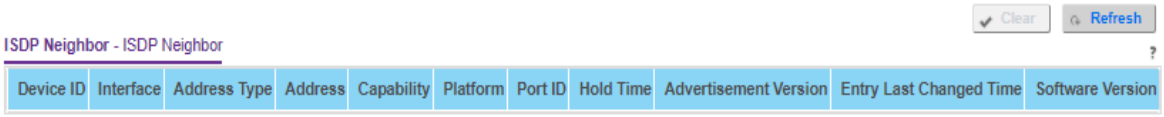
To configure an ISDP interface:
System > ISDP > Advanced > Interface Configuration.

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.

2.9.4. View an ISDP Neighbor

To view an ISDP neighbor:
System > ISDP > Advanced > Neighbor.



The following table describes the ISDP Neighbor fields.

Table40. ISDP Neighbor

Field	Description
Device ID	The device ID of the ISDP neighbor.
Interface	The interface on which the neighbor is discovered.
Address	The address of the neighbor.
Capability	The capability of the neighbor. These are supported: • Router • Trans Bridge • Source Route • Switch • Host • IGMP • Repeater
Platform	The model type of the neighbor. (0 to 32)
Port ID	The port ID on the neighbor.
Hold Time	The hold time for ISDP packets that the neighbor transmits.

Table41. ISDP Neighbor (continued)

Field	Description
Advertisement Version	The ISDP version sending from the neighbor.
Entry Last Changed Time	The time since last entry is changed.
Software Version	The software version on the neighbor.

2.9.5. View ISDP Statistics

To view ISDP statistics:
System > ISDP > Advanced > Statistics.

The following table describes the ISDP Statistics fields.

Table42. ISDP Statistics

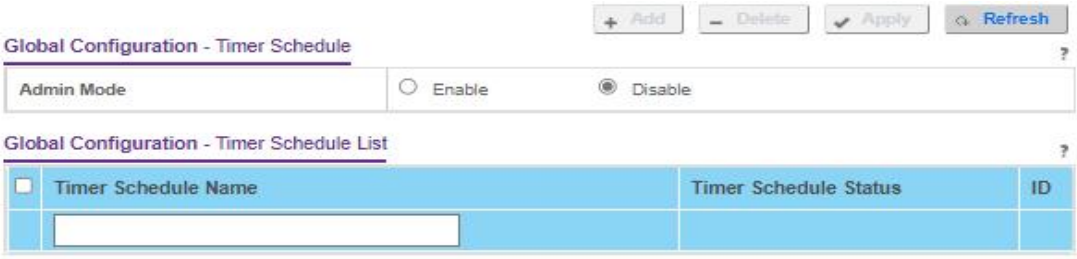
Field	Description
ISDP Packets Received	The ISDP packets received including ISDPv1 and ISDPv2 packets.
ISDP Packets Transmitted	The ISDP packets transmitted including ISDPv1 and ISDPv2 packets.
ISDPv1 Packets Received	The ISDPv1 packets received.
ISDPv1 Packets Transmitted	The ISDPv1 packets transmitted.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

2.9.6. Timer Schedule

You can configure the global timer settings and the timer schedule.

2.9.7. Configure the Global Timer Settings

To configure the global timer settings:
System > Timer Schedule > Basic > Global Configuration.



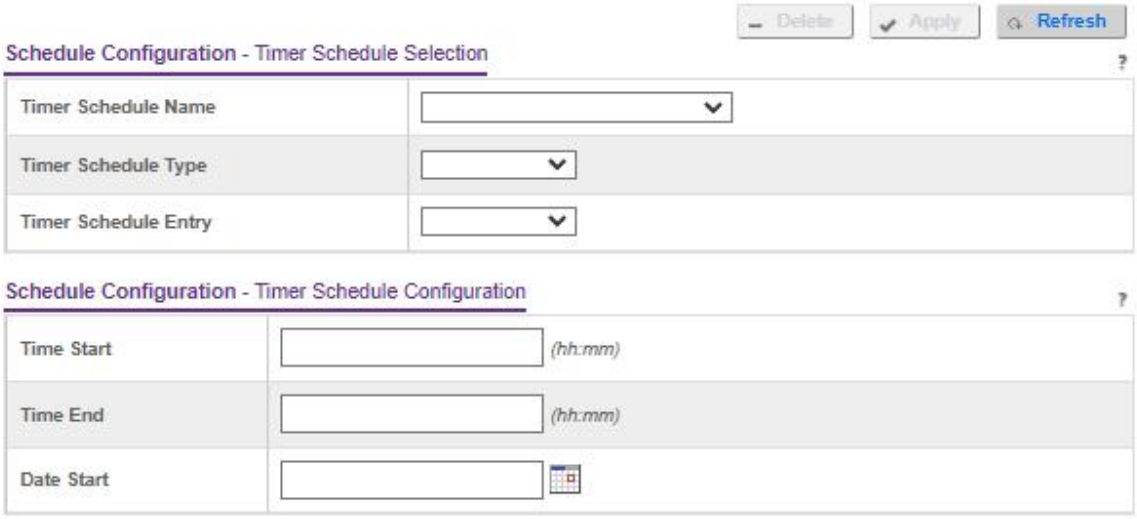
1. Use the **Timer Schedule Name** to specify the name of a timer schedule.
2. Click the **Add** button.

   The timer is added. The configuration changes take effect immediately.
3. To delete the selected timer schedules, click the **Delete** button.

   The configuration changes take effect immediately.

2.9.8. Configure the Timer Schedule

To configure the timer schedule:
System > Services > Timer Schedule > Advanced > Schedule Configuration.



1. In the **Timer Schedule Name** list, select the timer schedule.
2. In the **Timer Schedule Type** list, select **Absolute** or **Periodic**.
3. In the **Timer Schedule Entry** list, select the number of the timer schedule entries to be configured or added.

   If you are adding an entry, select **new**.
4. In the **Time Start** field, enter the time of the day in format (HH:MM) when the schedule operation is started.

   This field is required. If no time is specified, the schedule does not start running.
5. In the **Time End** field, enter 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 repeats.

   If recurrence is not needed (a timer schedule must 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 is triggered every day from Monday to Friday. Every Day(s) selection means that the schedule is triggered every defined number of days. If number of days is not specified, then the schedule is triggered every day.

   - **Weekly**. The timer schedule works with weekly recurrence

     Every Week(s). Define the number of weeks when the schedule is triggered. If number of weeks is not specified, then the schedule is triggered every week.

     - **WeekDay**. Specify the days of week when the schedule operates.

   - **Monthly**. The timer schedule works with monthly recurrence

     Monthly mode. Show the day of the month when the schedule is triggered. Field Every Month(s) means that the schedule is triggered every defined number of months.

9. Click the **Apply** button.

   The updated configuration is sent to the switch. The configuration changes take effect immediately.

3. Configure Switching Information

3.1. Port Settings

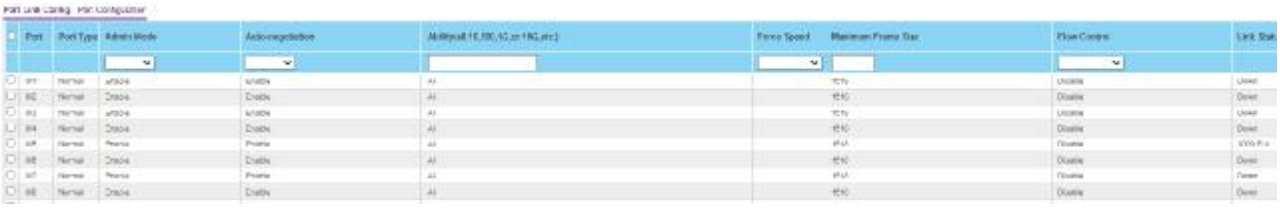
You can view and monitor the physical port information for the ports available on the switch.

3.1.1. Configure Port Settings

You can configure the physical interfaces on the switch.

To configure port settings:

Switching > Ports > Port Configuration.



1. Use **Port** to select the interface.
2. Use **STP Mode** to select the Spanning Tree Protocol administrative mode for the port or LAG.

   The possible values are as follows:

   - **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. In the **Admin Mode** list, select **Enable** or **Disable**.

   This sets the port control administrative mode.For the port to participate in the network, you must select **Enable**. The factory default is Enable.
4. From the **LACP Mode** list, select **Enable** or **Disable**.

   This selects the Link Aggregation Control Protocol administrative mode. The mode must be enabled in order for the port to participate in link aggregation. The factory default is Enable.
5. From the **Auto-negotiation** list, select **Enable** or **Disable**.

   This specifies the auto-negotiation mode for this port. The default is Enable.

   Note: After you change the auto-negotiation mode, the switch might be inaccessible for a number of seconds while the new settings take effect.

6. From the **Speed** list, select the speed value for the selected port.

   Possible field values are as follows:

   - **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 ( ). For you to set the auto-negotiation speed, the auto-negotiation mode must be set to **Enable**. The default is **Auto**.

   Note: After you change the speed value, the switch might be inaccessible for a number of seconds while the new settings take effect.

7. From the **Duplex Mode** list, select the duplex mode for the selected port.

   Possible values are as follows:

   - **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 you change the duplex mode, the switch might be inaccessible for a number of seconds while the new settings take effect.

8. Use the **Link Trap object** to determine whether to send a trap when link status changes.

   The factory default is enabled.

9. Use **Frame Size** to specify the maximum Ethernet frame size the interface supports or is configured to use , 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** list, select to **Enable** or **Disable** IEEE 802.3 flow control.

    The default is Disable. The switch does not send pause frames if the port buffers become full. Flow control helps to prevent data loss when the port cannot keep up with the number 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 responds 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 the **Apply** button.

The switch is updated with the values you entered. For the switch to retain the new values across a power cycle, you must save the configuration.

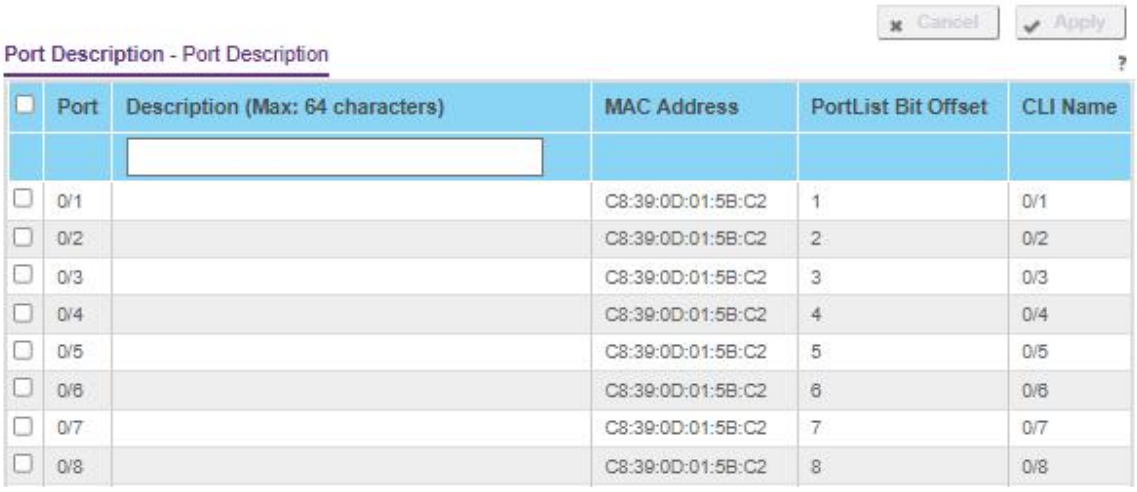
The following table describes the nonconfigurable data that is displayed.

Table43. Port Configuration

Field	Description
Media Type	The media type.
Port Type	For normal ports this field is **Normal**. Otherwise the possible values are as follows: • **Mirrored**. The port is a mirrored port on which all the traffic is 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 as follows: • **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.

3.1.2. Configure Port Descriptions

To configure and display the description for all ports in the device:
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.

The following table describes the nonconfigurable information displayed on the screen.

Table44. Port Description

Field	Description
Port	Selects the interface for which data is to be displayed or configured.
MAC Address	The physical address of the specified interface.
PortList Bit Offset	The bit offset value that corresponds to the port when the MIB object type PortList is used to manage in SNMP.
ifIndex	The interface index associated with the port.

3.1.3. View Port Transceiver Information

You can view the transceiver information for all fiber ports in the box.

To view port transceiver information:
Switching > Ports > Port Transceiver.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following describes the nonconfigurable data that is displayed.

Table45. Port Transceiver

Field	Description
Port	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 62, 5 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.

3.2. 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.

3.2.1. Configure LAG Settings

You can 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 configure LAG settings:
Switching > LAG > LAG Configuration.

1. Use **LAG Name** to enter the name to be assigned to the LAG.

   You can enter any string of up to 15 alphanumeric characters. A valid name must be specified for you to create the LAG.

2. Use **Admin Mode** to select enable or disable.

   When the LAG is disabled, no traffic flows and LACPDUs are dropped, but the links that form the LAG are not 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 L2 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 as follows:

   - **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**.

   When the LAG is enabled, it does not transmit or process received LACPDUs that is, the member ports do not transmit LACPDUs and all the LACPDUs it can receive are dropped. The factory default is Disable.

6. Use **Link Trap** to specify whether to send a trap when the link status changes.

   The factory default is Enable, which causes 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 the **Delete** button 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.

9. Click the **Apply** button.

   The switch is updated with the values you entered. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

Table46. LAG Configuration

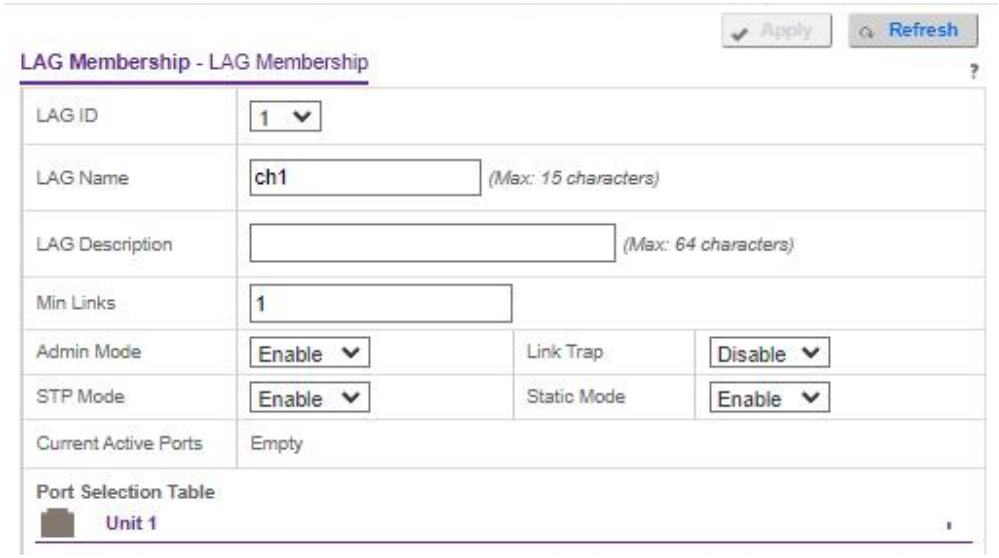
Field	Description

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.

3.2.2. Configure LAG Membership

You can 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 configure LAG membership:
Switching > LAG > LAG Membership.



1. Use **LAG ID** to select the identification of the LAG.
2. Use **LAG Name** to enter the name to be assigned to the LAG.

   You can enter any string of up to 15 alphanumeric characters. A valid name must be specified for you 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**.

   When the LAG is disabled, no traffic flows and LACPDUs are dropped, but the links that form the LAG are not released. The factory default is Enable.
5. Use **Link Trap** to specify whether to send a trap when the link status changes.

   The factory default is Enable, which causes 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 as follows:

   - **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.

   When the LAG is enabled, it does not transmit or process received LACPDUs that is, the member ports do not transmit LACPDUs and all the LACPDUs it can 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 L2 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.

3.3. Configure 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 is assigned 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 can omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet can either reject it or insert a tag using its default VLAN ID. A given port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.

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

3.3.1. Configure Basic VLAN Settings

The internal VLAN is reserved by a port-based routing interface and invisible to the end user. Once these internal VLANs are allocated by the port-based routing interface, they cannot be

assigned to a routing VLAN interface.

To configure internal VLAN settings:
Switching > VLAN > Basic > VLAN Configuration.

1. To reset VLAN settings to their default values, select the **Reset Configuration** check box.

   The factory default values are as follows:

   - 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.

   All VLANs, except for the default VLAN, are deleted.

2. Specify the internal VLAN settings.

   The Internal VLAN Configuration section displays the allocation base and the allocation mode of internal VLAN.

   a. Use **Internal VLAN Allocation Base** to specify the VLAN allocation base for the routing interface.

      The default base range of the internal VLAN is 1 to 4093.

   b. Select the Internal VLAN Allocation Policy **Ascending** or **Descending** radio button.

      This specifies a policy for the internal VLAN allocation.

3. Use **VLAN ID** to specify the VLAN identifier for the new VLAN.

   The range of the VLAN ID is 1 to 4093.

4. Use the optional **VLAN Name** field to specify a name for the VLAN.

   The VLAN name can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always uses the name Default.

   The **VLAN Type** 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 is always Static. A VLAN that is created by GVRP registration initially uses a type of Dynamic. When configuring a dynamic VLAN, you can change its type to Static.

5. Click the **Add** button.

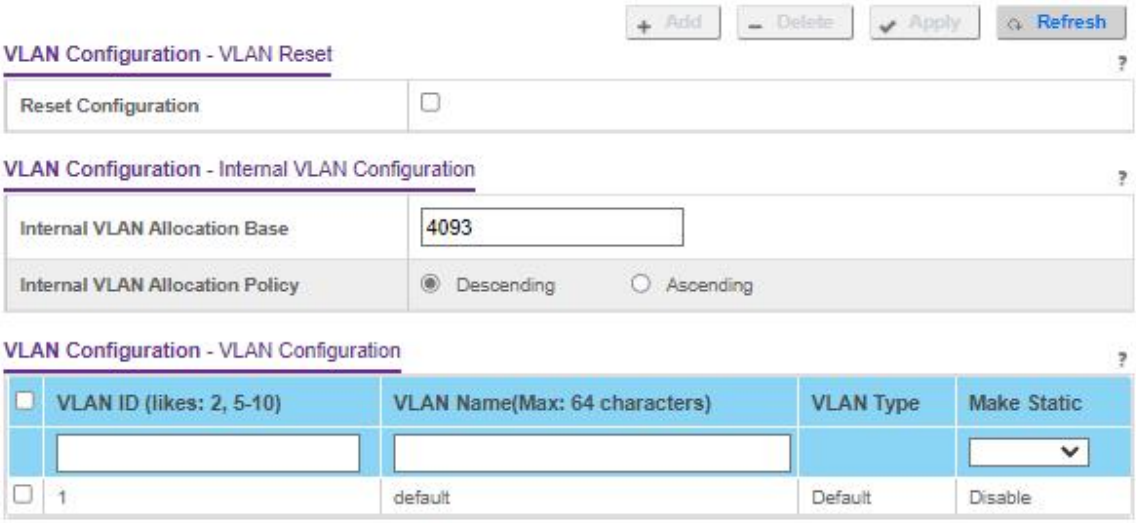
   The VLAN is added to the switch.

6. To delete a selected VLAN from the switch, click the **Delete** button .
7. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

3.3.2. Configure an Advanced VLAN

To configure an advanced VLAN:
Switching > VLAN > Advanced > VLAN Configuration.



1. **Reset Configuration** - If you select this button and confirm your selection on the next screen, all VLAN configuration parameters are reset to their factory default values.

   Also, all VLANs, except for the default VLAN, are deleted. The factory default values are as follows:

   - 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.

3.3.3. Configure an Internal VLAN

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

To configure an internal VLAN:
Switching > VLAN > Advanced > VLAN Configuration.

1. In the **Internal VLAN Allocation Base** field, specify the VLAN allocation base for the routing interface.

   You can enter a value from 1 to 4093.

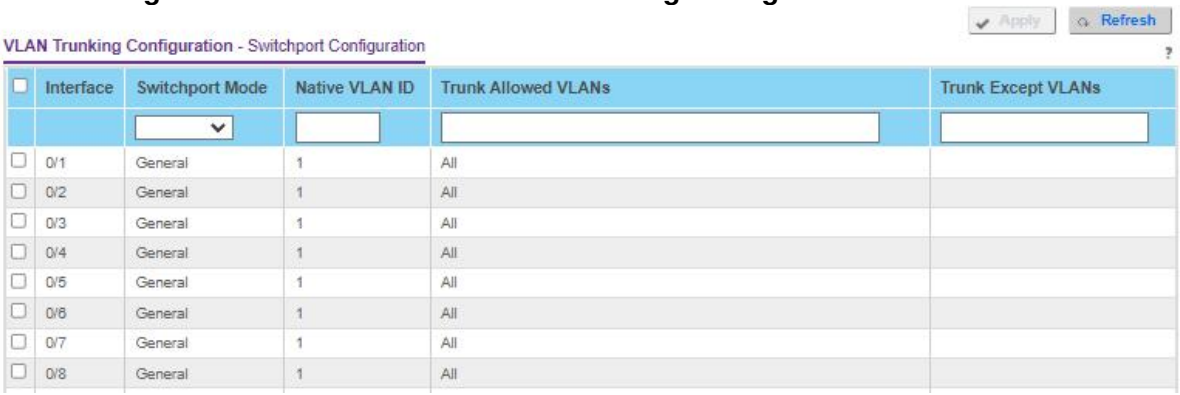
2. Select the Internal VLAN Allocation Policy **Ascending** or **Descending** radio button.

   This specifies a policy for the internal VLAN allocation.

3.3.4. Configure VLAN Trunking

You can configure switchport mode settings on interfaces. The switchport mode defines the purpose of the port based on the type of device it connects to and constraints the VLAN configuration of the port accordingly. Assigning the appropriate switchport mode helps simplify VLAN configuration and minimize errors.

To configure VLAN trunking:
Switching > VLAN > Advanced > VLAN Trunking Configuration.



Interface	Switchport Mode	Native VLAN ID	Trunk Allowed VLANs	Trunk Except VLANs
0/1	General	1	All	
0/2	General	1	All	
0/3	General	1	All	
0/4	General	1	All	
0/5	General	1	All	
0/6	General	1	All	
0/7	General	1	All	
0/8	General	1	All	

1. Select the interface:
   - Select the **Unit ID** field to display physical port information for the selected unit.
   - Use **LAG** to display LAGs only.
   - Use **All** to display all physical ports.
   - Use **Go To Interface** to select an interface by entering its number.
   - Use **Interface** to select the interface for which data is to be displayed or configured.
2. In the **Switchport Mode** list, select one of the following:
   - **Access**. This mode is suitable for ports connected to end stations or end users. Access ports participate in only one VLAN. They accept both tagged and untagged packets, but always transmit untagged packets.
   - **Trunk**. This mode is intended for ports that are connected to other switches. Trunk ports can participate in multiple VLANs and accept both tagged and untagged packets.
   - **General**. This mode enables custom configuration of a port. You configure the general port VLAN attributes, such as membership, PVID, tagging, ingress filter, and so on, using the settings on the Port Configuration screen. By default, all ports are initially configured in **General** mode.
   - **Host**. This mode is used for private VLAN configuration.
   - **Promiscuous**. This mode is used for private VLAN configuration.
3. Select from the list to configure the **Access VLAN ID**.

   This is the access VLAN for the port, and is valid only when the port switchport mode is **Access.**
4. Select from the list to configure the **Native VLAN ID**.

   This is the native VLAN for the port, and is valid only when the port switchport mode is **Trunk.**

5. Configure the **Trunk Allowed VLANs**.

   This is the set of VLANs of which the port can be a member when configured in **Trunk** mode. By default, this list contains all possible VLANs, even if they are not yet created. VLAN IDs are in the range 1 to 4093. Use a hyphen (-) to specify a range, or a comma (,) to separate VLAN IDs in a list. Spaces are not permitted. A zero value clears the allowed VLANs. An **All** value sets all VLANs in the range (1 to 4093).

6. Click the **Apply** button.

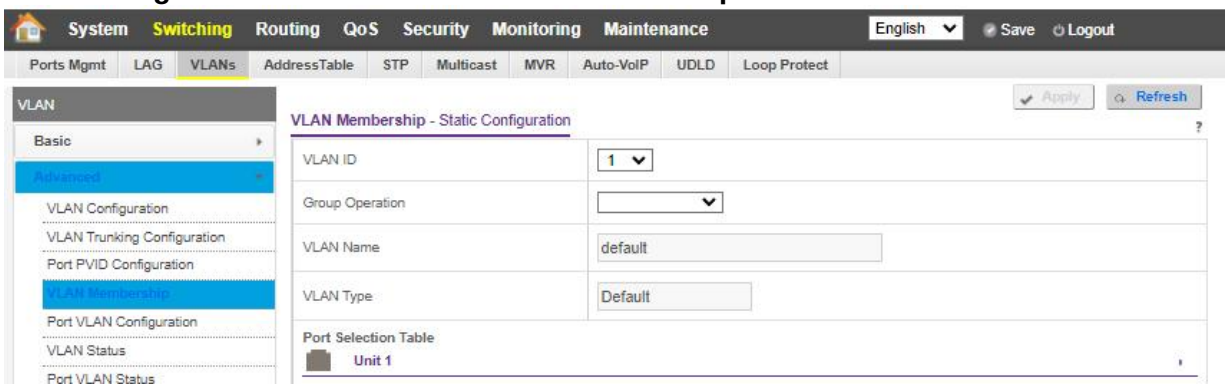
   The updated configuration is sent to the switch.Configuration changes take effect immediately.

The **Native VLAN Tagging** field displays enabled or disabled:

- When VLAN tagging is enabled, if the trunk port receives untagged frames, it forwards them on the native VLAN with no VLAN tag.
- When VLAN tagging is disabled, if the trunk port receives untagged frames, it includes the native VLAN ID in the VLAN tag when forwarding

3.3.5. Configure VLAN Membership

To configure VLAN membership:
Switching > VLAN > Advanced > VLAN Membership.



1. In the **VLAN ID** list, select the VLAN ID.
2. In the **Group Operation** list, select all the ports and configure them:
   - **Untag All**. Select all the ports on which all frames transmitted for this VLAN are untagged. All the ports are included in the VLAN.
   - **Tag All**. Select the ports on which all frames transmitted for this VLAN are tagged. All the ports are included in the VLAN.
   - **Remove All**. All the ports that can be dynamically registered in this VLAN through GVRP. This selection excludes all ports from the selected VLAN.
3. In the **Port** display, select port numbers to add them to this VLAN.

   Each port can use one of three modes:

   - **T (Tagged)**. Select the ports on which all frames transmitted for this VLAN are tagged. The ports that are selected are included in the VLAN.
   - **U (Untagged)**. Select the ports on which all frames transmitted for this VLAN are

untagged. The ports that are selected are included in the VLAN.

- **BLANK (Autodetect)**. Select the ports that can be dynamically registered in this VLAN through GVRP. This selection excludes a port from the selected VLAN.

The following table describes the nonconfigurable information displayed on the screen.

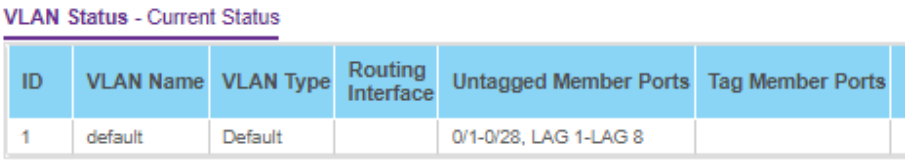
Table47. Advanced VLAN Membership

Field	Definition
VLAN Name	The name for the VLAN that you selected. It can be up to 32 alphanumeric characters long, including blanks. VLAN ID 1 always uses the name Default.
VLAN Type	The type of the VLAN you selected: • **Default** (VLAN ID = 1). Always present • **Static**. A VLAN that you configured • **Dynamic**. A VLAN created by GVRP registration that you did not convert to static, and that GVRP can therefore remove

3.3.6. View VLAN Status

You can view the status of all currently configured VLANs.

To view the VLAN status:
Switching > VLAN > Advanced > VLAN Status.



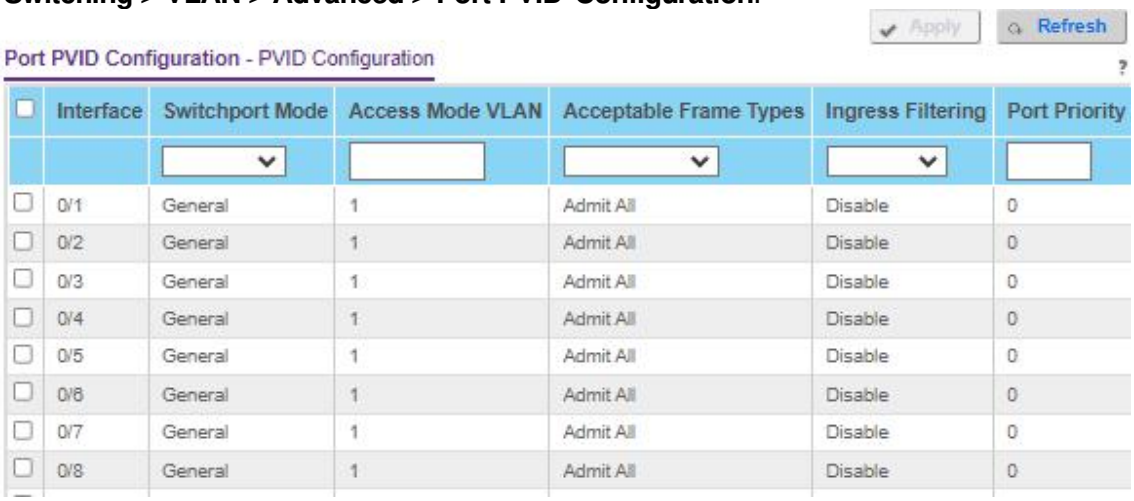
The following table describes the nonconfigurable information displayed on the screen.

Table48. 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 that you configured • **Dynamic**. A VLAN created by GVRP registration that you did not convert to static, and that GVRP can 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.

3.3.7. Configure Port PVID Settings

Switching > **VLAN** > **Advanced** > **Port PVID Configuration**.



Interface	Switchport Mode	Access Mode VLAN	Acceptable Frame Types	Ingress Filtering	Port Priority
0/1	General	1	Admit All	Disable	0
0/2	General	1	Admit All	Disable	0
0/3	General	1	Admit All	Disable	0
0/4	General	1	Admit All	Disable	0
0/5	General	1	Admit All	Disable	0
0/6	General	1	Admit All	Disable	0
0/7	General	1	Admit All	Disable	0
0/8	General	1	Admit All	Disable	0

1. To display information for all physical ports and LAGs, click the **ALL** button.
2. Select the interfaces.

   Select the **Interface** check box next to the interfaces. You can select multiple interfaces. To select all the interfaces, select the **Interface** check box in the heading row.
3. In the **PVID** field, specify the VLAN ID to assign to untagged or priority-tagged frames received on this port.

   The factory default is 1.
4. In the **VLAN Member** field, 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 hyphen (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.
5. In the **VLAN Tag** field, specify the VLAN ID or list of VLANs of a tagged port.

   VLAN IDs range from 1 to 4093. Use a hyphen (-) 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 obe set only if the port is a member of this VLAN.
6. In the **Acceptable Frame Types** list, specify the types of frames that can be received on this port.

   The options are **VLAN only** and **Admit All**:

   - When set to **VLAN only**, untagged frames or priotiry-tagged frames received on this port are discarded.
   - When set to **Admit All**, untagged frames or priotiry-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.
7. In the **Configured Ingress Filtering** field, select **Enabled** or **Disabled**.
   - 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.

8. In the **Port Priority** field, specify the default 802.1p priority assigned to untagged packets arriving at the port.

   You can enter a number from 0 to 7.

3.3.8. Configure a 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.

You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified through a source MAC address and the desired VLAN ID. The MAC to VLAN configurations are shared across all ports of the device (that is, there is a system-wide table with MAC address to VLAN ID mappings).

When untagged or priotiry-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 maintains this value; otherwise, the priority is 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 was not created on the system.

To configure a MAC-based VLAN:
Switching > VLAN > Advanced > MAC Based VLAN.

1. In the **MAC Address** field, type a valid MAC address to be bound to a VLAN ID.

   This field is configurable only when a MAC-based VLAN is created.

2. In the **VLAN ID** field, specify a VLAN ID in the range of 1 to 4093.
3. Click the **Add** button.

   The MAC address is added to the VLAN mapping.

4. To delete a MAC address from VLAN mapping, click the **Delete** button.

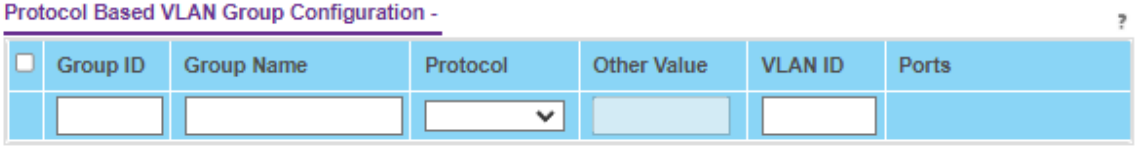
3.3.9. Configure Protocol-Based VLAN Groups

You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure any port-based (IEEE 802.1Q) or protocol-based VLANs, untagged packets are 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 are assigned the protocol-based VLAN ID. Untagged frames received on the port for other protocols are assigned the Port VLAN ID, either the default PVID (1) or a PVID you 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 specify a name and a group ID is assigned automatically.

To configure a protocol-based VLAN group:
Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration.



1. In the **Group Name** field, type a name for the new group.

   You can enter up to 16 characters.

2. In the **Protocol** field, select the protocols to be associated with the group.

   There are three configurable protocols:

   - **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. In the **VLAN ID** field, select the VLAN ID.

   It can be any number in the range of 1 to 4093. All the ports in the group assigns this VLAN ID to untagged packets received for the protocols that you included in this group.

4. Click the **Add** button.

   The protocol-based VLAN group is added to the switch.

5. To remove the protocol-based VLAN group identified by the value in the Group ID field, click the **Delete** button.

The following table describes the nonconfigurable information displayed on the screen.

Table49. Protocol Based VLAN Group

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 that belong to the group.

3.3.10. Configure Protocol-Based VLAN Group Membership

To configure protocol-based VLAN group membership:

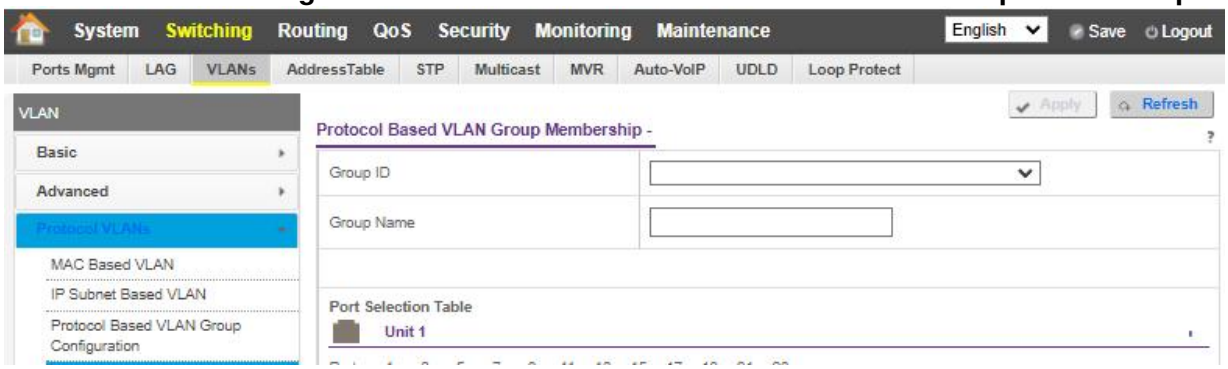
1. Prepare your computer with a static IP address in the 192.168.10.0 subnet, for example, 192.168.10.101.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

   The default IP address of the switch is 192.168.10.12.

   The Login screen displays.
5. Enter the user name and password.

   The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.

   The web management interface menu displays.
7. **Select Switching > VLAN > Advanced > Protocol Based VLAN Group Membership.**



8. In the **Group ID** list, select the protocol-based VLAN group ID.
9. Select port numbers (**1**, **2**, **3**, and so on) to select ports to add to this protocol-based VLAN group.

   An interface can belong to only one group for a given protocol. If you already added a port to a group for IP, you cannot add it to another group that also includes IP, although you can add it to a new group for IPX.

The following table describes the nonconfigurable information displayed on the screen.

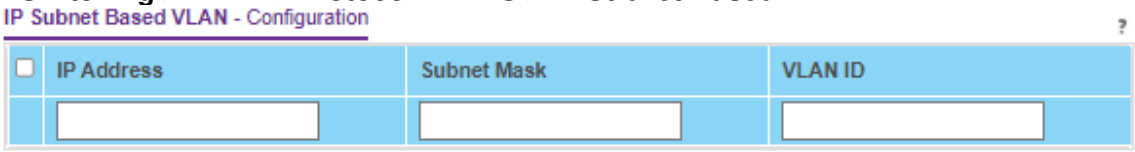
Table50. Protocol-Based VLAN Group Membership

Field	Description
Group Name	This field identifies the name for the protocol-based VLAN that 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.

3.3.11. Configure an 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 through 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 configure IP subnet-based VLAN:
Switching > VLAN > Protocol VLANS > IP Subnet Based VLAN.



1. In the **IP Address** field, specify a valid IP address bound to the VLAN ID.

   Enter the IP address in dotted-decimal notation.

2. In the **Subnet Mask** field, specify a valid subnet mask of the IP address.

   Enter the subnet mask in dotted-decimal notation.

3. In the **VLAN ID** field, specify a VLAN ID in the range of (1 to 4093).
4. Click the **Add** button.

   The IP subnet-based VLAN is added.

5. To delete the selected IP subnet–based VLAN, click the **Delete** button.

3.3.12. Configure a Port DVLAN

To configure a port DVLAN:
Switching > VLAN > 802.1Q TUNNELING > Port DVLAN Configuration.

1. Select **Interface** check boxes to select the physical interface.

   To select all ports, select the Interface check box at the top of the column.

2. In the **Admin Mode** field, select **Enabled** or **Disabled**.

   This specifies the administrative mode through which double VLAN ragging can be enabled or disabled. The default value for this is Disabled.

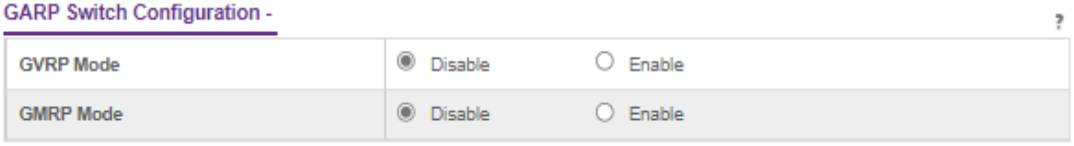
3. In the **Global EtherType** field, specify the first 16 bits of the DVLAN tag.

- **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

3.3.13. Configure GARP Switch Settings

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

To configure GARP switch settings:
Switching > VLAN > Advanced > GARP Switch Configuration.



1. Select the GVRP Mode **Disable** or **Enable** radio button.

   This selects the GARP VLAN registration protocol administrative mode for the switch. The factory default is Disable.

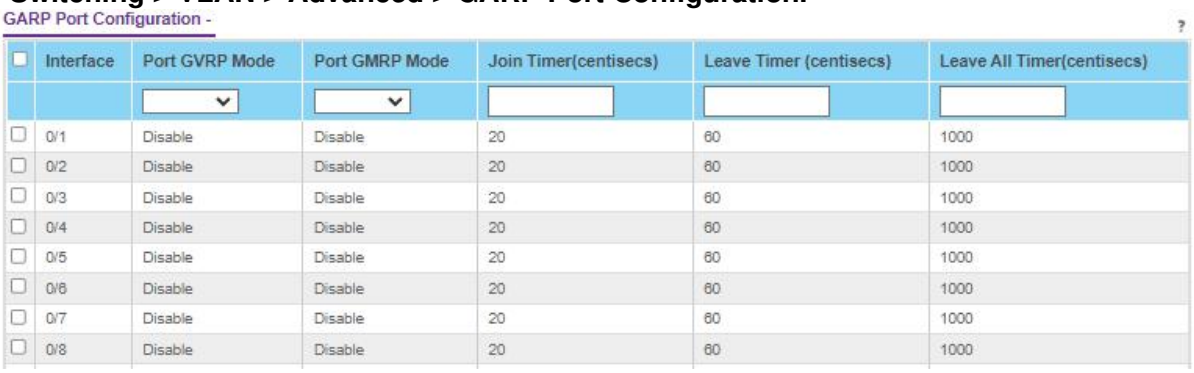
2. Select the GMRP Mode **Disable** or **Enable** radio button.

   This selects the GARP multicast registration protocol administrative mode for the switch. The factory default is Disable.

3.3.14. Configure GARP Port

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

To configure GARP port:
Switching > VLAN > Advanced > GARP Port Configuration.



1. Use **Interface** to select the physical interface for which data is to be displayed or configured.
2. In the **Port GVRP Mode** field, select **Enable** or **Disable**.

This specifies the GARP VLAN registration protocol administrative mode for the port.If you select Disable, the protocol is not active and the join time, leave time, and leave all time have no effect. The factory default is Disable.

3. In the **Port GMRP Mode** field, select **Enable** or **Disable**

   This specifies the GARP multicast registration protocol administrative mode for the port. If you select Disable, the protocol is not active, and the join time, leave time, and leave all time have no effect. The factory default is Disable.

4. In the **Join Time (centiseconds)** field, 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. In the **Leave Time (centiseconds)** field, 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 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.

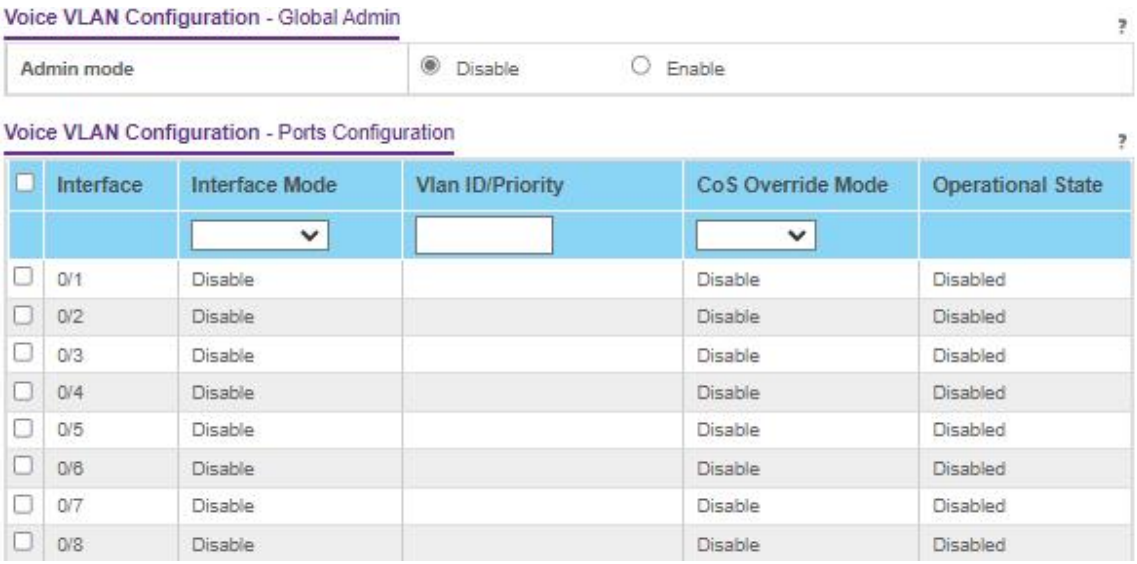
6. Use **Leave All Time (centiseconds)** to control how frequently LeaveAll PDUs are generated.

   A LeaveAll PDU indicates that all registrations will be deregistered soon. To maintain registration, participants must rejoin. 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.

3.3.15. Configure a Voice VLAN

You can configure the parameters for voice VLAN configuration. Only users with read/write access privileges can change the data on this screen.

To configure a voice VLAN:
Switching > VLAN > Advanced > Voice VLAN Configuration.



1. Select the Admin Mode **Disable** or **Enable** radio button.

   This specifies the administrative mode for voice VLAN for the switch. The default is Disable.

2. Use **Interface** to select the physical interface.
3. Use **Interface Mode** to select the voice VLAN mode for selected interface:
   - **Disable**. This is the 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, 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 enabled only when VLAN ID or dot1p is selected as the interface mode.

5. In the **CoS Override Mode** field, select **Disable** or **Enable**.

   The default is Disable.

6. In the **Authentication Mode** field, select **Enable** or **Disable**.

   The default is **Enable**. When the authentication mode is enabled, voice traffic is allowed on an unauthorized voice VLAN port. When the authentication mode is disabled, devices are authorized through dot1x.

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

7. In the **DSCP Value** field, configure the Voice VLAN DSCP value for the port.

   The valid range is 0 to 64. The default value is 0.

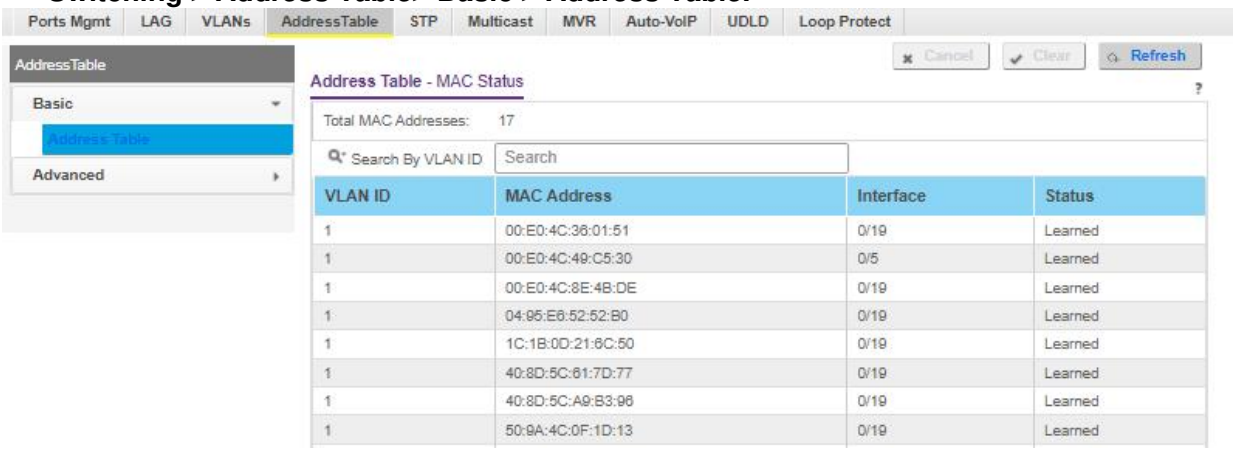
The Operational State field displays the operational status of the voice VLAN on the given interface.

3.3.16. MAC Address Table

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

3.3.17. Configure the MAC Address Table

To configure the MAC Address Table:
Switching > Address Table> Basic > Address Table.



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

The following table describes the nonconfigurable information displayed on the screen.

Table51. Basic Address Table

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 as follows: • 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.

3.3.18. Set the Dynamic Address Aging Interval

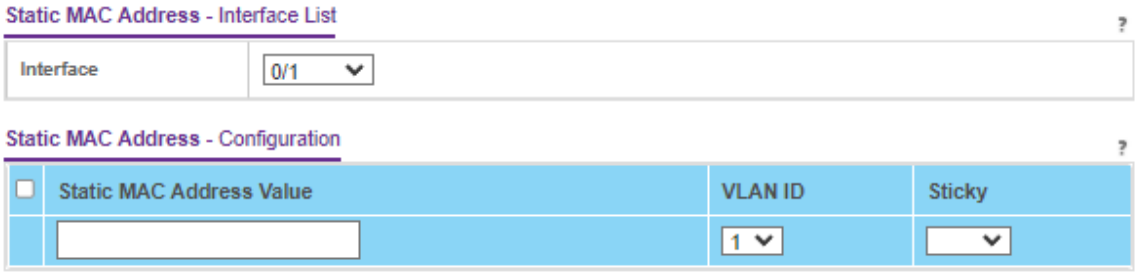
You can set the address aging interval for the specified forwarding database.

To set the address aging interval,
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 can be specified as any number between 10 and 1000000 seconds. The factory default is 300.

3.3.19. Configure a Static MAC Address



1. Use **Interface** to select the physical interface/LAGs.
2. In the **Static MAC Address** field, type the MAC address.
3. Select the **VLAN ID** associated with the MAC address.
4. Click the **Add** button.

   The static MAC address is added to the switch.

To delete a existing static MAC address from the switch, click the **Delete** button.

3.4. 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 *Configure CST Port Settings* on page 236.

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 must be 802.1s and their configuration name, digest key, and revision level must match. For additional information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

3.4.1. Configure Basic STP Settings

To configure STP basic settings:
Switching > STP > Basic > STP Configuration.

STP Configuration - Configuration

Spanning Tree Admin Mode	○ Disable ◉ Enable
Force Protocol Version	○ IEEE 802.1d ◉ IEEE 802.1w ○ IEEE 802.1s
Configuration Name	C8-39-0D-01-5B-C0
Configuration Revision Level	0
BPDU Guard	◉ Disable ○ Enable
BPDU Filter	◉ Disable ○ Enable
Configuration Digest Key	0xac36177f50283cd4b83821d8ab26de62
Fast Backbone	◉ Disable ○ Enable
Fast Uplink	◉ Disable ○ Enable
Max Update Rate	150 *(0 to 32000 packets/second. Default: 150)*

STP Configuration - Status

MST ID	VID	FID
0	1	1

1. Select the Spanning Tree Admin Mode **Disable** or **Enable** radio button.

This specifies whether spanning tree operation is enabled on the switch.

2. Use **Force Protocol Version** to specify the Force Protocol Version parameter for the switch.

   The options are IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, PVST, and RPVST.

3. Use **Configuration Name** to specify an identifier used to identify the configuration currently being used.

   It can 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. Select the Forward BPDU while STP Disabled **Disable** or **Enable** radio button.

   This specifies whether spanning tree BPDUs are forwarded or not while spanning-tree is disabled on the switch.

6. Select the BPDU Guard **Disable** or **Enable** radio button.

   This specifies 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 with STP BPDU guard enabled do not 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. Select the BPDU Filter **Disable** or **Enable** radio button.

   This specifies 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. Select the e **Fast Backbone** Mode **Disable** or **Enable** radio button. (*PVSTP only.*)

   Use this option to choose a new indirect link when an indirect link fails. The system does not ignore inferior BPDUs, as is done in 802.1d. Rather the system uses the BPDUs to age out on the port it received the BPDUs. Later the system sends out root link queries on other non-designated ports. Based on the replies, if there is a positive response to at least one of them, it chooses a new indirect link. Fast Backbone mode is disabled by default.

9. Select the **Fast Uplink** Mode **Disable** or **Enable** radio button. (*PVSTP only.*)

   This option reduces the recovery time in selecting a new root port when the primary root port goes down. Fast Uplink mode is disabled by default.

10. Use the **Max Update Rate** field to configure the Fast Uplink Maximum Update Rate.

    This field is enabled for configuration when Fast Uplink mode is enabled. Allowed values are 0 to 32000 packets per second. The default value is 150.

11. Click the **Apply** button.

    The updated configuration is sent to the switch. Configuration changes take effect immediately.

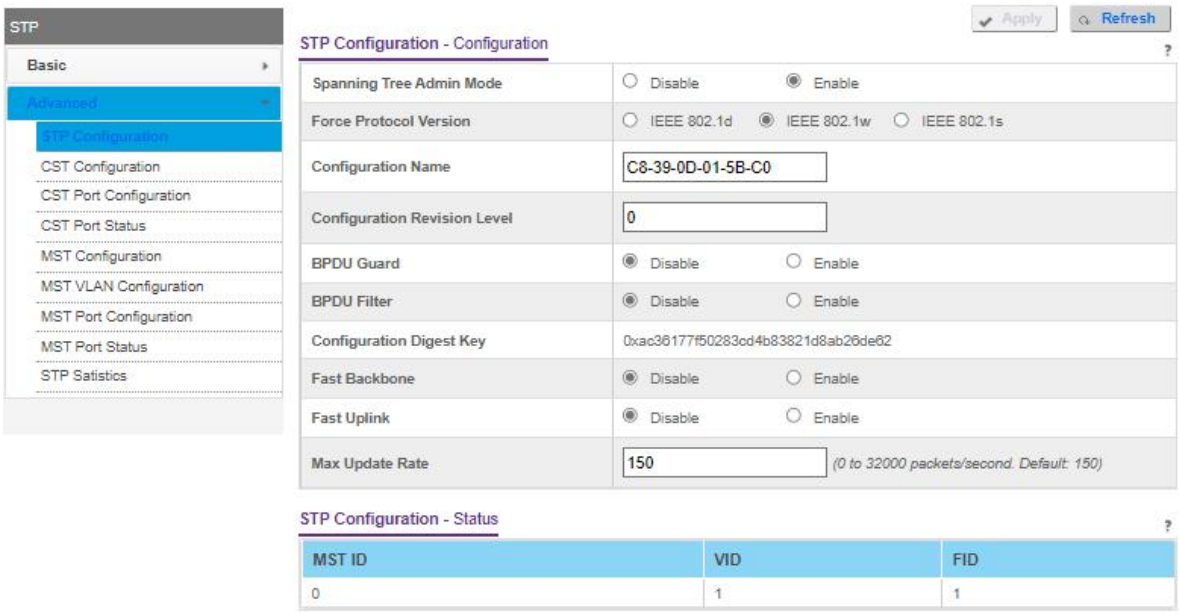
The following table describes the nonconfigurable fields.

Table52. STP Configuration

Field	Description
Configuration Digest Key	Identifier used to identify the configuration currently being used.
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.
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.

3.4.2. Configure Advanced STP Settings

To configure advanced STP settings:
Switching > STP > Advanced > STP Configuration.



1. Select the Admin Mode **Disable** or **Enable** radio button.

   This specifies whether spanning tree operation is enabled on the switch. 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, IEEE 802.1s, PVST, and RPVST. The default is IEEE 802.1w.

3. Use **Configuration Name** to specify the identifier used to identify the configuration currently being used.

   It can 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. Select the Forward BPDU while STP Disabled **Disable** or **Enable** radio button.

   This specifies whether spanning tree BPDUs are forwarded while spanning-tree is disabled on the switch. The default is Disable.

6. Select the BPDU Guard **Disable** or **Enable** radio button.

   This specifies 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 with STP BPDU guard enabled do not 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. Select the BPDU Filter **Disable** or **Enable** radio button.

   This specifies 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. Select the Fast Backbone Mode **Disable** or **Enable** radio button. (*PVSTP only*.)

   Use this option to choose a new indirect link when an indirect link fails. The system does not ignore inferior BPDUs, as is done in 802.1d. Rather the system uses the BPDUs to age out on the port it received the BPDUs. Later the system sends out root link queries on other non-designated ports. Based on the replies, if there is a positive response to at least one of them, it chooses a new indirect link. Fast Backbone mode is disabled by default.

9. Select the Fast Uplink Mode **Disable** or **Enable** radio button. (*PVSTP only*.)

   This option reduces the recovery time in selecting a new root port when the primary root port goes down. Fast Uplink mode is disabled by default.

10. Use the **Max Update Rate** field to configure the Fast Uplink Maximum Update Rate.

    This field is enabled for configuration when Fast Uplink mode is enabled. Allowed values are 0 to 32000 packets per second. The default value is 150.

11. Click the **Apply** button.

    The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

Table53. STP Configuration

Field	Description
Configuration Digest Key	The 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID-to-MST ID mapping) which is used to identify the configuration currently being used.
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.
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.

3.4.3. Configure CST Settings

You can configure Common Spanning Tree (CST) and Internal Spanning Tree on the switch.

To configure CST settings:
Switching > STP > Advanced > CST Configuration.

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 is set to 0. The default priority is 32768.
   - **Bridge Max Age (secs)**. 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)**. 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).** 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**. 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 the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the CST Status information that is displayed.

Table54. STP Advanced CST Configuration

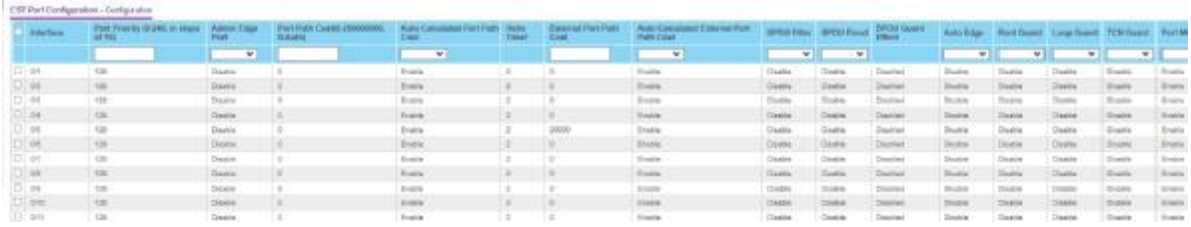
Field	Description
Bridge identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time since topology change	The time in seconds since the topology of the CST last changed.
Topology change count	Number of times topology changed for the CST.
Topology change	The value of the topology change parameter for the switch indicating if a topology change is in progress on any port assigned to the CST. It takes a value if True or False.
Designated root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Path Cost to the Designated Root for the CST.
Root Port Identifier	Port to access the Designated Root for the CST.
Max Age(secs)	Path Cost to the Designated Root for the CST.
Forward Delay(secs)	Derived value of the Root Port Bridge Forward Delay parameter.
Hold Time(secs)	Minimum time between transmission of Configuration BPDUs.
CST Regional Root	Priority and base MAC address of the CST Regional Root.
CST Path Cost	Path Cost to the CST tree Regional Root.

3.4.4. Configure CST Port Settings

You can 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 configure CST port settings:
Switching > STP > Advanced > CST Port Configuration.



1. Select an **Interface**.

   You can select a physical or port channel interface 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 is set to 0. If it is tried to be set to any value between 16

and (2*16-1) it is 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 or 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 the **Apply** button.

    The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable information displayed on the screen.

Table55. CST Port Configuration

Field	Description
Auto Calculated Port Path Cost	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
Hello Timer	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 is 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.

3.4.5. View CST Port Status

You can view the Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

To view the CST port status:
Switching > STP > Advanced > CST Port Status.

To refresh the screen with the latest information on the switch, click the **Update** button.

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

Table56. CST Port Status

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.

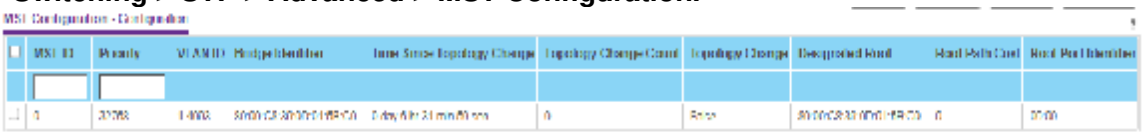
Table57. CST Port Status (continued)

Field	Description
Port Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role is one of the following values: **Root Port**, **Designated Port**, **Alternate Port**, **Backup Port**, **Master Port** or **Disabled Port**.
Designated Root	Root Bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Topology Change Acknowledge	Identifies whether the topology change acknowledgement flag is set for the next BPDU to be transmitted for this port. 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 transitioned into loop inconsistent state.
Transitions Out Of Loop Inconsistent State	The number of times this interface transitioned out of loop inconsistent state.

3.4.6. Configure MST Settings

You can configure Multiple Spanning Tree (MST) on the switch.

To configure an MST instance:
Switching > STP > Advanced > MST Configuration.



1. Configure the MST values:

- **MST ID**. Specify the ID of the MST to create. The valid values for this are 1 to 4094. This is only visible when the select option of the MST ID select box is selected.
- **Priority**. 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 is 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 the **Add** button

   This creates the new MST that you configured.

3. To modify an MST instance:
   a. Select the check box next to the instance (You can select multiple check boxes to apply the same setting to all selected ports.)
   b. Update the values
   c. click the **Apply** button.
4. To delete an MST instance, select the check box for the instance and click the **Delete** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

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

Table58. MST Configuration

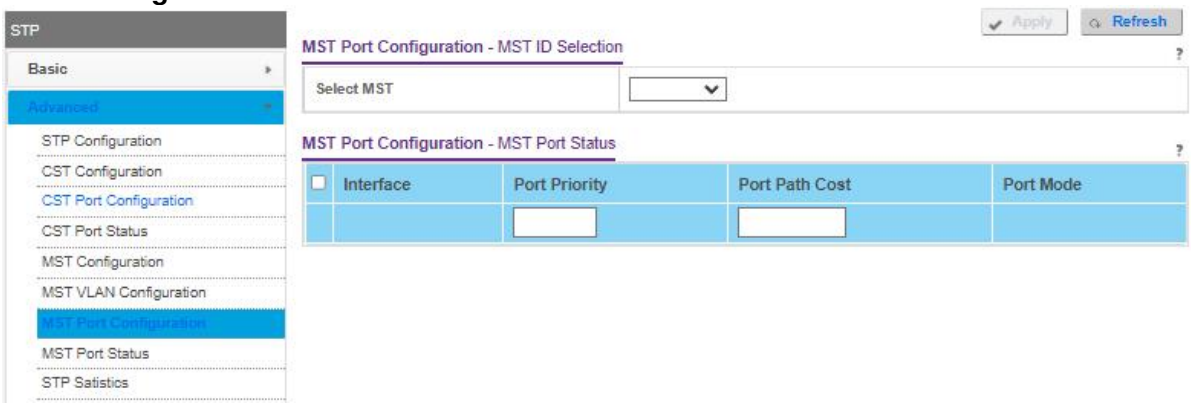
Field	Description
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time n seconds since the topology of the selected MST instance last changed.
Topology Change Count	Number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

3.4.7. View the Spanning Tree MST Port Status

You can 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 view the Spanning Tree MST port status:
Switching > STP > Advanced > MST Port Status.



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

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 is set to 0. If it is tried to be set to any value between 16 and (2*16-1) it is 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 the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

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

Table59. MST Port Status

Field	Description
Auto Calculated Port Path Cost	Displays whether the path cost is automatically calculated (**Enable**) or not (**Disable**). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
Port ID	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port 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 is 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.

3.4.8. View STP Statistics

You can view information about the number and type of bridge protocol data units (BPDUs) transmitted and received on each port.

To view Spanning Tree statistics:
Switching > STP > Advanced > STP Statistics.

STP Satistics - Status

Interface	STP BPDUs Received	STP BPDUs Transmitted	RSTP BPDUs Received	RSTP BPDUs Transmitted	MSTP BPDUs Received	MSTP BPDUs Transmitted
0/1	0	0	0	0	0	0
0/2	0	0	0	0	0	0
0/3	0	0	0	0	0	0
0/4	0	0	0	0	0	0
0/5	0	0	0	11778	0	0
0/6	0	0	0	0	0	0
0/7	0	0	0	0	0	0
0/8	0	0	0	0	0	0

To refresh the screen with the latest information on the switch, click the **Update** button.

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

Table60. STP Statistics

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.

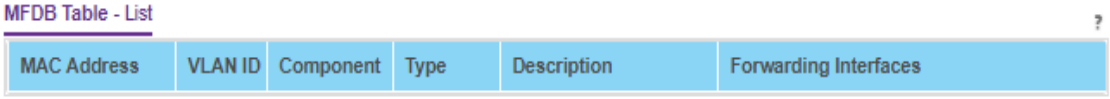
3.5. Multicast

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.

3.5.1. View the 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 can contain data for more than one protocol.

To view the MFDB Table:
Switching > Multicast > MFDB > MFDB Table.



1. Use **Search by MAC Address** to enter a MAC address.

   Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67.

2. Click the **GO** button.

   If the address exists, that entry is displayed. An exact match is required.

Table61. MFDB Table

Field	Description
MAC Address	The multicast MAC address for which you requested data.

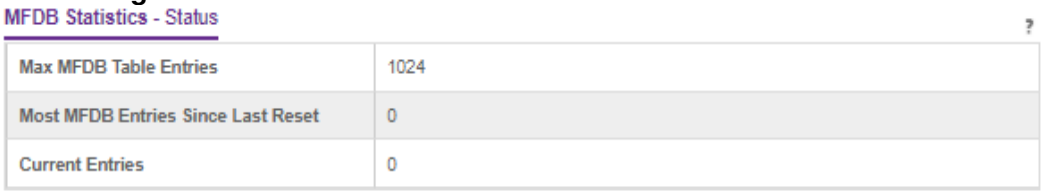
VLAN ID	The VLAN ID to which the multicast MAC address is related.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Component	This is the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP snooping, GMRP, Static Filtering and MLD snooping.

Table62. MFDB Table

Field	Description
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.

3.5.2. View the MFDB Statistics

To view the MFDB statistics:
Switching > Multicast > MFDB > MFDB Statistics.



The following table describes the MFDB Statistics fields.

Table63. 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 were 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.

3.5.3. 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 can 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 forwards 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 are flooded into network segments where no node is receptive to the packet. While nodes rarely incur any processing overhead to filter packets addressed to unrequested group addresses, they cannot 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.

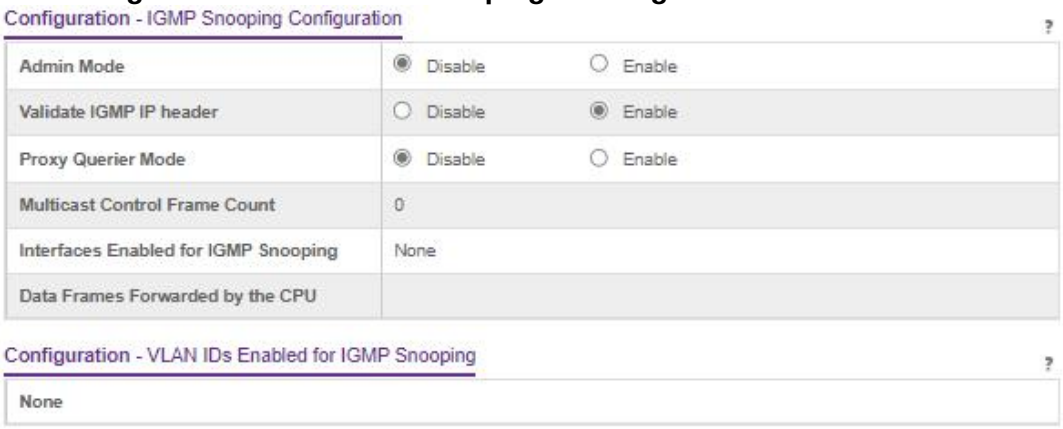
Allowing switches to snoop IGMP packets is a creative effort to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments receive packets directed to the group address.

3.5.4. Configure IGMP Snooping

You can configure the parameters for IGMP snooping, which is used to build forwarding lists for multicast traffic.

Note: You must log in as the admin user, which has read/write access privileges to change the data on this screen.

To configure IGMP snooping:
Switching > Multicast > IGMP Snooping > Configuration.



1. Select the Admin mode **Enable** or **Disable** radio button

   This specifies 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. Select the Proxy Querier Mode **Enable** or **Disable** radio button.

   This enables or disables 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 the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

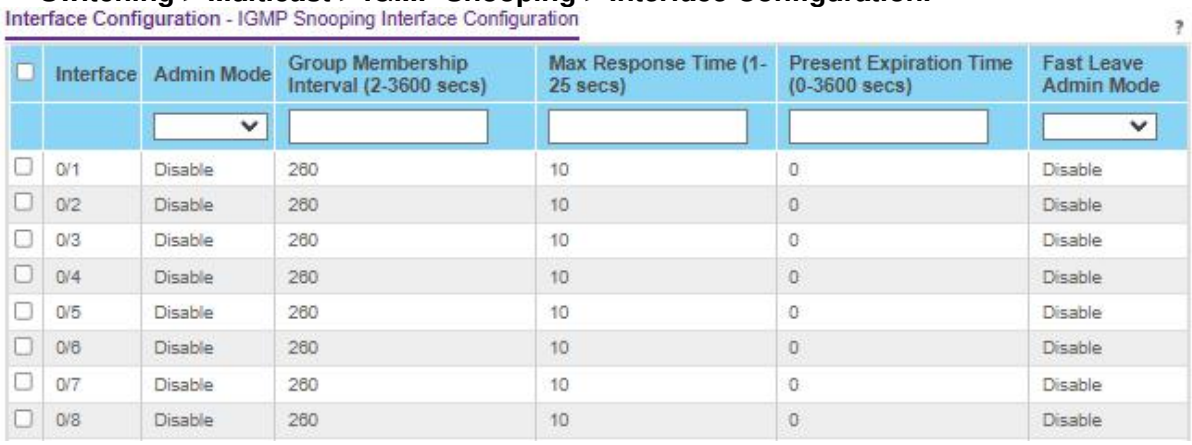
The following table displays information about the global IGMP snooping status and statistics on the screen.

Table64. IGMP Snooping Configuration

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.

3.5.5. Configure IGMP Snooping for Interfaces

To configure IGMP snooping for interfaces:
Switching > Multicast > IGMP Snooping > Interface Configuration.



The screen lists all physical, VLAN, and LAG interfaces.

1. Use the **Interface** check boxes to select interfaces.
2. In the **Admin Mode** field, select **Disable** or **Enable**.

This specifies the interface mode for the selected interface for IGMP snooping for the switch. The default is Disable.

3. Use **Group Membership Interval** to specify the amount of time the switch waits 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 the switch waits 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 the switch waits 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.

   The default is Disable.

7. Use **Proxy Querier Mode** to select the proxy querier mode for a particular interface.

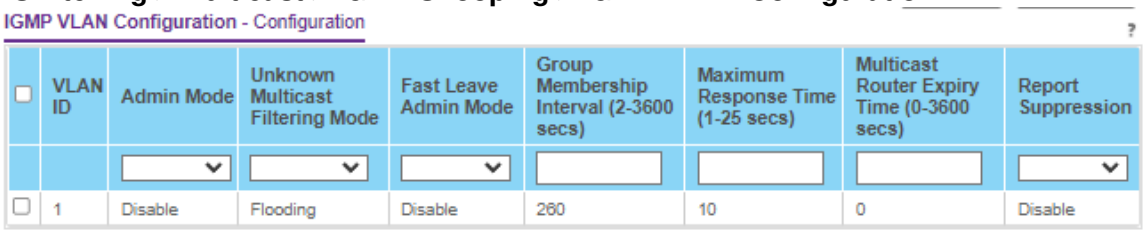
   If it is disabled, then IGMP proxy query with source IP 0.0.0.0 is not sent in response to IGMP leave packet. The default value is Enable.

8. Click the **Apply** button.

   The settings are applied to the switch. Configuration changes take effect immediately.

3.5.6. Configure IGMP Snooping for VLANs

To configure IGMP snooping settings for VLANs:
Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration.



1. To enable IGMP snooping on a VLAN, enter the VLAN ID 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. The 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. The valid range is 1 to Group Membership Interval - 1. Its value must 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. The 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.

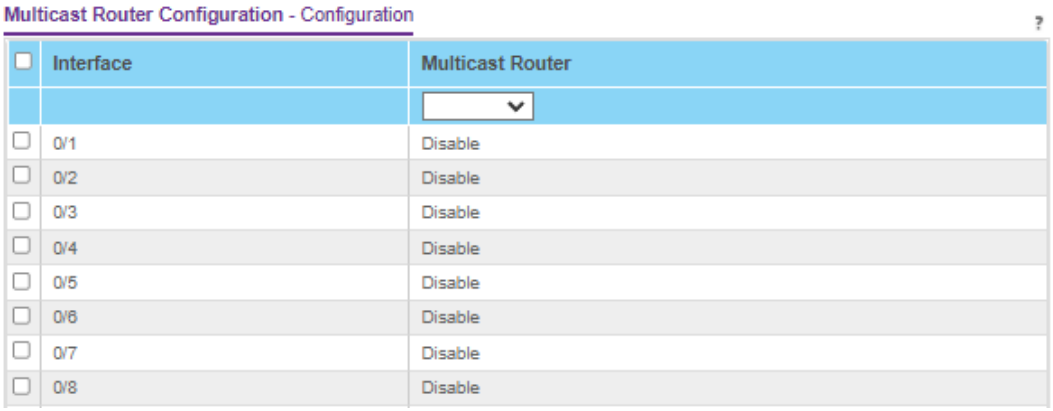
2. To disable IGMP snooping on a VLAN and remove it from the list:
   a. Select the check box next to the VLAN ID
   b. Click the **Delete** button.
3. To modify IGMP snooping settings for a VLAN:
   a. Select the check box next to the VLAN ID
   b. Update the values
   c. Click the **Apply** button.

   The settings are sent to the switch.

3.5.7. Configure a Multicast Router

You can configure the interface as the one the multicast router is attached to. All IGMP packets snooped by the switch are forwarded to the multicast router reachable from this interface. The configuration is not needed most of the time since the switch automatically detects the multicast router and forwards IGMP packets accordingly. It is needed only if you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

To configure a multicast router:
Switching > Multicast > IGMP Snooping > Multicast Router Configuration.



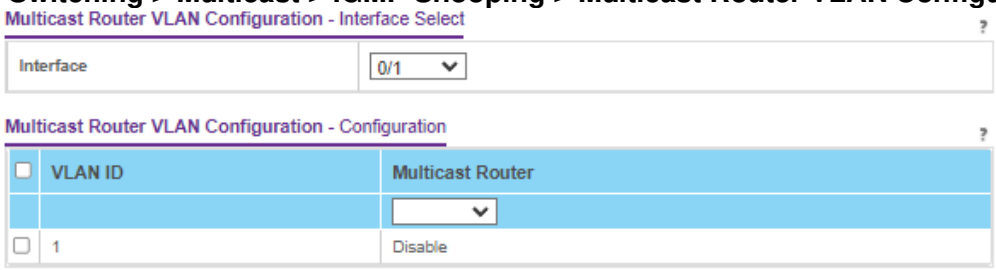
1. Use **Interface** to select the physical interface.
2. In the **Multicast Router** field, select **Enable** or **Disable**.
3. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

3.5.8. Configure a Multicast Router VLAN

You can configure 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 automatically detects a multicast router and forwards the IGMP packets accordingly. It is needed only when you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

To configure a multicast router VLAN:
Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration.



1. Use **Interface** to select the interface.
2. Use **VLAN ID** to select the VLAN ID.
3. In the **Multicast Router** field, select **Enable** or **Disable**.
4. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

3.5.9. IGMP Snooping Querier Overview

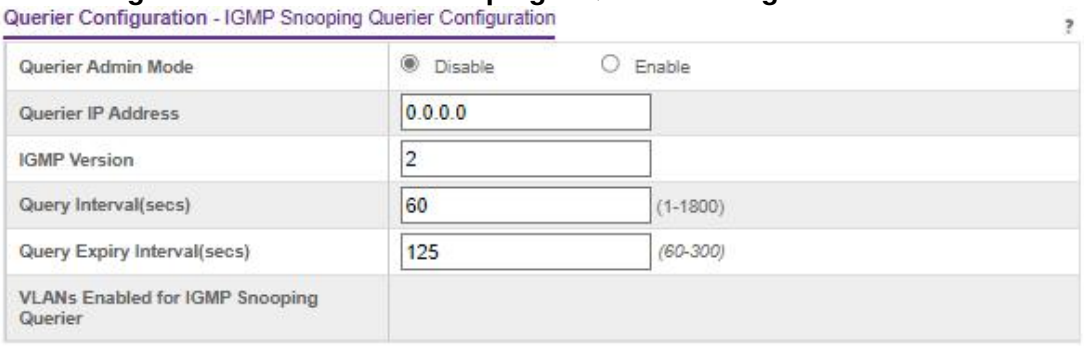
IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP querier. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership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

You can configure and display information on IGMP snooping queriers on the network and, separately, on VLANs.

3.5.10. Configure IGMP Snooping Querier

You can configure the parameters for IGMP snooping querier. Only a user with read/write access privileges can change the data on this screen.

To configure IGMP snooping querier settings:
Switching > Multicast > IGMP Snooping > Querier Configuration.



1. Use **Querier Admin Mode** to select the administrative mode for IGMP snooping for the switch.

   The default is Disable.

2. In the **Snooping Querier IP Address** field, type an IP address.

   This specifies the snooping querier address to be used as the 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 the **Apply** button.

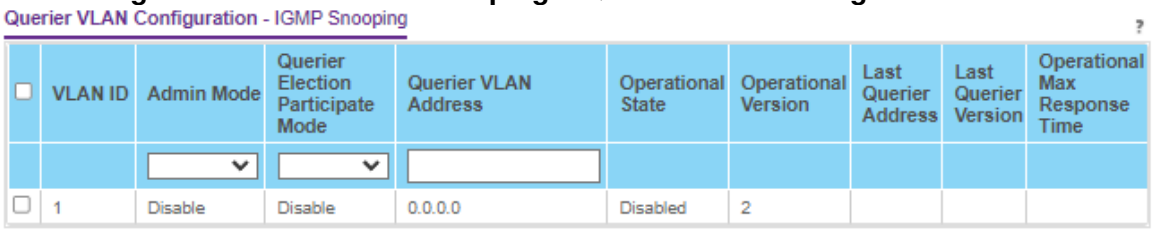
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

   The screen displays the VLAN IDs enabled for IGMP snooping querier.

3.5.11. Configure IGMP Snooping Querier for VLANs

You can configure IGMP queriers for use with VLANs on the network.

To configure querier VLAN settings:
Switching > Multicast > IGMP Snooping > Querier VLAN Configuration.



1. To create a new VLAN ID for IGMP snooping, select **New Entry** from the VLAN ID field and complete the following fields.

   You can also set pre-configurable snooping querier parameters.

   - **VLAN ID**. 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 the **Apply** button.

   The settings are applied to the switch. Configuration changes take effect immediately

3. To disable snooping querier on a VLAN, select the VLAN ID and click the **Delete** button.

The following table describes the nonconfigurable information displayed on the screen.

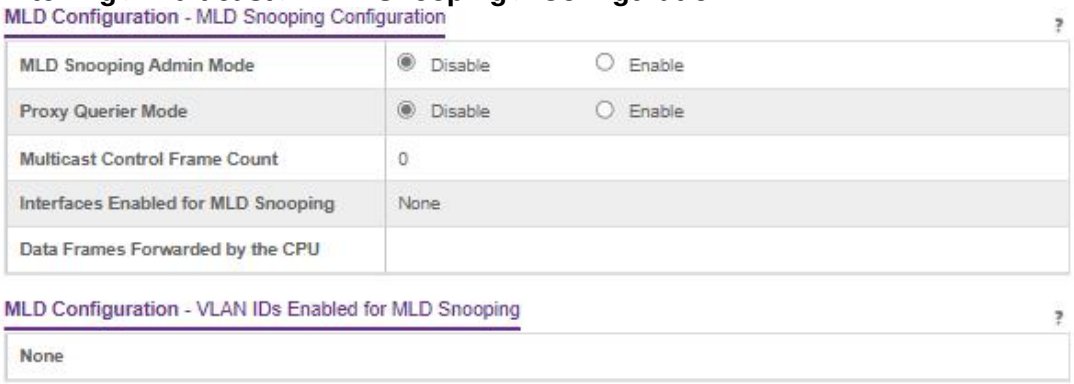
Table65. Querier VLAN Configuration

Field	Description
Operational State	The operational state of the IGMP snooping querier on a VLAN. It can be in any of the following states: • **Querier**: The snooping switch is the querier in the VLAN. The snooping switch sends out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch finds a better querier in the VLAN, it moves to non-querier mode. • **Non-Querier**: The snooping switch is innNon-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. • **Disabled**: The snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when IGMP snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.
Operational Version	The operational IGMP protocol version of the querier.
Last Querier Address	The IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	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.

3.5.12. Configure MLD Snooping

You can configure the parameters for MLD snooping, which is used to build forwarding lists for multicast traffic. Only a user with read/write access privileges can change the data on this screen.

To configure MLD snooping:
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 **Enable** or **Disable** radio button.

   This enables or disables an MLD proxy querier on the system. If it is disabled, then an 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 the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

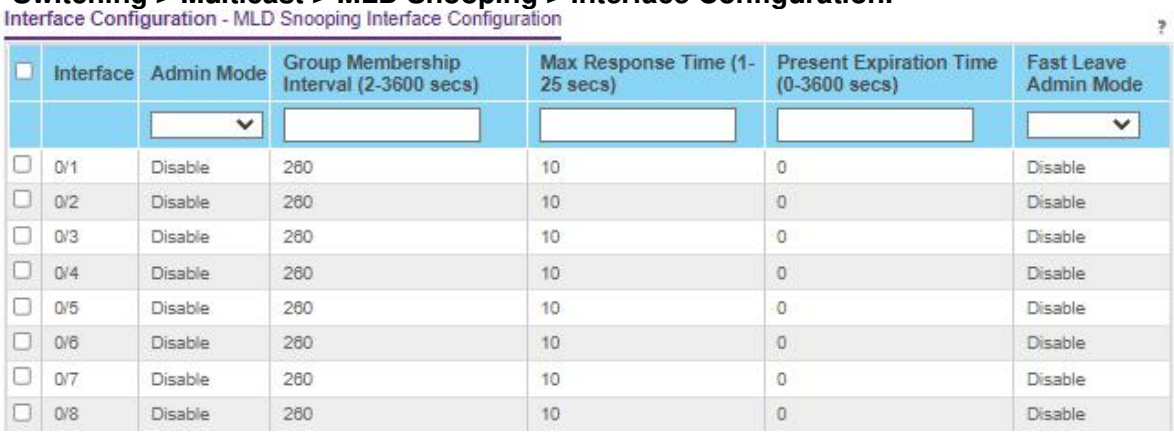
The following table describes the nonconfigurable MLD Snooping Configuration fields.

Table66. 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.

3.5.13. Configure a MLD Snooping Interface

To configure a MLD snooping interface:
Switching > Multicast > MLD Snooping > Interface Configuration.



All physical, VLAN, and LAG interfaces are displayed.

1. Use the **Interface** check boxes to select the interface.
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 the switch waits 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 the switch waits 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 the switch waits to receive a query on an interface before removing it from the list of interfaces with multicast routers attached.

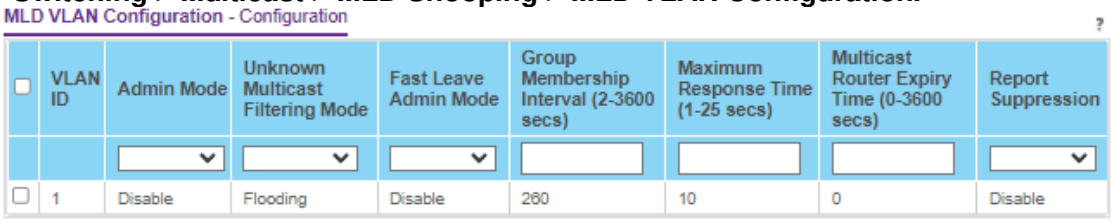
   Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite time-out, that is, no expiration.

6. Use **Fast Leave Admin Mode** to select the fast leave mode for a particular interface. 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 an 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.

3.5.14. Configure MLD VLAN Settings

To configure MLD VLAN settings:
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.

   The valid range is (Maximum Response Time + 1) to 3600.

5. Use **Maximum Response Time** to set the value for the maximum response time of MLD snooping for the specified VLAN ID.

   The valid range is 1 to (Group Membership Interval –1). Its value must be less than group membership interval value.

6. Use **Multicast Router Expiry Time** to set the value for the multicast router expiry time of MLD snooping for the specified VLAN ID.

The valid range is 0 to 3600.

7. Click the **Apply** button.

   The updated configuration is sent to the switch.

3.5.15. Enable or Disable a Multicast Router on an Interface

To enable or disable a multicast router on an interface:
Switching > Multicast > MLD Snooping > Multicast Router Configuration.

Multicast Router Configuration - MLD Configuration

	Interface	Multicast Router
☐	0/1	Disable
☐	0/2	Disable
☐	0/3	Disable
☐	0/4	Disable
☐	0/5	Disable
☐	0/6	Disable
☐	0/7	Disable
☐	0/8	Disable

1. **Interface**: Select the interface.
2. Use **Multicast Router** to enable or disable s multicast router on the selected interface.
3. Click the **Apply** button.

   The updated configuration is sent to the switch.

3.5.16. Configure Multicast Router VLAN Settings

To configure multicast router VLAN settings:
Switching > Multicast > MLD Snooping > Multicast Router VLAN Configuration.

Multicast Router VLAN Configuration - MLD Interface Select

Interface	0/1

Multicast Router VLAN Configuration - MLD Configuration

	VLAN ID	Multicast Router
☐	1	Disable

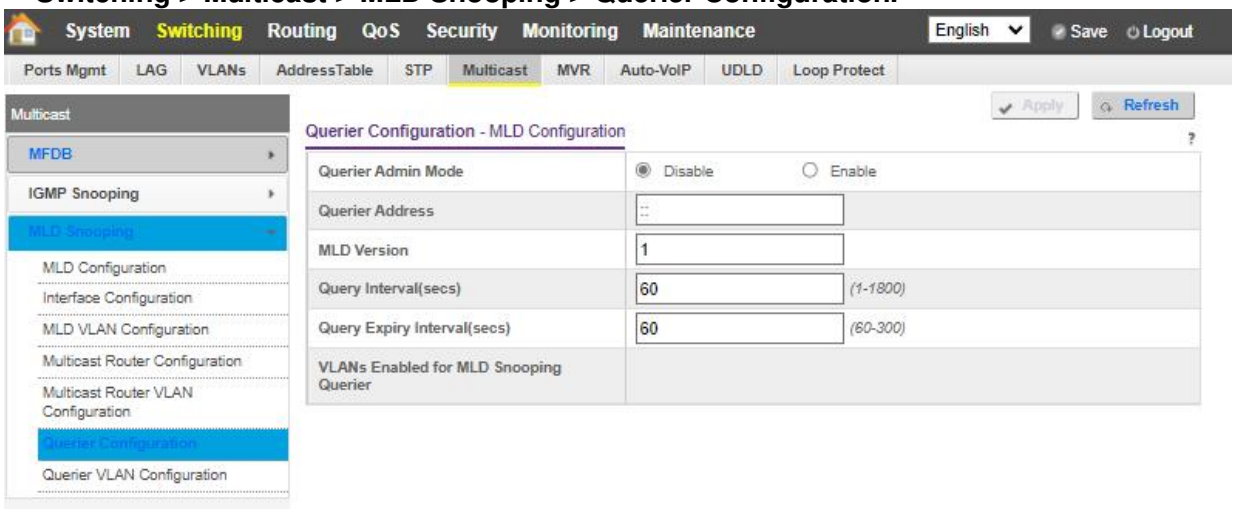
1. Use **Interface** to select the interface.
2. Use **VLAN ID** to select the VLAN ID.
3. Use **Multicast Router** to enable or disable the multicast router for the VLAN ID.
4. Click the **Apply** button.

   The updated configuration is sent to the switch.

3.5.17. Configure MLD Snooping Querier

You can configure the parameters for an MLD snooping querier. Only a user with read/write access privileges can change the data on this screen.

To configure an MLD snooping querier:
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.
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 to 1800. The default value is 60.

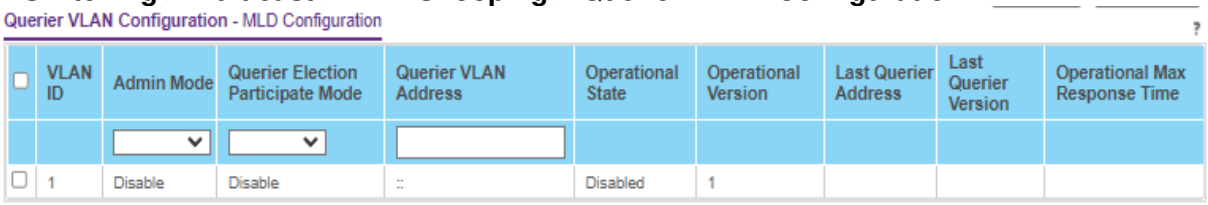
5. Use **Querier Expiry Interval(secs)** to specify the time interval in seconds after which the last querier information is removed.

   The querier expiry Interval must be a value in the range of 60 to 300. The default value is 60.

   The screen displays VLAN IDs enabled for the MLD snooping querier.

3.5.18. Configure MLD Snooping Querier VLAN Settings

To configure MLD snooping querier VLAN settings:
Switching > Multicast > MLD Snooping > Querier VLAN Configuration.



1. Use **VLAN ID** to select the VLAN ID on which the MLD snooping querier is administratively enabled and a VLAN exists in the VLAN database.
2. Use **Querier Election Participate Mode** to enable or disable the MLD snooping querier participation in election mode.

   When this mode is disabled, on detecting another querier of same version in the VLAN, the snooping querier moves to a non-querier state. When this mode is enabled, the snooping querier participates in querier election where the lowest IP address wins 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 the source address in periodic MLD queries sent on the specified VLAN.

The following table describes the nonconfigurable information displayed on the screen.

Table67. Querier VLAN Configuration

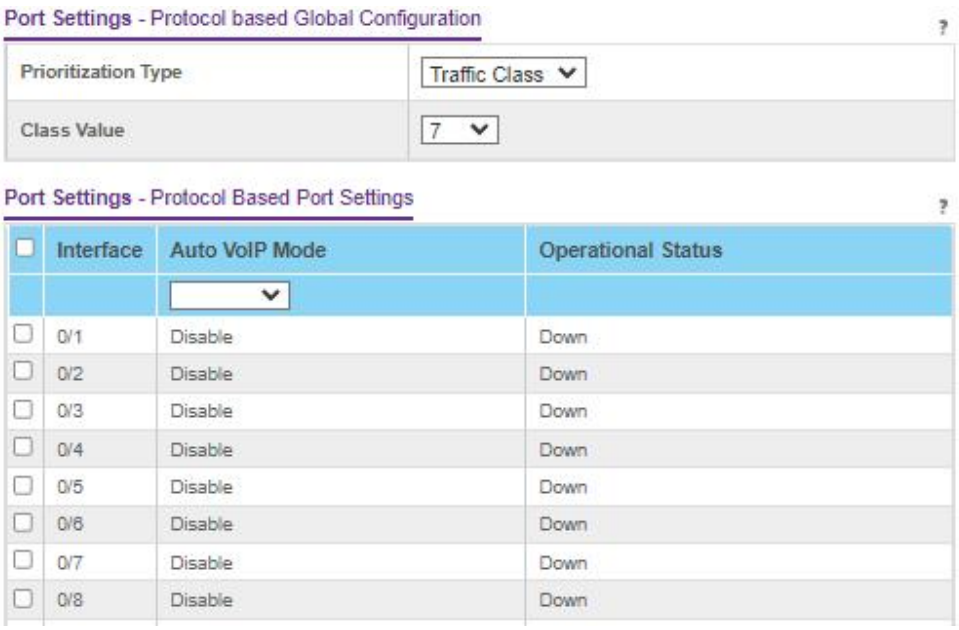
Field	Description
Operational State	The operational state of the MLD snooping querier on a VLAN. It can be in any of the following states: • **Querier**: Snooping switch is the querier in the VLAN. The snooping switch sends out periodic queries with a time interval equal to the configured querier query 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 moves 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	The operational MLD protocol version of the querier.
Last Querier Address	The IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	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.

3.6. Auto-VoIP

You can configure protocol-based port settings and OUI settings.

3.6.1. Configure Protocol-Based Port Settings

To configure protocol-based port settings:
Switching > Auto-VoIP > Protocol-based > Port Settings.



1. In the **Prioritization Type** field, select **Traffic Class** or **Remark**.

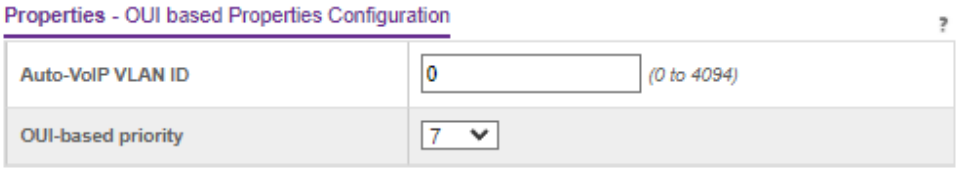
   This specifies the type of prioritization.

2. In the **Class Value** list, specify the CoS tag value to be reassigned for packets received on the voice VLAN when Remark CoS is enabled.
3. Click the **Apply** button.

   The switch is updated with the values you entered. For the switch to retain the new values across a power cycle you must perform a save.

3.6.2. Configure Auto-VoIP OUI-Based Properties

To configure auto-VoIP OUI-based properties:
Switching > Auto-VoIP > OUI-based> Properties.



1. In the **VoIP VLAN ID** field, type the VoIP VLAN ID of the switch.

   There is no default VLAN for auto-VoIP, you must create a VLAN for it first.

2. In the **OUI-based priority** list, select the OUI-based priority of the switch.

   The default value is 7.

3. Click the **Apply** button.

   The switch is updated with the values you entered. For the switch to retain the new values across a power cycle, you must perform a save.

3.6.3. OUI-Based Port Settings

To configure auto-VoIP OUI-based port settings:
Switching > Auto-VoIP > OUI-based > Port Settings.

The Operational Status field displays the current operational status of each interface.

1. Use **Interface** check boxes to select the interfaces.
2. In the **Auto VoIP Mode** field, select **Disable** or **Enable**.

   Auto-VoIP is disabled by default.

3. Use **Go To Interface** to select an interface by entering its number.
4. Click the **Apply** button.

   The switch is updated with the values you entered. For the switch to retain the new values across a power cycle, you must perform a save.

3.6.4. Configure the OUI Table

To configure the OUI Table:
Switching > Auto-VoIP > OUI-based > OUI Table.

OUI Table - Configuration

	Telephony OUI (xx:xx:xx)	Description (0-32 characters)
☐	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
☐	00:04:13	SNOM

1. In the **Telephony OUI(s)** field, specify the VoIP OUI prefix to be added in the format AA:BB:CC.

   Up to 128 OUIs can be configured.

2. In the **Description** field, enter the description for the OUI.

   The maximum length of description is 32 characters. 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

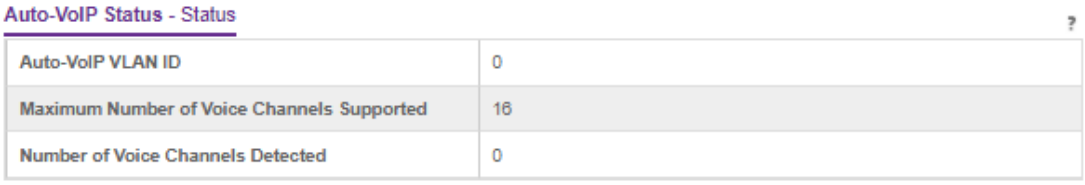
3. Click the **Add** button.

   The telephony OUI entry is added.

4. To delete a created entry, click the **Delete** button.

3.6.5. View the Auto-VoIP Status

To view the auto-VoIP status:
Switching > Auto-VoIP > Auto-VoIP Status



To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable Auto-VoIP status information.

Table68. Auto-VoIP Status

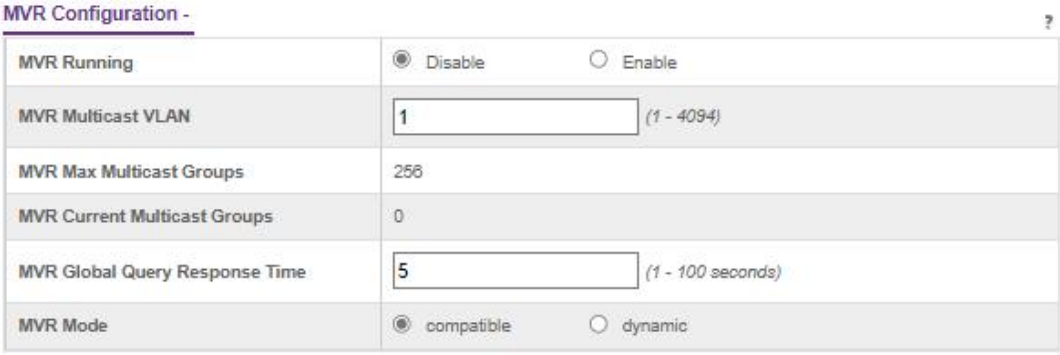
Field	Description
Auto-VoIP VLAN ID	The auto-VoIP VLAN ID.
Maximum Number of Voice Channels Supported	The maximum number of voice channels supported.
Number of Voice Channels Detected	The number of VoIP channels prioritized successfully.

3.7. Configure MVR

You can configure basic, advanced, group, interface or group membership settings.

3.7.1. Configure Basic MVR Settings

To configure basic MVR settings:
Switching > MVR > Basic > MVR Configuration.



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 is 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.

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 a 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 the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

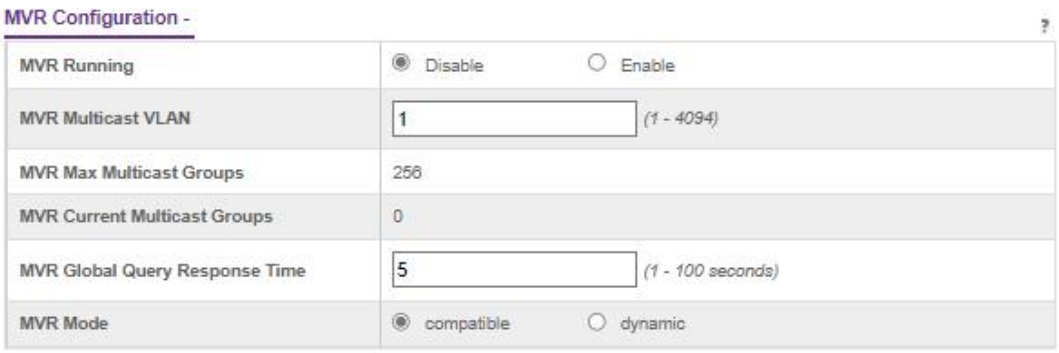
The following table describes the nonconfigurable information displayed on the screen.

Table69. MVR Configuration

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

3.7.2. Configure Advanced MVR Settings

To configure advanced MVR settings:
Switching > MVR > Advanced > MVR Configuration.



1. Select the MVR Running **Enable** or **Disable** radio button.

   The factory default is Disable.

2. Use the **MVR Multicast VLAN** to specify the VLAN on which MVR multicast data is 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. Select a **MVR Mode** radio button to specify the MVR mode of operation.

   The factory default is compatible.

5. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

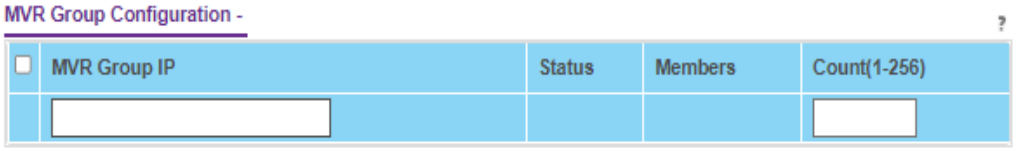
The following table describes the nonconfigurable information displayed on the screen.

Table70. Advanced MVR Configuration

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

3.7.3. Configure an MVR Group

To configure an MVR group:
Switching > MVR > Advanced > MVR Group Configuration.



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.

   This helps you to create multiple MVR groups through a single click of the **Add** button. If the field is empty, then clicking 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 the **Add** button.

   The MVR group is added.
4. T delete a selected MVR group, click the **Delete** button.

The following table describes the nonconfigurable information displayed on the screen.

Table71. MVR Group Configuration

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

3.7.4. Configure an MVR Interface

To configure an MVR interface:
Switching > MVR > Advanced > MVR Interface Configuration.

The status of each port displays.

1. Use **Interface** to select the interface.
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 the MVR on a port.

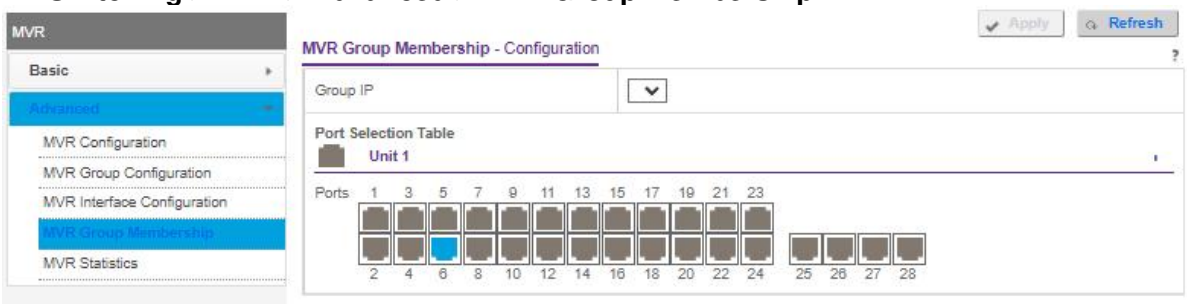
   The factory default is **Disable**.
5. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

3.7.5. Configure MVR Group Membership

To configure MVR group membership:
Switching > MVR > Advanced > MVR Group Membership.



1. Use the **Group IP** to specify the IP multicast address of the MVR group.
2. Use the **Port List** to view the configured list of members of the selected MVR group.

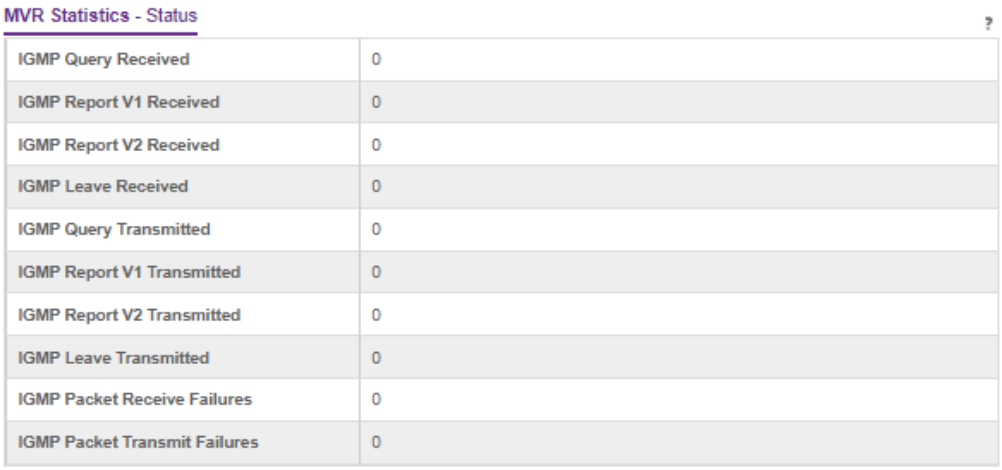
   You can use this port list to add the ports you selected to this MVR group.

3. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

3.7.6. View MVR Statistics

To view MVR statistics:
Switching > MVR > Advanced > MVR Statistics.



To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable information displayed on the screen.

Table72. MVR Statistics

Field	Definition
IGMP Query Received	The number of received IGMP queries.
IGMP Report V1 Received	The number of received IGMP reports V1.
IGMP Report V2 Received	The number of received IGMP reports V2.
IGMP Leave Received	The number of received IGMP leaves.
IGMP Query Transmitted	The number of transmitted IGMP queries.
IGMP Report V1 Transmitted	The number of transmitted IGMP reports V1.
IGMP Report V2 Transmitted	The number of transmitted IGMP reports V2.
IGMP Leave Transmitted	The number of transmitted IGMP leaves.
IGMP Packet Receive Failures	The number of IGMP packet receive failures.
IGMP Packet Transmit Failures	The number of IGMP packet transmit failures.

4. Configure Quality of Service

This chapter covers the following topics:

- *QoS Overview*
- *Class of Service*
- *Differentiated Services Overview*

4.1. QoS Overview

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 cannot be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets with 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 that is not QoS capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

4.2. 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.

Use CoS 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 is forwarded on the appropriate egress ports. 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 cannot be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

4.2.1. Configure Global CoS Settings

To configure global CoS settings:

QoS > Basic > CoS Configuration.

Note: You can also navigate to this screen by selecting **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 be one of the following:

   - untrusted
   - trust dot1p
   - trust ip-dscp

   The default value is trust dot1p.

4. Use **Interface Trust Mode** to specify whether to trust a particular packet marking at ingress.

   Interface Trust mode can be one of the following:

   - untrusted
   - trust dot1p
   - trust ip-dscp

   The default value is untrusted.

5. Click the **Apply** button.

   The updated configuration is sent to the switch.

4.2.2. Map 802.1p Priorities to Queues

The 802.1p to Queue Mapping screen also displays the Current 802.1p Priority Mapping table.

To map 802.1p priorities to queues:

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

1. Use **Interface** to select interfaces.

   You can specify CoS configuration settings per-interface or for 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 list 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 the **Apply** button.

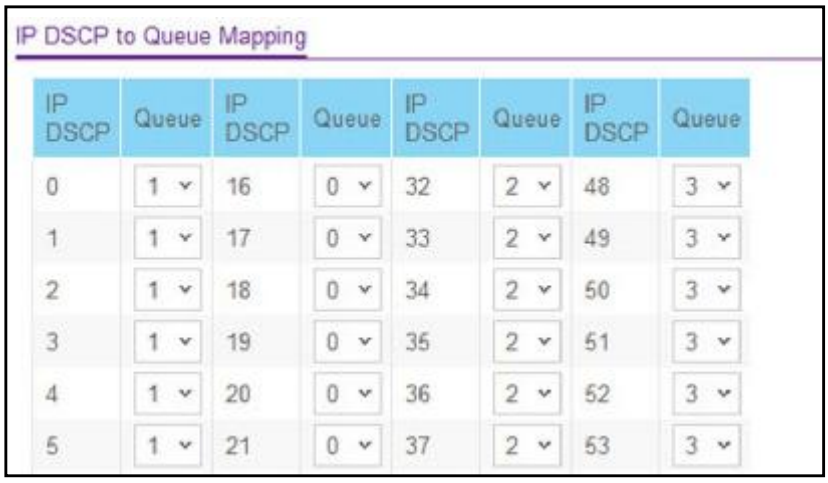
   The updated configuration is sent to the switch.

4.2.3. Map DSCP Values to Queues

You can specify which internal traffic class to map the corresponding DSCP value.

To map DSCP values to queues:

QoS > **CoS** > **Advanced** > **IP DSCP to Queue Mapping**.



The **IP DSCP** field displays an IP DSCP value from 0 to 63.

1. For each DSCP value, specify which internal traffic class to map the corresponding IP DSCP value.

   The queue number depends on specific hardware.

2. Click the **Apply** button.

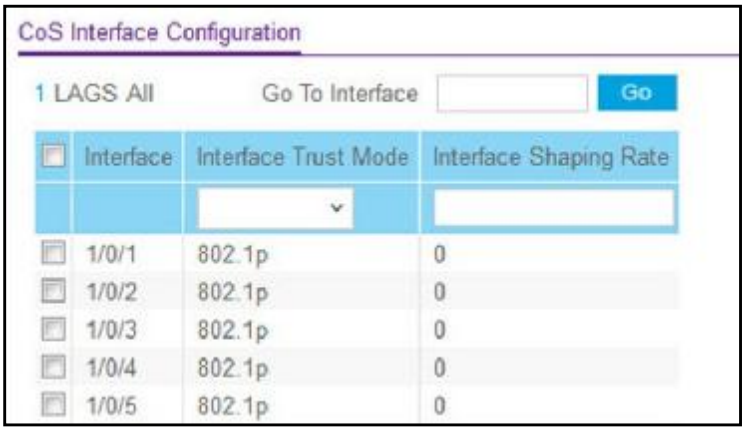
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

4.2.4. Configure CoS Interface Settings for an Interface

You can apply an interface shaping rate to all interfaces or to a specific interface.

To configure CoS settings for an interface:

QoS > CoS> Advanced > CoS Interface Configuration.



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 the **Go**

button.

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 be one of the following:

   - Untrusted
   - 802.1p
   - IP DSCP

   The default value is 802.1p.

6. Use **Interface Shaping Rate** to specify the maximum bandwidth allowed.

   This is 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. The default value is 0. Valid Range is 0 to 100 in increments of 1. The value 0 means that the maximum is unlimited.

7. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

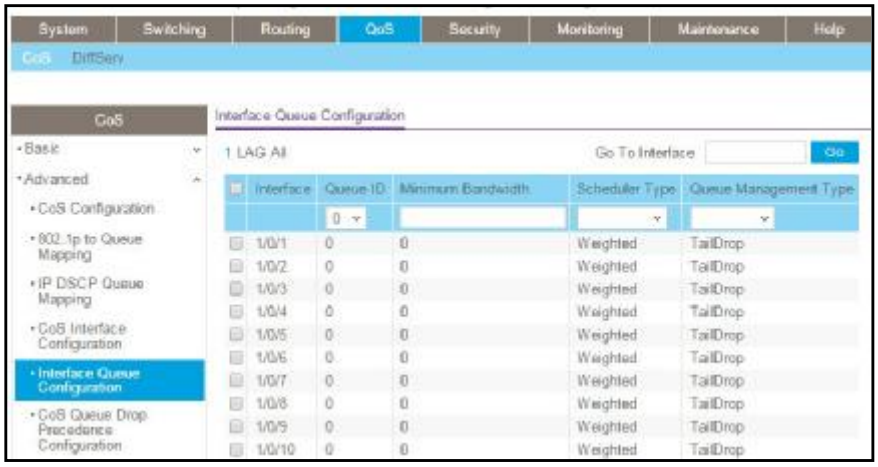
4.2.5. Configure CoS Queue Settings for an Interface

You can 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 configure CoS queue settings for an interface:

QoS > CoS >Advanced > Interface Queue Configuration.



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. The 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 used only if the device supports independent settings per queue. From the Queue Management Type menu, select either **TailDrop** or **WRED**. The default value is **TailDrop**.

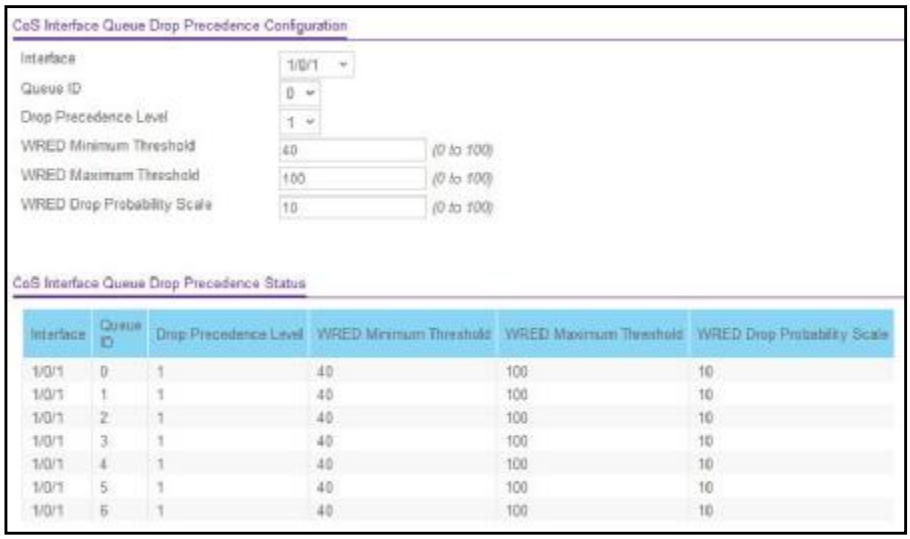
5. Click the **Apply** button.

   Your changes are applied to the system.

4.2.6. Configure CoS Drop Precedence Settings

To configure CoS Drop Precedence settings:

QoS > CoS> Advanced > CoS Queue Drop Precedence Configuration.



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 the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable data that is displayed.

Table73. CoS Interface Queue Drop Precedence Status

Field	Description
Interface	The CoS configurable interface.
Queue ID	The queue ID.

Table 198. CoS Interface Queue Drop Precedence Status (continued)

Field	Description
Drop Precedence Level	The drop precedence level.
WRED Minimum Threshold	The weighted RED minimum queue threshold value.
WRED Maximum Threshold	The weighted RED maximum queue threshold value.
WRED Drop Probability Scale	The packet drop probability value.

4.3. Differentiated Services Overview

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. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email 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.

To use DiffServ for QoS, you must first 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 are defined by a class. The processing is defined by a policy's attributes. Policy attributes can 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.

4.3.1. DiffServ Wizard Overview

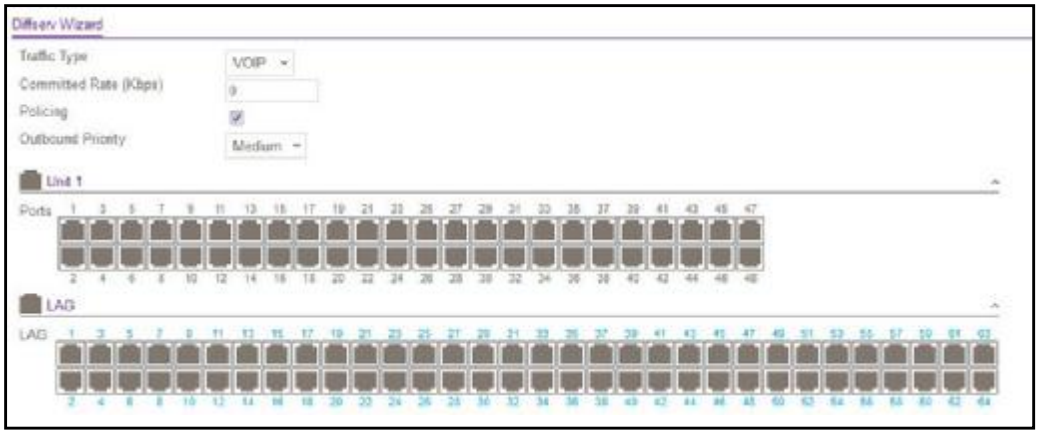
The DiffServ Wizard enables DiffServ on the switch by creating a traffic class, adding the traffic class to a policy, and then adding the policy to the ports that you select. The DiffServ Wizard does the following:

- Creates a **DiffServ Class** and defines match criteria used as a filter to determine if incoming traffic meets the requirements to be a member of the class.
- Sets the **DiffServ Class** match criteria based on **Traffic Type** selection as follows:
  - **VOIP**. Sets the match criteria to UDP protocol.
  - **HTTP**. Sets the match criteria to HTTP destination port.
  - **FTP**. Sets match criteria to FTP destination port.
  - **Telnet**. Sets the match criteria to Telnet destination port.
  - **Every**. Sets the match criteria for 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 is processed according to the **Outbound Priority** selection. **Outbound Priority** configures the handling of conforming traffic as below:
  - **High**. Sets the policing action to markdscp ef.
  - **Med**. Sets the policing action to markdscp af31.
  - **Low**. Sets the policing action to send.
- If **Policing** is set to **NO**, then all traffic is marked as follows:
  - **High**. Sets the policy mark to ipdscp ef.
  - **Med**. Sets the policy mark to ipdscp af31.
  - **Low**. Sets the policy mark ito pdscp be.
- Each port selected is added to the policy created.

4.3.2. Use the DiffServ Wizard

To use the DiffServ Wizard:

QoS > DiffServ > DiffServ Wizard.



1. Use **Traffic Type** to define the **DiffServ Class**.

   Traffic type options are: **VOIP**, **HTTP**, **FTP**, **Telnet**, and **Every**.

2. Ports displays the ports which can be configured to support a **DiffServ** policy.

   The **DiffServ** policy is added to selected ports.

3. Use **Enable Policing** to add policing to the **DiffServ p**olicy.

   The policing rate to be applied.

4. Specify the Committed Rate:
   - When **Policing** is enabled, the committed rate is 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. Specify the Outbound Priority:
   - When **Policing** is enabled, **Outbound Priority** defines the type of policing conform action where: **High** sets action to markdscp ef, **Med** sets the action to markdscp af31, and **Low** sets the action to send.
   - When **Policing** is disabled, **Outbound Priority** defines the policy where: **High** sets the policy to mark ipdscp ef, **Med** sets policy to mark ipdscp af31, and **Low** sets the policy to mark ipdscp be.

4.3.3. Configure Basic DiffServ Settings

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 can be defined on a per–class instance basis, and it is these attributes that are applied when a match occurs.

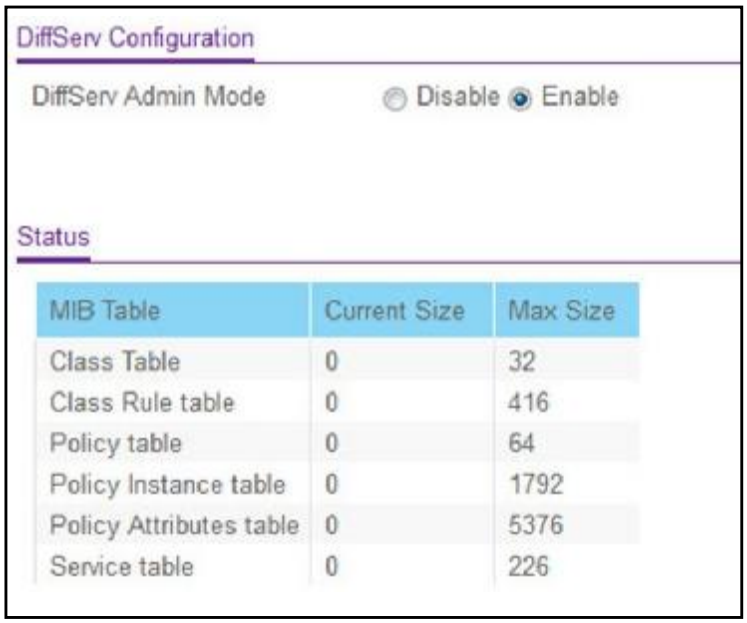
The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.

Packet processing begins by testing the match criteria for a packet. The all class type option specifies that each match criteria within a class must evaluate to true for a packet to match that class. The *any* class type option specifies 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 configure basic DiffServ settings:

QoS > DiffServ > Basic > DiffServ Configuration.



The following table describes the nonconfigurable data that is displayed.

Table74. 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	The number of configured DiffServ classes out of the total allowed on the switch.
Class Rule table	The number of configured class rules out of the total allowed on the switch.
Policy table	The number of configured policies out of the total allowed on the switch.
Policy Instance table	The number of configured policy class instances out of the total allowed on the switch.
Policy Attributes table	The number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
Service table	The number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

4.3.4. Configure the Global DiffServ Settings

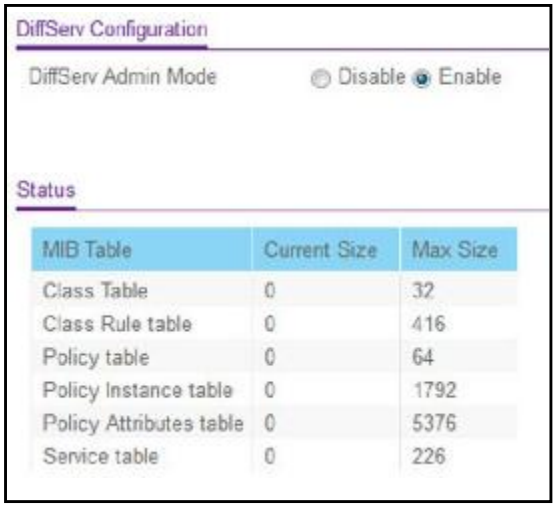
Packets are filtered and processed based on defined criteria. The filtering criteria are defined by a class. The processing is defined by a policy's attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.

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 specifies that each match criteria within a class must evaluate to true for a packet to match that class. The *any* class type option specifies 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 configure the global DiffServ mode:

QoS > DiffServ > Advanced > Diffserv Configuration.



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 the **Apply** button.

   Your settings are applied to the system.

The following table describes the information displayed in the Status table on the DiffServ Configuration screen.

Table75. DiffServ Status

Field	Description
Class Table	The number of configured DiffServ classes out of the total allowed on the switch.

Class Rule table	The number of configured class rules out of the total allowed on the switch.
Policy table	The number of configured policies out of the total allowed on the switch.

Table76. DiffServ Status (continued)

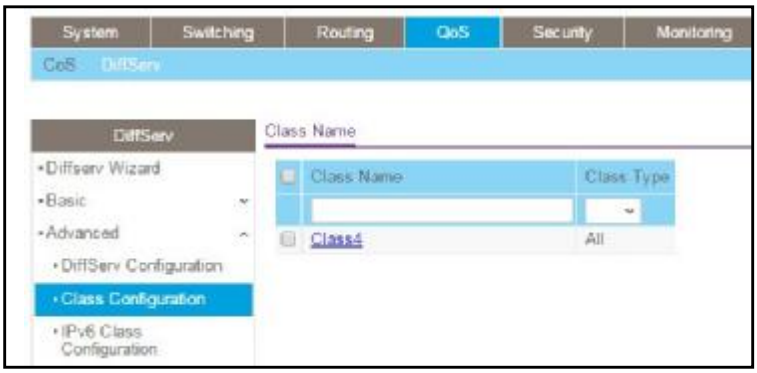
Field	Description
Policy Instance table	The number of configured policy class instances out of the total allowed on the switch.
Policy Attributes table	The number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
Service table	The number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

4.3.5. Configure a DiffServ Class

You can add a new DiffServ class name or rename or delete an existing class. You can also define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can use 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 screen.

To configure a DiffServ class:

QoS > DiffServ > Advanced > Class Configuration.



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

   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 is satisfied for a packet match. All signifies the logical AND of all the match criteria. You can select the class type only when you are creating a new class. After the class is created, the Class Type field becomes nonconfigurable.

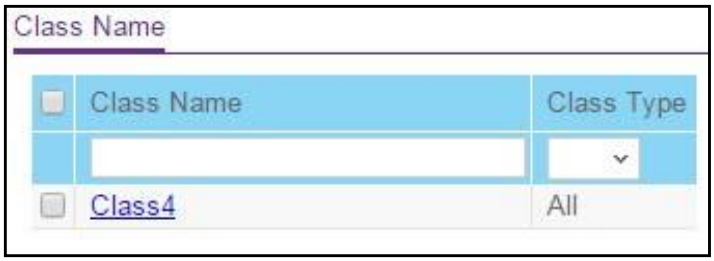
2. To rename an existing class, select the check box next to the configured class, update the name.
3. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

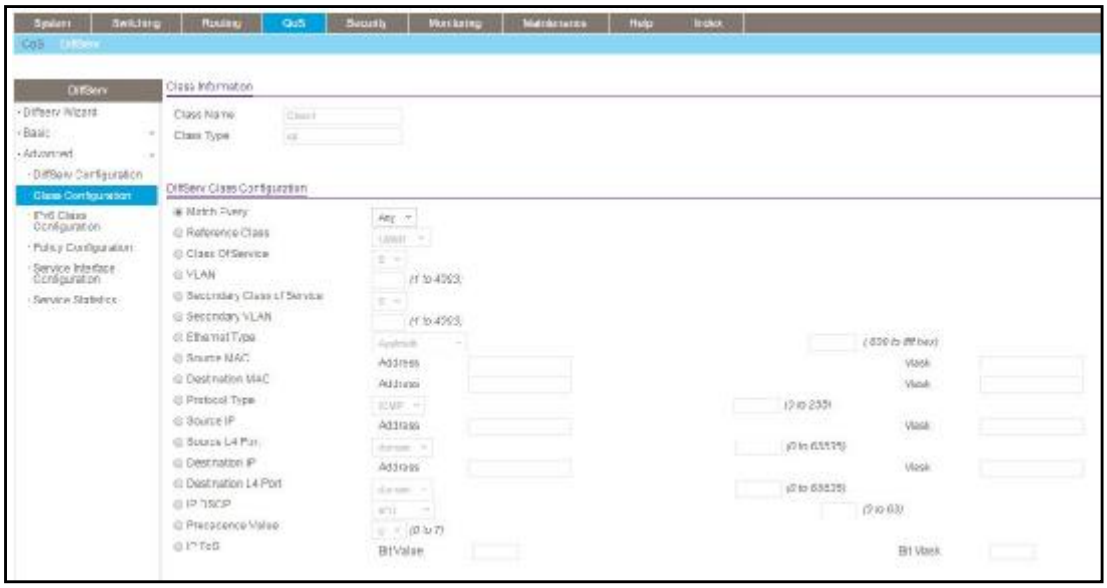
4. To remove a class, select the class name check box and click the **Delete** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

5. After creating a class, click the class link to the Class screen.
6. Click the **class name** for an existing class.



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



7. To configure the class details, complete the fields:
   - **Class Name** - The name for the configured DiffServ class.
   - **Class Type** - The DiffServ class type.

     You can select the class type only when you are creating a new class. After you create the class, this field displays the class type, but you cannot change it.
8. 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.
   - Secondary Class of Service. Select this option to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value.

- **Secondary VLAN**. Select this option to require a packet's VLAN ID to match a secondary VLAN ID or a secondary VLAN ID within a continuous range. If you configure a range, a match occurs if a packet's secondary VLAN ID is the same as any secondary VLAN ID within the range. After you select this option, use the following fields to configure the secondary VLAN match criteria:
  - **Secondary VLAN ID Start**. The secondary VLAN ID to match or the secondary VLAN ID with the lowest value within a range of VLANs.
  - **Secondary VLAN ID End**. The secondary VLAN ID with the highest value within the range of VLANs. This field is not required if the match criteria is a single VLAN ID.
- **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, 2-digit hexadecimal numbers separated by colons.
- **Source MAC Mask**. This is a bit mask in the same format as a 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, 2-digit hexadecimal numbers separated by colons.
- **Destination MAC Mask**. This is a bit mask in the same format as a 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.

9. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed in the Class Summary at the bottom of the DiffServ Advanced Class Configuration screen.

Table77. DiffServ Class Configuration - Class Summary

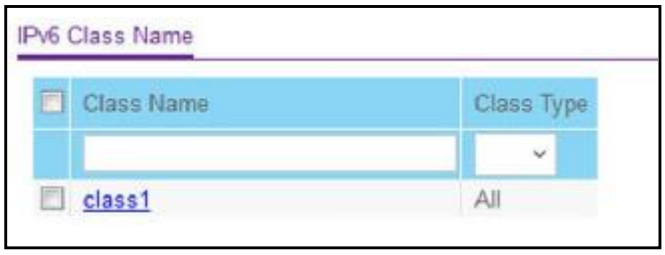
Field	Description
Match Criteria	The configured match criteria for the specified class.
Values	The values of the configured match criteria.

4.3.6. Configure DiffServ IPv6 Class Settings

You can add a new IPv6 DiffServ class name, or to rename or delete an existing class. You can also define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can use 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 screen.

To configure DiffServ IPv6 class settings:

QoS > DiffServ > Advanced > IPv6 Class Configuration.



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

   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 is 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 nonconfigurable field displaying the configured class type.

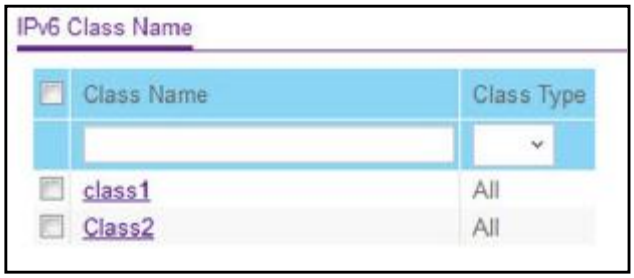
2. To rename an existing class, select the check box next to the configured class, and update the name
3. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

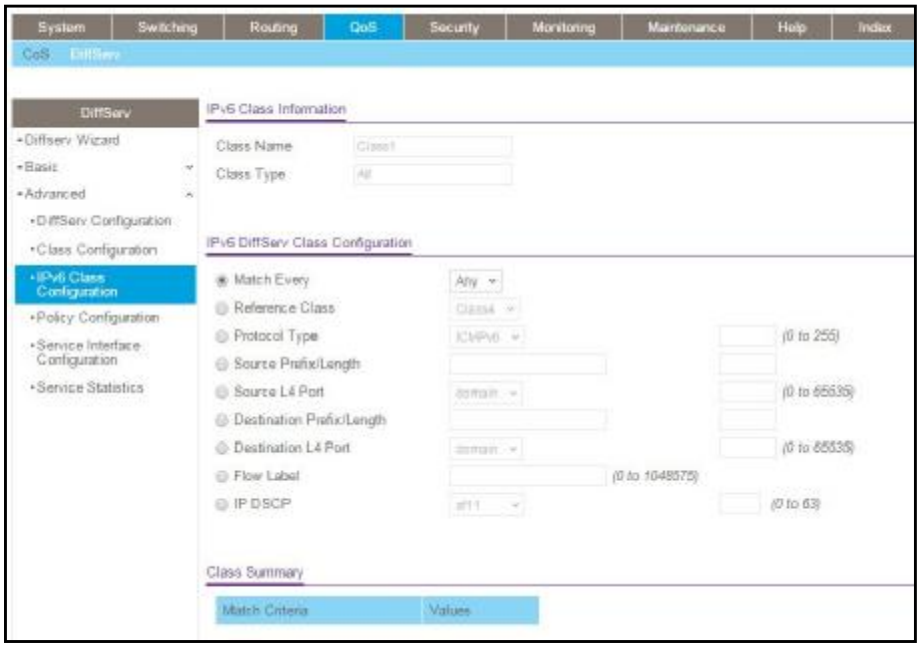
4. To remove a class, select the **Class Name** check box and then click the **Delete** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

5. After creating a class, click the **class name** for an existing class.



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



6. To configure the IPv6 class, complete the fields:
   - **Class Name** - The name for the configured DiffServ class.
   - **Class Type** - The DiffServ class type.

     Options: All

   You can specify the class type only when you are creating a new class. After the class is created, this field displays the class type, but you cannot change it.

7. 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. The prefix can be entered in the range of 0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and the 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. The prefix is always specified with the prefix length. The prefix can be entered in the range of 0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and the 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. The flow label can be specified in the range of 0 to 1048575.
- **IP DSCP** - You can select a keyword for the known DSCP values. The list includes Other as an option for the remaining values.

8. **Match Criteria** - Displays the configured match criteria for the specified class.
9. **Values** - Displays the values of the configured match criteria.
10. Click the **Apply** button.

    The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed in the Class Summary at the bottom of the DiffServ Advanced IPv6 Class Configuration screen.

Table78. DiffServ IPv6 Class Configuration - Class Summary

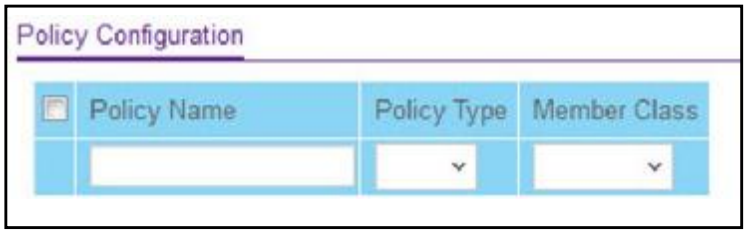
Field	Description
Match Criteria	The configured match criteria for the specified class.
Values	The values of the configured match criteria.

4.3.7. Configure DiffServ Policy

You can associate a collection of classes with one or more policy statements. After creating a policy, click the policy link to the Policy screen.

To configure DiffServ policy:

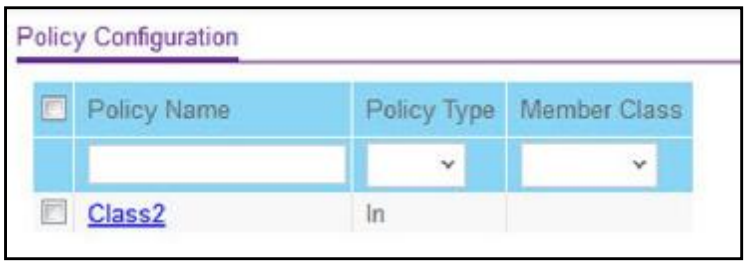
QoS > DiffServ > Advanced > Policy Configuration.



1. Use **Policy Name** to uniquely identify a policy using a case-sensitive alphanumeric string from 1 to 31 characters.
2. In the **Member Class** list, select a DiffServ class.

   This lists all existing DiffServ classes currently defined as members of the specified policy. 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 nonconfigurable field.
3. **Policy Type** - Indicates the type is specific to inbound traffic direction.
4. Click the **Add** button.

   The new policy is added to the switch.
5. Click the **Delete** button to delete the currently selected policy from the switch.
6. To configure the policy attributes, click the name of the policy.



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

7. Select the **Assign Queue** to which packets of this policy-class are assigned. This is an integer value in the range 0 to 6.
8. 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.
- **Mirror**
- **Redirect**
- **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).

9. 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 according to 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 according to the policing metrics, from which one can be selected. The default is send.
   - For each of the 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 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 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 field be set.

10. If you select **Two Rate**, you can configure additional fields (same fields as for a simple policy).
11. Click the **Apply** button.

    The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

Table 203. DiffServ Policy Configuration - Policy Attribute

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.

4.3.8. Configure the DiffServ Service Interface

To configure the DiffServ service interface:

QoS > DiffServ > Advanced > Service Interface Configuration.

1. Use **Interface** to select the interface for 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 the inbound service policy attachment is not supported by the platform.

Table79. Service Interface Configuration

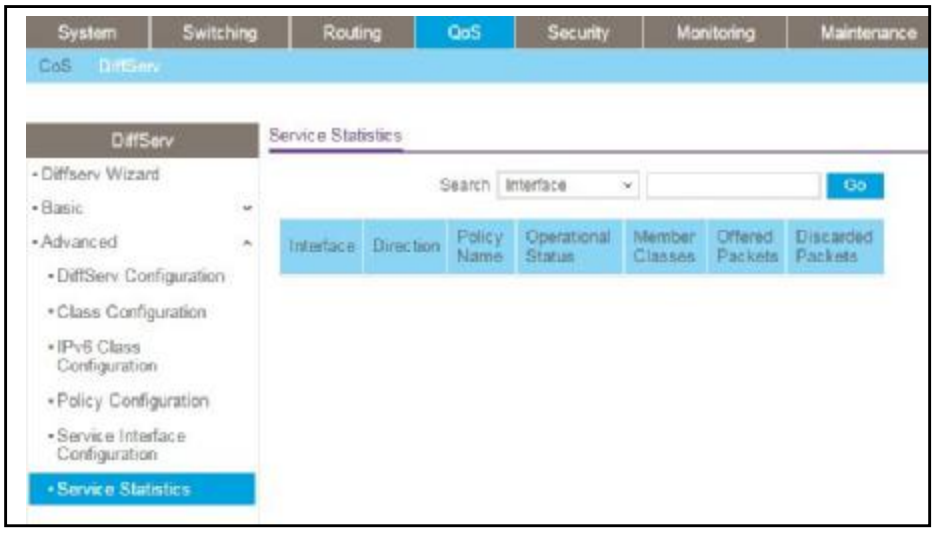
Field	Description
Direction	Shows that the traffic direction of this service interface is In.
Operational Status	Shows the operational status of this service interface, either Up or Down.

4.3.9. View DiffServ Service Statistics

This screen displays class-oriented statistical information for the policy, which is specified by the interface and direction. The Member Class 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 view the DiffServ service statistics:

QoS > DiffServ > Advanced > Service Statistics.



1. Use the **Search** menu to search for neighbor entries by MAC Interface, or Neighbor IP.
2. To search by interface, select **Interface**, enter the interface in unit/slot/port format, for example, 1/0/13. Then click the **Go** button.

   If the neighbor entry exists, the entry is displayed as the first entry, followed by the remaining entries.
3. To search by member class, select **Member Class**, enter the Member Class, then click the **Go** button.

   If the entry with a matching Member Class exists, that entry is displayed as the first entry, followed by the remaining entries. An exact match is required.

To refresh the screen with the latest information on the switch, click the **Update** button.

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

Table80. DiffServ Service Statistics

Field	Description
Interface	List of all valid slot number and port number combinations in the system with a DiffServ policy currently attached in In direction.
Direction	List of the traffic direction of interface as In. Shows only 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. Select a member class name to display its statistics. If no class is associated with the selected polic,y then nothing is populated in the list.
Offered Packets	A count of the total number of packets 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	A count of the total number of packets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per interface, per direction. The discarded packets are supported in the inbound direction but not in the outbound direction.

5. Manage Device Security

This chapter covers the following topics:

- *Management Security Settings*
- *TACACS Overview*
- *Configure Management Access*
- *Port Authentication*
- *Traffic Control*
- *Port Security*
- *DHCP Snooping*
- *Configure Access Control Lists*

5.1. Management Security Settings

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.

5.1.1. Configure Users

By default, two user accounts exist:

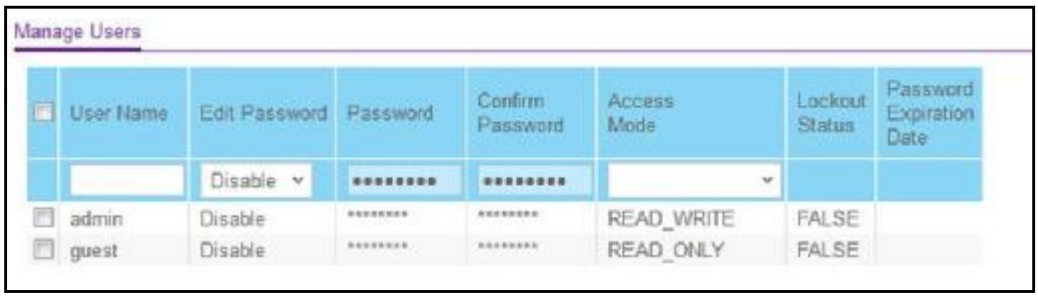
- admin, with read/write privileges
- guest, with read-only privileges

By default, the password is blank for both of these accounts. The names are not case-sensitive.

If you log on to a user account with read/write privileges (as admin), you can assign passwords and set security parameters for the default accounts and add and delete accounts (other than admin), up to a maximum of six. Only a user with read/write privileges can modify data on the web interface screens, and only one account can be created with read/write privileges.

To configure users:

Security > Management Security > Local User > User Management.



1. In the **User Name** field, enter the name for the new account.

   You can enter a new user name only when you are creating an 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 hyphen (-) and underscore (_) characters. The user name default is not valid. User names once created cannot be changed or modified.

2. Set the **Edit Password** field to **Enable** only when you are changing the password.

   The default value is Disable.

3. In the **Password** field, enter the password for the account.

   The characters do not display as they are typed; only asterisks (*) show. Passwords are up to eight alphanumeric characters in length, and are case-sensitive.

4. In the **Confirm Password** field, enter the password again, to confirm that you entered it

correctly.

This field does not display the password as it is typed, but shows asterisks (*).

The **Access Mode** field displays the user's access mode. The admin account always has read/write access, and all other accounts are assigned read-only access. The default value is read-only.

The **Lockout Status** field indicates whether the user account is locked out (TRUE or FALSE).

The **Password Expiration Date** field indicates the current password expiration date.

5. Click the **Add** button.

   The user account is added.

6. To delete the selected user account, click the **Delete** button.

   You cannot delete the admin read/write user.

5.1.2. Configure a User Password

To configure a user password:

Security > Management Security > Local User > User Password Configuration.

1. In the **Password Minimum Length** field, type the minimum character length of all new local user passwords.
2. In the **Password Aging (days)** field, type 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 must enter a new password following the first login after password expiration. A value of 0 indicates that passwords never expire.

3. In the **Password History** field, type 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 are stored.

4. In the **Lockout Attempts** field, specify the number of allowable failed local authentication attempts before the user's account is locked.

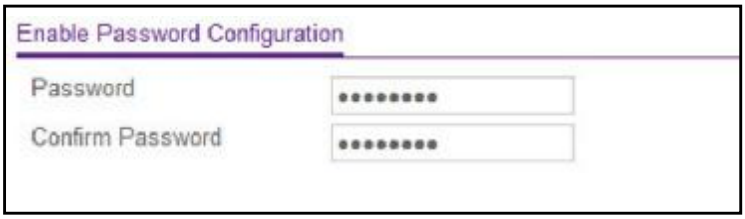
   A value of 0 indicates that user accounts are never locked.

5.1.3. Enable Password Configuration

You can change the privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case-sensitive.

To enable password configuration:

Security > Management Security > Enable Password.



1. In the **Password** field, type the password.

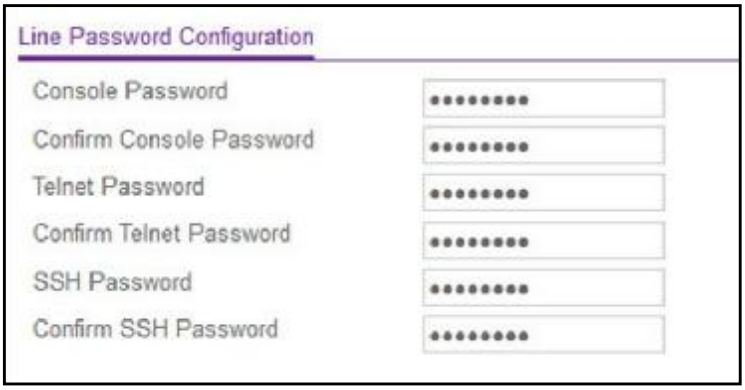
   Passwords are a maximum of 64 alphanumeric characters.

2. In the **Confirm Password** field, type the password again, to confirm that you entered it correctly.

5.1.4. Configure a Line Password

To configure a line password:

Security > Management Security > Line Password.



1. In the **Console Password** field, enter the console password.

   Passwords are a maximum of 64 alphanumeric characters.

2. In the **Confirm Console Password** field, type the password again to confirm that you typed it correctly.
3. In the **Telnet Password** field, type the Telnet password.

   Passwords are a maximum of 64 alphanumeric characters.

4. In the **Confirm Telnet Password** field, type the password again to confirm that you entered it correctly.
5. In the **SSH Password** field, type the SSH password.

   Passwords are a maximum of 64 alphanumeric characters.

6. In the **Confirm SSH Password** field, type the password again, to confirm that you entered it correctly.

5.1.5. RADIUS Overview

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 the following:

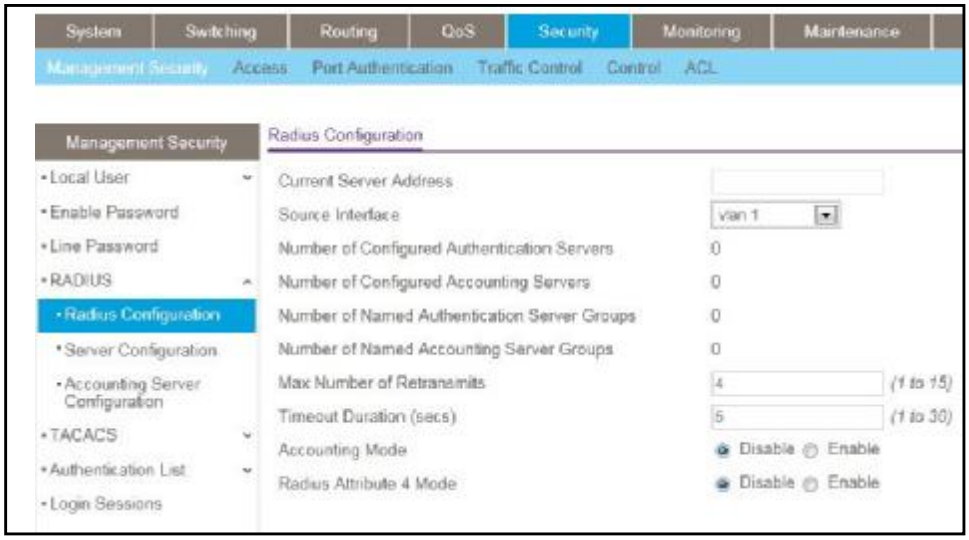
- Web access
- Access control port (802.1X)

5.1.6. Configure Global RADIUS Server Settings

You can add information about one or more RADIUS servers on the network.

To configure global RADIUS server settings:

Security > Management Security > RADIUS > Radius Configuration.



The **Current Server IP Address** field is blank if no servers are configured (see *Configure a RADIUS Server* on page 548). The switch supports up to three configured RADIUS servers. If more than one RADIUS servers is configured, the current server is the primary server. If no servers are configured as the primary server, the current server is the most recently added RADIUS server.

1. In the **Source Interface** list, select the interface to use for RADIUS.

   Possible values are as follows:

   - **None**
   - **Routing interface**
   - **Routing VLAN**
   - **Routing loopback interface**
   - **Service Port**

   By default, VLAN 1 is used as source interface.

2. In the **Max Number of Retransmits** field, specify 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.

Consider the maximum delay time when you configure the RADIUS maximum retransmit and RADIUS time-out. If multiple RADIUS servers are configured, the maximum retransmit value on each is exhausted before the next server is attempted. A retransmit does not occur until the configured time-out value on that server passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the retransmit times the time-out for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a response.

3. 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.

   Consider the maximum delay time when you configure RADIUS maximum retransmit and RADIUS time-out. If multiple RADIUS servers are configured, the maximum retransmit value on each is exhausted before the next server is attempted. A retransmit does not occur until the configured time-out value on that server passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the retransmit times the time-out for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a response.

4. Select the Accounting Mode **Disable** or **Enable** radio button.

   This specifies whether the RADIUS accounting mode is enabled or disabled on the current server.

5. Select the RADIUS Attribute 4 **Disable** or **Enable** radio button.

   This enables or disables RADIUS attribute 4. The default value is Disable. 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.

Table81. Radius Configuration

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	The number of configured authentication RADIUS servers. The value can range from 0 to 32.
Number of Configured Accounting Servers	The number of RADIUS accounting servers configured. The value can range from 0 to 32.
Number of Named Authentication Server Groups	The number of Named RADIUS server authentication groups configured.
Number of Named Accounting Server Groups	The number of named RADIUS server accounting groups configured.

5.1.7. Configure a RADIUS Server

To configure a RADIUS server:

Security > Management Security> RADIUS > Server Configuration.

1. To add a RADIUS server, specify the following settings:
   - In the **Radius Server IP Address** field, specify the IP address of the RADIUS server.
   - In the **Radius Server Name** field, specify the name of the server.
   - Use **Port** to specify the UDP port used by this server. The valid range is 0–65535.
   - **Secret Configured**. The secret is applied only if this option is **Yes**. If the option is **No**, anything entered in the secret field has no effect and is not 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 the **Add** button.

   The server is added to the switch.

   This button is available only when you log in with the admin user name, which has read-write permission. These changes are not retained across a power cycle unless a save is performed.
3. To remove the selected server from the configuration, click the **Delete** button.

   This button is available only when you log in with the admin user name, which has read-write permission. These changes are not retained across a power cycle unless a save is performed.

The **Current** field indicates if this server is currently in use as the authentication server.

To reset the authentication server and RADIUS statistics to their default values, click the **Clear Counters** button at the bottom of the screen.

The following table describes the RADIUS server statistics displayed on the screen.

Table82. RADIUS statistics

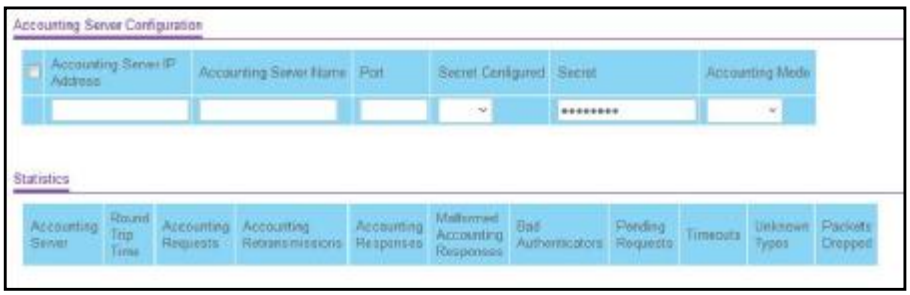
Field	Description
Radius Server	The address of the RADIUS server or the name of the RADIUS server for which the statistics are displayed.
Round Trip Time	The time interval, in hundredths of a second, between the most recent access-reply/access-challenge and the access-request that matched it from this 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 did not yet time out or receive a response.
Timeouts	The number of authentication time-outs to this server.
Unknown Types	The number of RADIUS packets of unknown type that 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.

5.1.8. Configure RADIUS Accounting Servers

To configure a RADIUS accounting server:

Security > Management Security > RADIUS > Accounting Server Configuration.



1. In the **Accounting Server IP Address** field, specify the IP address of the RADIUS accounting server.
2. In the **Accounting Server Name** field, enter the name of the accounting server.
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 read-only access, the value is displayed but cannot be changed.

4. From the **Secret Configured** list, 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 is configured.

5. In the **Secret** field, type the shared secret to use with the specified accounting server.
6. From the **Accounting Mode** list, enable or disable the RADIUS accounting mode.
7. To delete a configured RADIUS accounting server, click the **Delete** button.

To clear the accounting server statistics, click the **Clear Counters** button.

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

Table83. RADIUS Accounting Server Statistics

Field	Description
Accounting Server Address	The accounting server associated with the statistics.
Round Trip Time(secs)	The time interval, in hundredths of a second, between the most recent accounting-response and the accounting-request that matched it from this RADIUS accounting server.
Accounting Requests	The number of RADIUS accounting-request packets sent not including retransmissions.
Accounting Retransmissions	The number of RADIUS accounting-request packets retransmitted to this RADIUS accounting server.
Accounting Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Accounting Responses	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	The number of RADIUS accounting-response packets that contained invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS accounting-request packets sent to this server that did not yet time out or receive a response.
Timeouts	The number of accounting time-outs to this server.
Unknown Types	The number of RADIUS packets of unknown type that were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

5.2. TACACS Overview

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 through 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.

5.2.1. Configure Global TACACS Settings

You can configure the TACACS settings for communication between the switch and the TACACS server you configure through the inband management port.

To configure global TACACS settings:

Security > Management Security > TACACS > TACACS Configuration.

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. The key must match the key configured on the TACACS server.

2. In the **Connection Timeout** field, specify the maximum number of seconds allowed to establish a TCP connection between the managed switch and the TACACS server.
3. In the **Source Interface** list, select the source for TACACS.

   Possible values are as follows:

   - None
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Service port

   By default VLAN 1 is used as source interface.

4. Click the **Apply** button.

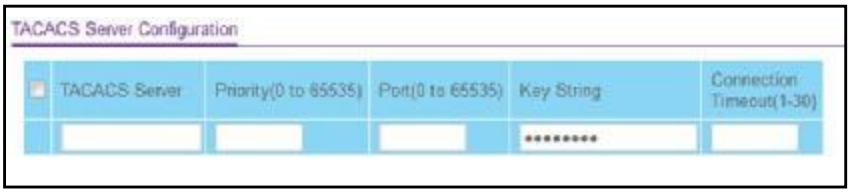
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

5.2.2. Configure TACACS Server Settings

You can configure up to five TACACS servers with which the switch can communicate.

To configure TACACS server settings:

Security > Management Security> TACACS > TACACS Server Configuration.



1. Use **TACACS Server** to configure the TACACS server IP address.
2. Use **Priority** to specify the order in which the TACACS servers are used.

   The valid range is 0–65535.

3. Use **Port** to specify the authentication port. It must 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. 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 1–30.

6. Click the **Add** button.

   The server is added to the switch.

   This button is available only to read/write users. These changes are not retained across a power cycle unless a save is performed.

7. To delete the selected server from the configuration, click the **Delete** button.

5.2.3. Configure a Login Authentication List

A login list specifies the authentication methods to be used to validate switch or port access for the users associated with the list. The preconfigured users, admin and guest, are assigned to a preconfigured 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 configure a login authentication list:

Security > Management Security > Authentication List > Login Authentication List.

1. To create a new login list, enter the name in the **List Name** field.

   The name can be up to 15 alphanumeric characters long and is not case-sensitive.

2. In the numbered lists (1, 2, 3, 4, 5, 6) select the method to appear first in the selected authentication enable list.

   The options are as follows:

   - **Enable**. The privileged EXEC password is used for authentication.
   - **Line**. The line password is used for authentication.
   - **None**. The user cannot be authenticated.
   - **RADIUS**. The user's name and password are authenticated using the RADIUS server instead of local server.
   - **TACACS**. The user's name and password are authenticated using the TACACS server.
   - **Deny**. Authentication always fails.

3. Click the **Add** button.

   The login list is added to the switch.

4. To remove the selected authentication login list from the configuration, click the **Delete** button.

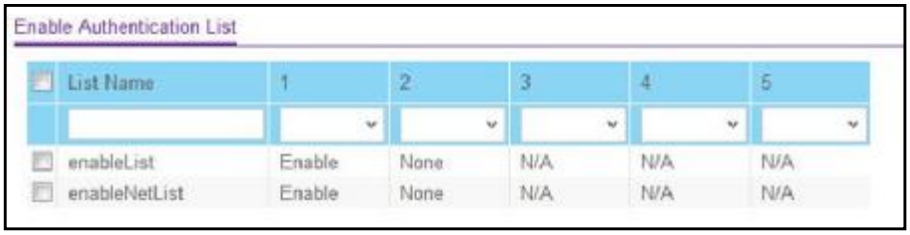
   The delete fails if the selected login list is assigned to any user (including the default user) for system login. You can use this button only if you logged in as the admin user, which has read/write access. The change is not retained across a power cycle unless you perform a save.

5.2.4. Configure an Enable Authentication List

An enable list specifies the authentication methods to validate privileged EXEC access for the users associated with the list. The preconfigured users, admin and guest, are assigned to a preconfigured 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 configure an enable authentication list:

Security > Management Security > Authentication List > Enable Authentication List.



1. To create a new enable list, enter the name in the **List Name** field.

   It can be up to 15 alphanumeric characters long and is not case-sensitive.

2. In the numbered lists (1, 2, 3, 4, 5, 6) select the method to appear first in the selected authentication enable list.

   The options are as follows:

   - **Enable**. The privileged EXEC password is used for authentication.
   - **Line**. The line password is used for authentication.
   - **None**. The user cannot be authenticated.
   - **RADIUS**. The user's name and password are authenticated using the RADIUS server instead of local server.
   - **TACACS**. The user's name and password are authenticated using the TACACS server.
   - **Deny**. Authentication always fails.

3. Click the **Add** button.

   The login list is added to the switch.

4. To remove the selected authentication enable list from the configuration, click the **Delete** button.

   You can use this button only if you have read/write access. The change is not retained across a power cycle unless you perform a save.

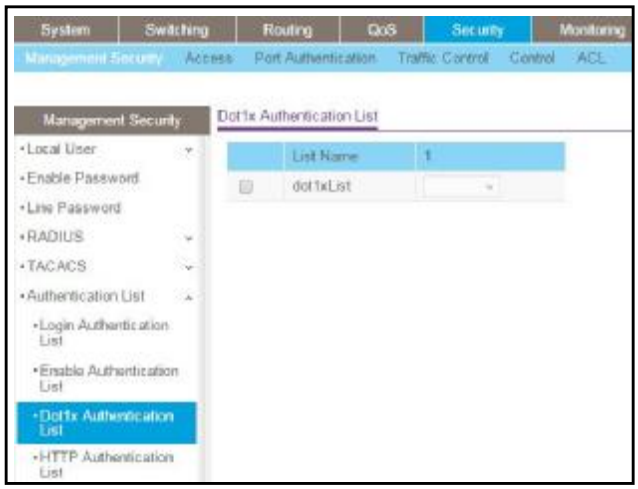
5.2.5. Configure the Dot1x Authentication List

You can configure a dot1x list. A dot1x list specifies the authentication methods to validate port access for the users associated with the list. Only one dot1x method can be supported.

The default list is dot1xList.

To configure the dot1x authentication list:

Security > Management Security > Authentication List > Dot1x Authentication List.



1. In the **List Name** field, select the dot1x list name.
2. Select the method to appear first in the selected authentication login list.

   The options are as follows:

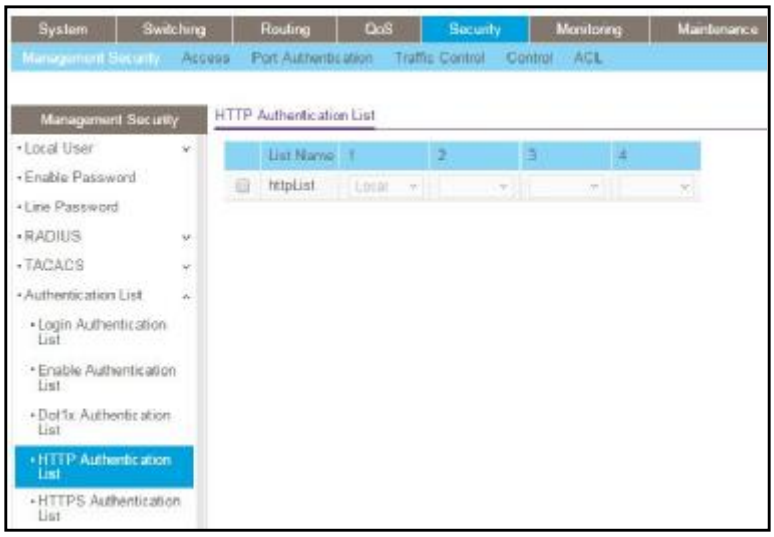
   - **IAS**. The user's ID and password in internal authentication server database is used for authentication.
   - **Local**. The user's locally stored ID and password are used for authentication.
   - **RADIUS**. The user's ID and password are authenticated using the RADIUS server instead of locally.
   - **None**. The user authenticated without a user name and password.

5.2.6. Configure an HTTP Authentication List

You can configure an HTTP list. An HTTP list specifies the authentication methods to validate the switch or port access through HTTP.

To configure an HTTP authentication list:

Security > Management Security > Authentication List > HTTP Authentication List.



1. Use **List Name** to select the HTTP list name.
2. In the numbered lists (1, 2, 3, 4) select the method to appear first in the selected authentication enable list.

   The options are as follows:

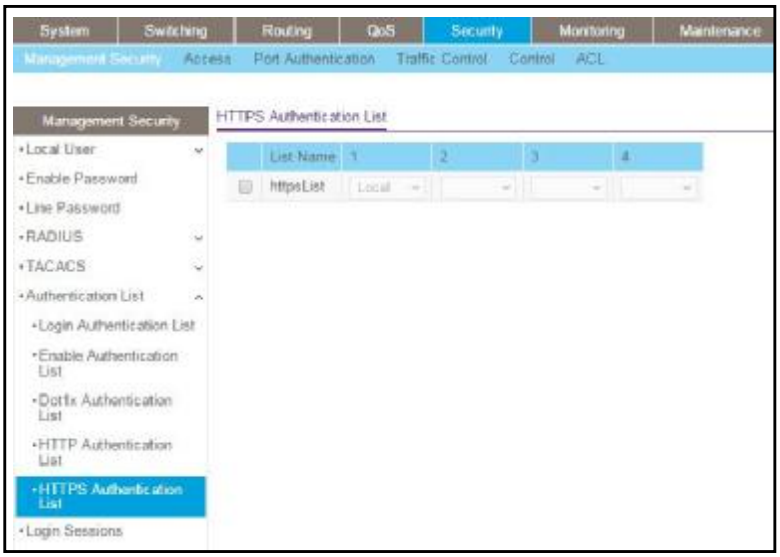
   - **Enable**. The privileged EXEC password is used for authentication.
   - **None**. The user cannot be authenticated.
   - **RADIUS**. The user's name and password are authenticated using the RADIUS server instead of local server.
   - **TACACS**. The user's name and password are authenticated using theTACACS server.

5.2.7. Configure an HTTPS Authentication List

You can configure an HTTPS list. A login list specifies the authentication methods to validate the switch or port access through HTTPS for the users associated with the list. The default list is httpsList.

To configure an HTTPS authentication list:

Security > Management Security > Authentication List > HTTPS Authentication List.



1. Select the **List Name** check box for the HTTPS list name.
2. In the numbered lists (1, 2, 3, 4, 5, 6) select the method to appear first in the selected authentication enable list.

   The options are as follows:

   - **Enable**. The privileged EXEC password is used for authentication.
   - **None**. The user cannot be authenticated.
   - **RADIUS**. The user's name and password are authenticated using the RADIUS server instead of local server.
   - **TACACS**. The user's name and password are authenticated using theTACACS server.

5.2.8. View Login Sessions

To view login sessions:

Security > Management Security > Login Sessions.

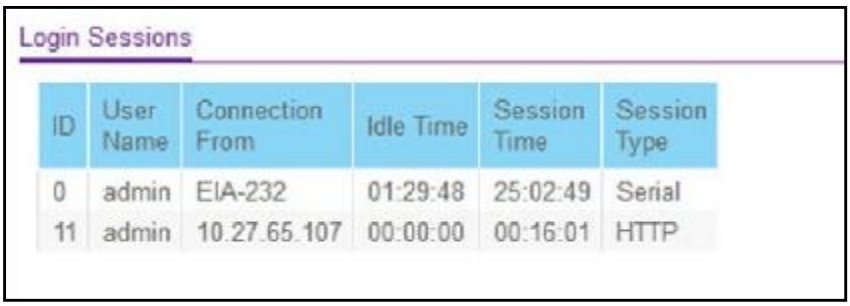


Table84. Login Sessions

Field	Description
ID	Identifies the ID of this row.

User Name	The user's name whose session is open.
Connection From	The machine from which the user is connected.
Idle Time	The idle session time.
Session Time	The total session time.
Session Type	The type of session: Telnet, Serial, or SSH

5.3. Configure Management Access

You can configure HTTP and Secure HTTP access to the switch's management interface.

5.3.1. Configure HTTP Server Settings

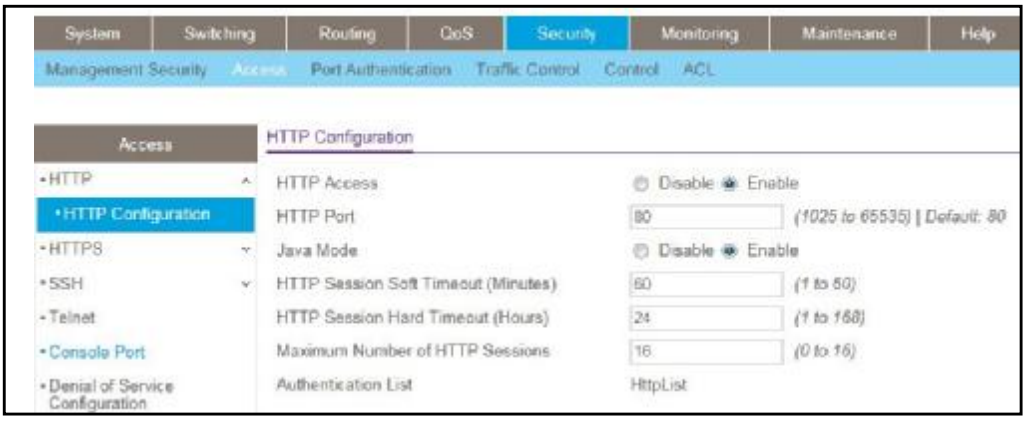
To access the switch using a web browser, you must first configure it with IP information (IP address, subnet mask, and default gateway). You can configure the IP information using any of the following:

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

Once you establish in-band connectivity, you can change the IP information using a web-based management.

To configure the HTTP server settings:

Security > Access> HTTP > HTTP Configuration.



1. Select the HTTP Access **Disable** or **Enable** radio button.

   This specifies whether the switch can be accessed from a web browser. If you enable web mode, you can manage the switch from a web browser. The factory default is Enable.

2. In the **HTTP Port** field, enter the HTTP port number.

   The valid range is 80 and 1025 to 65535. The default value is 80.

3. Select the Java Mode **Disable** or **Enable** radio button.

This enables or disables the Java applet, which displays a picture of the switch in the Device view tab of the System tab. If you run the applet, you can click 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.

4. In the **HTTP Session Soft Timeout (Minutes)** field, 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 displays.

5. In the **HTTP Session Hard Timeout (Hours)** field, 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 displayed.

6. In the **Maximum Number of HTTP Sessions** field, 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 displayed.

   The **Authentication List** field displays the list that HTTP is using.

5.3.2. 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.

You can to configure the settings for HTTPS communication between the management station and the switch.

To configure HTTPS settings:

Security > Access > HTTPS > HTTPS Configuration.

1. Select the HTTPS Admin Mode **Disable** or **Enable** radio button.

   This enables or disables the administrative mode of Secure HTTPS. The currently

configured value is displayed. The default value is Disable. You can download SSL certificates only when the HTTPS admin mode is disabled. HTTPS admin mode can be enabled only if a certificate is present on the device.

2. Select the SSL Version 3 **Disable** or **Enable** radio button.

   This enables or disables Secure Sockets Layer version 3.0. The currently configured value is displayed. The default value is Enable.

3. Select the TLS Version 1 **Disable** or **Enable** radio button

   This enables or disables Transport Layer Security version 1.0. The currently configured value is displayed. The default value is Enable.

4. In the **HTTPS Port** field, type 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 displayed.

5. In the **HTTPS Session Soft Timeout (Minutes)** field, enter the inactivity time-out for HTTPS sessions.

   The value must be in the range of 1 to 60 minutes. The default value is 5 minutes. The currently configured value is displayed.

6. In the **HTTPS Session Hard Timeout (Hours)** field, 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 displayed.

7. In the **Maximum Number of HTTPS Sessions** field, enter 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 displayed.

   The **Authentication List** field displays the authentication list for HTTPS.

5.3.3. Manage Certificates

You can generate or delete certificates.

To manage certificates:

Security > Access > HTTPS > Certificate Management.

The **Certificate Present** field displays whether there is a certificate present on the device.

1. Select one of the following radio buttons:
   - **None**. There is nothing to be done with respect to certificate management. This is the default selection.
   - **Generate Certificates**. Begin generating the certificate files.
   - **Delete Certificates**. Delete the corresponding certificate files, if present.

The **Certificate Generation Status** field displays the SSL certificate generation status.

5.3.4. Download Certificates

You can 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, offline) and download it to the switch.

Before you download a file to the switch, the following conditions must be true:

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

To download certificates:

Security > Access > HTTPS > Certificate Download.

1. In the **File Type** list, specify the type of file 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. In the **Transfer Mode** list, specify the protocol to use to transfer the file:
   - **TFTP**. Trivial File Transfer Protocol
   - **SFTP**. Secure File Transfer Protocol
   - **SCP**. Secure Copy Protocol
3. In the **Server Address Type** list, specify either IPv4, IPv6, or DNS to indicate the format of the TFTP/SFTP/SCP Server Address field.

   The factory default is IPv4.
4. In the **Server Address** field, type the IP address or DNS host name 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. In the **Remote File Path** field, enter the path of the file to download.

   You can enter up to 96 characters. The factory default is blank.
6. In the **Remote File Name** field, enter the name of the file on the TFTP server to download.

   You can enter up to 32 characters. The factory default is blank.

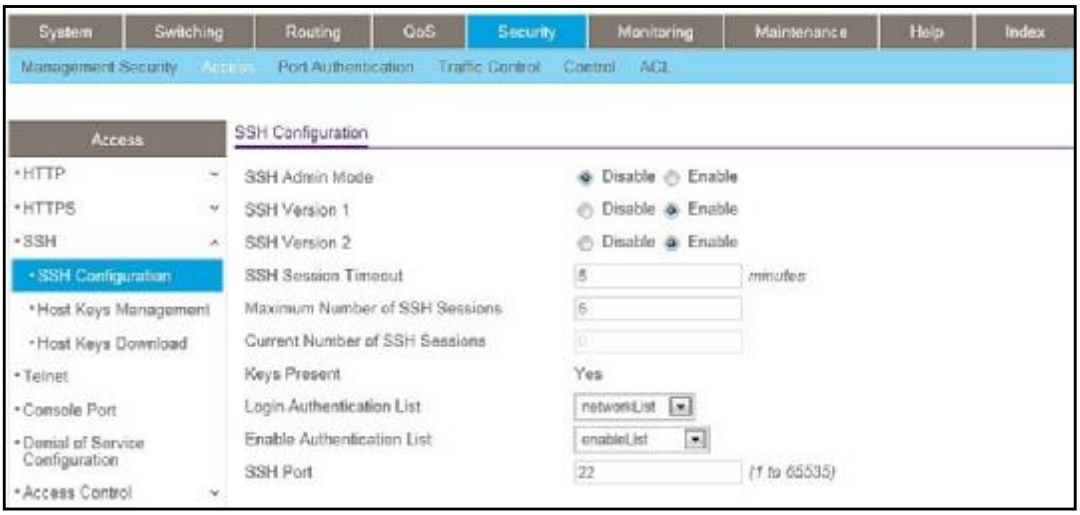
5.3.5. Configure SSH Settings

You can view and modify the Secure Shell (SSH) server settings on the device. SSH is a network protocol that enables access to the CLI management interface by using an SSH client on a remote administrative system. SSH is a more secure access method than Telnet

because it encrypts communication between the administrative system and the device. You can download or generate SSH host keys for secure CLI-based management.

To configure SSH settings:

Security > Access > SSH > SSH Configuration.



1. Select the SSH Admin Mode **Disable** or **Enable** radio button.

   This enables or disables the SSH server administrative mode. When this mode is enabled, the device can be accessed by using an SSH client on a remote system. The currently configured value is displayed. The default value is Disable.

2. Select the SSH Version 1 **Disable** or **Enable** radio button.

   This enables or disables Protocol Level 1 for SSH. When Enable is selected, the SSH server on the device can accept connections from an SSH client using Protocol Level 1 for SSH (SSH-1). When Disable is selected, the device does not allow connections from clients using the SSH-1 protocol. The currently configured value is displayed. The default value is Enable.

3. Select the SSH Version 2 **Disable** or **Enable** radio button.

   This enables or disables Protocol Level 2 for SSH. When Enable is selected, the SSH server on the device can accept connections from an SSH client using Protocol Level 2 for SSH (SSH-2). When Disable is selected, the device does not allow connections from clients using the SSH-2 protocol.The currently configured value is displayed. The default value is Enable.

4. Use **SSH Session Timeout** to configure the SSH session inactivity time-out value for incoming SSH sessions to the switch.

   A connected user that does not exhibit any SSH activity for this amount of time is automatically disconnected from the device. 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 that can be connected to the device simultaneously.

   The currently configured value is displayed. The acceptable range for this field is 0–5.

6. Use **Login Authentication List** to select an authentication list.

   This list is used to authenticate users who try to login to the switch.

7. Use **Enable Authentication List** to select an authentication list.

This list is used to authenticate users who try to get *enable* level privilege.

8. Use **SSH Port** to enter the port range from 1 to 65535.

   The default value is 22.

9. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

Table85. SSH Configuration

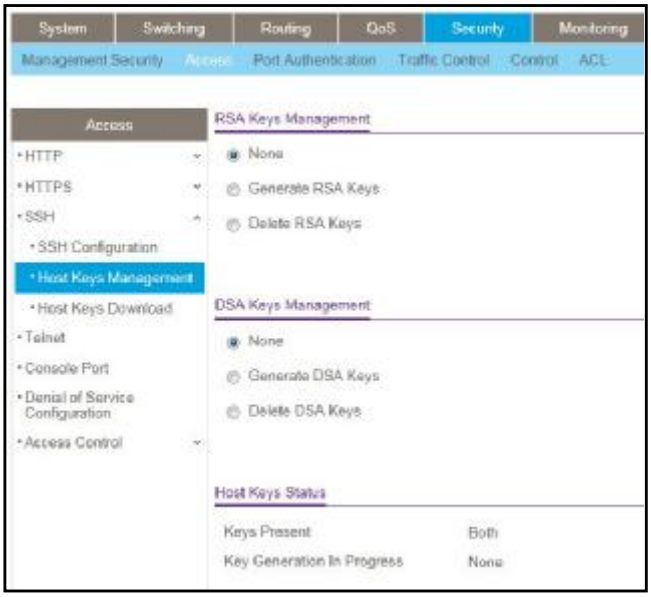
Field	Description
Current Number of SSH Sessions	The number of active SSH sessions between remote SSH clients and the SSH server on the device.
Keys Present	Displays **Yes** or **No** whether one or both (if any) of the following keys are present on the device: • SSH-1 Rivest-Shamir-Adelman (RSA) key file or SSH-2 RSA key file (PEM encoded) • SSH-2 Digital Signature Algorithm (DSA) key file (PEM encoded)

5.3.6. Manage Host Keys

You can generate or delete RSA and DSA keys.

To manage host keys:

Security > Access > SSH > Host Keys Management.



1. Select an RSA Keys Management radio button:
   - **None**. This is the default selection.
   - **Generate RSA Keys**. Begin generating the RSA host keys. To generate SSH key files SSH must be administratively disabled and there can be no active SSH sessions.
   - **Delete RSA Keys**. Delete the corresponding RSA key file, if it is present.
2. Select a DSA Keys Management radio button:
   - **None**. This is the default selection.
   - **Generate DSA Keys**. Begin generating the DSA host keys.

     To generate SSH key files SSH must be administratively disabled and there can be no active SSH sessions.
   - **Delete DSA Keys**. Delete the corresponding DSA key file, if it is present.
3. Click the **Apply** button.

   The host key file starts downloading. To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

To refresh the screen with the latest information on the switch, click the **Update** button.

Table86. Table 211. RSA Key Management

Field	Description
Keys Present	Displays which of the following keys or both (if any) are present on the device: • SSH-1 Rivest-Shamir-Adelman (RSA) key file or SSH-2 RSA key file (PEM Encoded) • SSH-2 Digital Signature Algorithm (DSA) key file (PEM Encoded)
Key Generation In Progress	Displays which key is being generated (if any), RSA, DSA, or None.

5.3.7. Download Host Keys

You can download an SSH-1 RSA, SSH-2 RSA, or SSH-2 DSA key file from a remote system to the device.

To download host keys:

Security > Access > SSH > Host Keys Download.

1. In the **File Type** list, select the type of file to transfer:
   - **SSH-1 RSA Key File**. SSH-1 Rivest-Shamir-Adelman (RSA) key file
   - **SSH-2 RSA Key PEM File**. SSH-2 Rivest-Shamir-Adelman (RSA) key file (PEM Encoded)
   - **SSH-2 DSA Key PEM File**. SSH-2 Digital Signature Algorithm (DSA) key file (PEM Encoded)
2. In the **Transfer Mode** list, select the protocol to use to transfer the file:
   - **TFTP**. Trivial File Transfer Protocol
   - **SFTP**. Secure File Transfer Protocol
   - **SCP**. Secure Copy Protocol
3. In the **Server Address Type** field, specify either **IPv4**, **IPv6**, or **DNS**.

   This specifies the format of the TFTP/SFTP/SCP Server Address field. The factory default is IPv4.
4. In the **Server Address** field, enter the IP address or DNS host name 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. In the **Remote File Path** field, enter the path of the file to download.

   You can enter up to 96 characters. The factory default is blank.

6. Iin the **Remote File Name** field, enter the name of the file on the TFTP server to download.

   You can enter up to 32 characters. The factory default is blank.

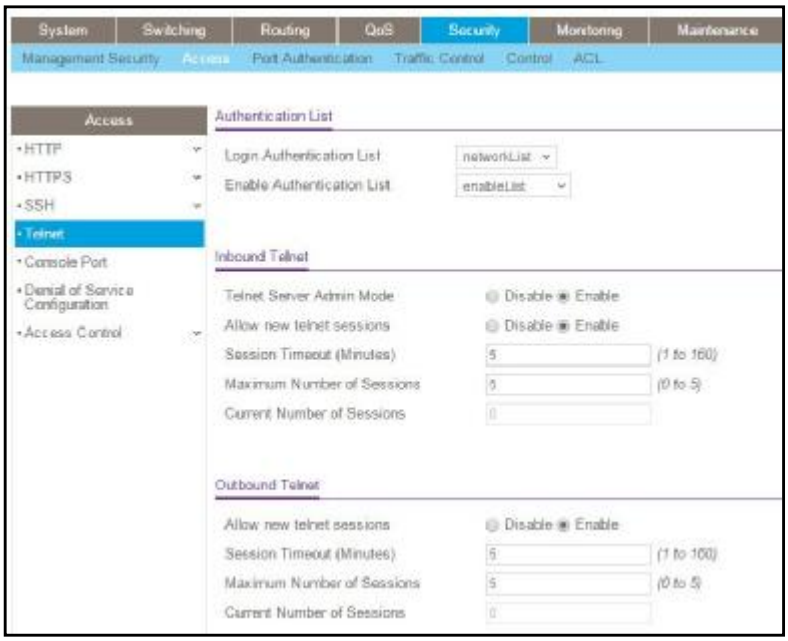
7. Click the **Apply** button.

   The host key file starts downloading. To download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

5.3.8. Configure Telnet Settings

To configure Telnet settings:

Security > Access > Telnet.



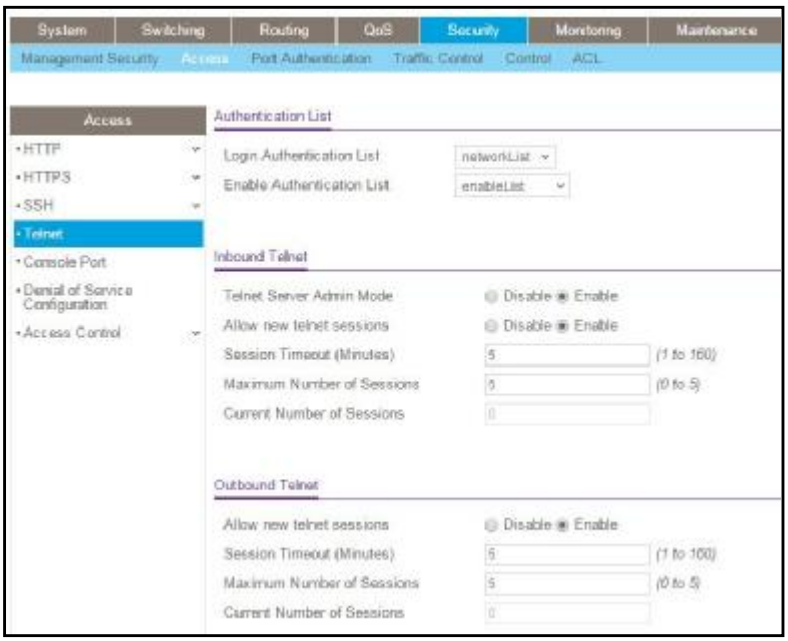
5.3.9. Configure the Telnet Authentication List

You can select the Login and Enable authentication list available. The login list specifies the authentication methods to use to validate switch or port access for the users associated with

the list. The enable list specifies the authentication methods 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.

To configure the Telnet authentication list:

Security > **Access > Telnet**.



1. Use **Login Authentication List** to specify which authentication list to use log in 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.

3. To configure inbound Telnet settings, specify the following:

   - Select the Telnet Server Admin Mode **Disable** or **Enable** radio button.

     This enables or disables the administrative mode of the Telnet server. The default value is Enabled.

   - Select the Allow New Telnet Sessions **Disable** or **Enable** radio button.

     This specifies whether the new inbound Telnet session is enabled or disabled. The default value is Enabled so that new inbound Telnet sessions can be established until there are no more sessions available. If it 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.

   - Use **Session Timeout** to specify how many minutes of inactivity occur on a Telnet session before the session is logged off.
   - You can enter any number from 1 to 160. The factory default is 5 minutes.
   - Use **Maximum Number of Sessions** to specify how many simultaneous Telnet sessions are allowed. The maximum is 5, which is also the factory default.

   The **Current Number of Sessions** field displays the number of current sessions.

4. To configure outbound Telnet settings, specify the following:

   - Select the **Allow New Telnet Sessions Disable** or **Enable** radio button.

This specifies whether the new outbound Telnet sessions are enabled or disabled. The default value is Enabled so that 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.

- Use **Session Timeout** to specify the outbound Telnet login inactivity time-out in minutes.

  The default value is 5 minutes. Valid range is 1 to 160.

- Use **Maximum Number of Sessions** to specify the maximum number of outbound Telnet sessions allowed.

  The default value is 5. The valid range is 0 to 5.

The **Current Number of Sessions** field displays the number of current sessions.

5.3.10. Configure the Console Port

To configure the console port:

Security > Access > Console Port.

1. In the **Serial Port Login Timeout (minutes)** field, specify how many minutes of inactivity 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. In the **Baud Rate (bps)** list, select the default baud rate for the serial port connection.

   You can choose from 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory default is 115200 baud.

3. In the **Login Authentication List** list, select which authentication list to use when you log in through Telnet.

The default value is defaultList.

4. In the **Enable Authentication List** list, select which authentication list to use when going into the privileged EXEC mode.

   The default value is enableList

The following table describes the nonconfigurable data that is displayed.

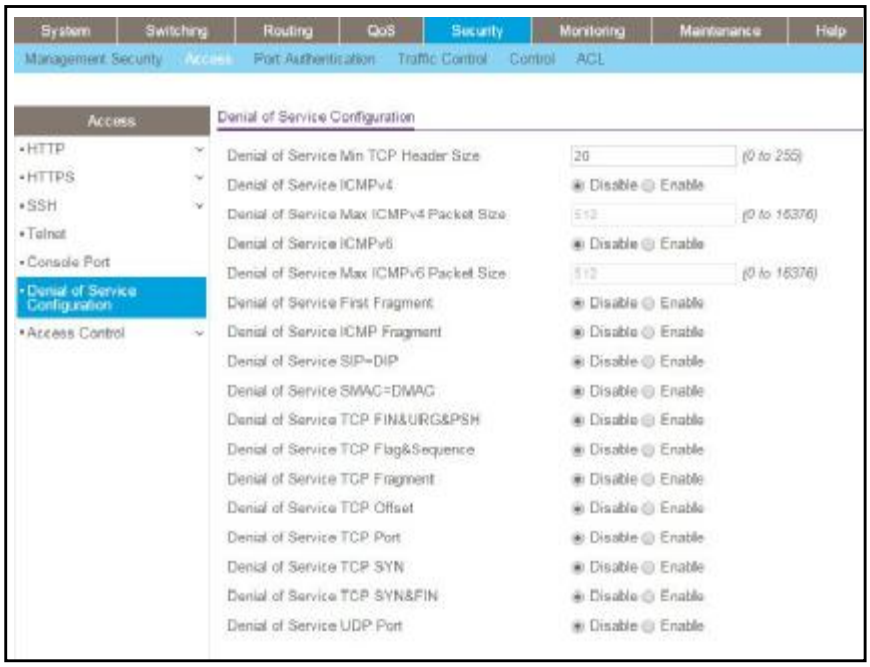
Table87. Console Port

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. It is always 1.
Parity	The parity method used on the serial port. It is always None.

5.3.11. Configure Denial of Service Settings

To configure Denial of Service settings:

Security > Denial of Service Configuration.



1. In the **Denial of Service Min TCP Header Size** field, specify the minimum TCP header size allowed.

   If DoS TCP Fragment is enabled, the switch drops these packets:

   - First TCP fragments with 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. Select the Denial of Service ICMPv4 **Disable** or **Enable** radio button.

   Enabling ICMPv4 DoS prevention causes the switch to drop ICMPv4 packets with a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 packet size. The factory default is Disable.

3. Specify the **Denial of Service Max ICMPv4 Packet Size**.

   This is the maximum ICMPv4 Pkt Size allowed. If ICMPv4 DoS prevention is enabled, the switch drops IPv4 ICMP ping packets with a size greater than the configured Max ICMPv4 packet size. Its range is 0 to 16376. The default value is 512.

4. Use **Denial of Service ICMPv6** to enable ICMPv6 DoS prevention.

   This causes the switch to drop ICMPv6 packets with a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 Pkt Size. The factory default is Disable.

5. Use **Denial of Service Max ICMPv6 Packet Size** to specify the maximum IPv6 ICMP packet size allowed.

   If ICMPv6 DoS prevention is enabled, the switch drops IPv6 ICMP ping packets with a size greater than the configured maximum ICMPv6 packet size. Its range is 0 to 16376. The default value is 512.

6. Select the Denial of Service First Fragment **Disable** or **Enable** radio button.

   This enables 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 Disable.

7. Select the Denial of Service ICMP Fragment **Disable** or **Enable** radio button.

   Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP Fragmented packets. The factory default is Disable.

8. Select the Denial of Service SIP=DIP **Disable** or **Enable** radio button.

   Enable SIP=DIP DoS prevention causes the switch to drop packets with a source IP address equal to the destination IP address. The factory default is Disable.

9. Select the Denial of Service SMAC=DMAC **Disable** or **Enable** radio button.

   Enabling SMAC=DMAC DoS prevention causes the switch to drop packets with a source MAC address equal to the destination MAC address. The factory default is Disable.

10. Select the Denial of Service TCP FIN&URG&PSH **Disable** or **Enable** radio button.

    Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets with TCP Flags FIN, URG, and PSH set and TCP Sequence Number=0. The factory default is Disable.

11. Select the Denial of Service TCP Flag&Sequence **Disable** or **Enable** radio button.

    Enabling TCP Flag DoS prevention causes the switch to drop packets with TCP control flags set to 0 and TCP sequence number set to 0. The factory default is Disable.

12. Select the Denial of Service TCP Fragment Disable or **Enable** radio button.

    Enabling TCP Fragment DoS prevention causes the switch to drop packets as follows:

First TCP fragments with a TCP payload: IP_Payload_Length - IP_Header_Size < Min_TCP_Header_Size.

The factory default is Disable.

13. Select the Denial of Service TCP Offset **Disable** or **Enable** radio button.

    Enabling TCP Offset DoS prevention causes the switch to drop packets with a TCP header Offset=1. The factory default is Disable.

14. Select the Denial of Service TCP Port **Disable** or **Enable** radio button.

    Enabling TCP Port DoS prevention causes the switch to drop packets with TCP source port equal to TCP destination port. The factory default is Disable.

15. Select the Denial of Service TCP SYN **Disable** or **Enable** radio button.

    Enabling TCP SYN DoS prevention causes the switch to drop packets with TCP flags SYN set. The factory default is Disable.

16. Select the Denial of Service TCP SYN & FIN **Disable** or **Enable** radio button.

    Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets with TCP flags SYN and FIN set. The factory default is Disable.

17. Select the **Denial of Service UDP Port Disable** or **Enable** radio button.

    Enabling UDP Port DoS prevention causes the switch to drop packets with UDP source port equal to UDP destination port. The factory default is Disable.

5.4. 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**. The port that is authenticated before permitting system access.
- **Supplicants**. The host connected to the authenticated port requesting access to the system services.
- **Authentication Server**. 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.

5.4.1. Configure Global 802.1X Settings

To configure global 802.1X settings:

Security > Port Authentication > Basic > 802.1X Configuration.

1. Select the Administrative Mode **Disable** or **Enable** radio button.

   This enables or disables 802.1X administrative mode on the switch.

   - **Enable**. Port-based authentication is permitted on the switch.

     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, select **Security > Management Security > Authentication List** and select RADIUS as method 1 for defaultList. For more information, see *Configure a Login Authentication List* on page 555.

   - **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. Select the VLAN Assignment Mode **Disable** or **Enable** radio button.

   The default value is Disable.

3. Select the EAPOL Flood Mode **Disable** or **Enable** radio button.

   The default value is Disable.

4. Use **Dynamic VLAN Creation Mode** to select **Disable** or **Enable**.

   The default value is Disable.

5. Use **Monitor Mode** to select **Disable** or **Enable**.

   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 for 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. The Authentication List field displays the authentication list that is used by 802.1X

5.4.2. Configure 802.1X Settings

You can enable or disable 802.1X access control on the system.

To configure 802.1X settings:

Security > Port Authentication > Advanced > 802.1X Configuration.

1. Select the Administrative Mode **Disable** or **Enable** radio button.

   The default value is Disable.

2. Select the VLAN Assignment Mode **Disable** or **Enable** radio button.

   The default value is Disable.

3. Select the EAPOL Flood Mode **Disable** or **Enable** radio button.

   The default value is Disable.

4. Use **Dynamic VLAN Creation Mode** to select **Disable** or **Enable**.

   The default value is Disable.

5. Use **Monitor Mode** to select **Disable** or **Enable**.

   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 for the selected login list for 802.1x port security.
7. Use **Login** to select the login list to apply to the specified user.

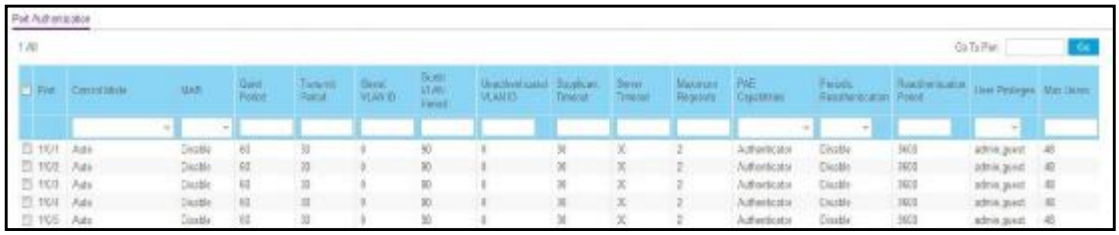
   All configured login lists are displayed. The **Authentication List** field displays the list that is used by 802.1X.

5.4.3. Configure Port Authentication

You can enable and configure port access control on one or more ports.

To configure 802.1X settings for the port:

Security > Port Authentication > Advanced > Port Authentication.



Note: Use the horizontal scroll bar at the bottom of the screen to view all the fields.

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 ports, specify the following settings:
   - **Control Mode**. Select an option for the control mode. The control mode is set only if the link status of the port is Link Up. The options are as follows:
     - **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 you 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 does 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 never acquires a supplicant. The default value is 60. Changing the value does not change the configuration until you click the **Apply** button.
   - **Transmit Period**. This input field allows you to configure the transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP request/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

does not change the configuration until the **Apply** button is clicked.

- **GuestVLAN ID**. This field allows you to configure guest VLAN ID on the interface. The valid range is 0–4093.The default value is 0. Changing the value does not change the configuration until the **Apply** button is clicked. 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 for guest VLAN authentication. The guest VLAN time-out must be a value from 1 to 300.

  The default value is 90. Changing the value does not change the configuration until the **Apply** button is clicked.
- **Unauthenticated VLAN ID**. Enter the unauthenticated VLAN ID for the selected port. The valid range is 0–4093.The default value is 0. Changing the value does not change the configuration until the **Apply** button is clicked. Enter 0 to clear the unauthenticated VLAN ID on the interface.
- **Supplicant Timeout**. 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 in the range of 1 to 65535. The default value is 30. Changing the value does not change the configuration until the **Apply** button is clicked.
- **Server Timeout**. 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 in the range of 1 to 65535. The default value is 30. Changing the value does not change the configuration until the **Apply** button is clicked.
- **Maximum Requests**. 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 retransmits an EAPOL EAP request/identity before timing out the supplicant. The maximum requests value must be in the range of 1 to 10. The default value is 2. Changing the value does not change the configuration until the **Apply** button is clicked.
- **PAE Capabilities**. Select the port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant.
- **Periodic Reauthentication**. Enable or disable reauthentication of the supplicant for the specified port. The selectable values are Enable or Disable. If the value is Enable, reauthentication occurs. Otherwise, reauthentication is not allowed. The default value is Disable. Changing the selection does not change the configuration until the **Apply** button is clicked.
- **Reauthentication Period**. Enter the reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer for 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 to 65535. The default value is 3600. Changing the value does not change the configuration until the **Apply** button is clicked.
- **User Privileges**. Add the specified user to the list of users with access to the specified port or all ports.
- **Max Users**. Enter the limit to the number of supplicants on the specified interface.

3. To begin the initialization sequence on the selected port, click the **Initialize** button.

   The initialization sequence begins.

   You can click this button only if the control mode is auto. If the button is not available, it is grayed out. Once this button is clicked, the action is immediate. You do not need to click the **Apply** button for the action to occur.

4. Click the **Reauthentication** button.

   The reauthentication sequence begins on the selected port.

   You can click this button only if the control mode is auto. If the button is not available, it is grayed out. Once you click this button, the action is immediate. You do not need to click the **Apply** button for the action to occur.

5.4.4. View the Port Summary

You can view information about the port access control settings on a specific port.

To view the port summary:

Security > Port Authentication > Advanced > Port Summary.

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

Table88. Port Summary

Field	Description
Port	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 as follows: • **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	The control mode under which the port is actually operating. Possible values are as follows: • ForceUnauthorized • ForceAuthorized • Auto • MAC Based • N/A: If the port is in detached state, it cannot participate in port access control.
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 occurs. Otherwise, reauthentication is not allowed.
Control Direction	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	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	The port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant. This field is not configurable.

Table89. Port Summary (continued)

Field	Description
Authenticator PAE State	The current state of the authenticator PAE state machine. Possible values are as follows: • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized
Backend State	The current state of the backend authentication state machine. Possible values are as follows: • Request • Response • Success • Fail • Timeout • Initialize • Idle

VLAN Assigned	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	The 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 as follows: • 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 does not occur. Otherwise, key transmission is supported on the selected port.
Session Timeout	The session rimeout 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.

Table90. Port Summary (continued)

Field	Description
Session Termination Action	The 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 as follows: • Default • Reauthenticate If the termination action is set to default, then at the end of the session, the client details are initialized. Otherwise re-authentication is attempted.
Port Status	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 is N/A because the port cannot participate in port access control.

5.4.5. View the Client Summary

To view the client summary:

Security > Port Authentication > Advanced > Client Summary.

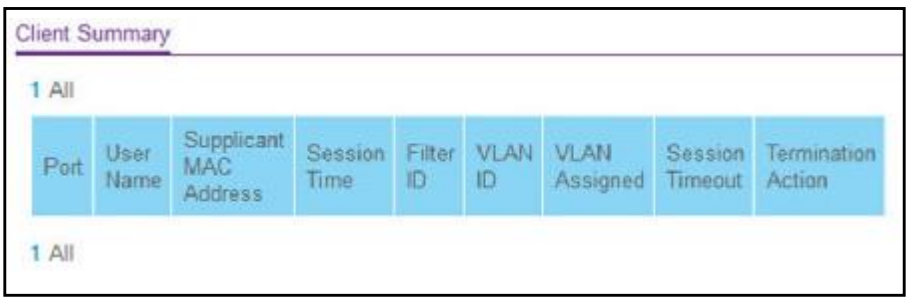


Table91. Client Summary

Field	Description
Port	The port to be displayed.
User Name	The user name representing the identity of the supplicant device.
Supplicant Mac Address	The supplicant's device MAC address.
Session Time	The time since the supplicant as logged in seconds.
Filter ID	The policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID	The VLAN ID assigned by the authenticator to the supplicant device.
VLAN Assigned	The reason for the VLAN ID assigned by the authenticator to the supplicant device.
Session Timeout	The session time-out set by the RADIUS server to the supplicant device.
Termination Action	The termination action set by the RADIUS server to the supplicant device.

5.5. Traffic Control

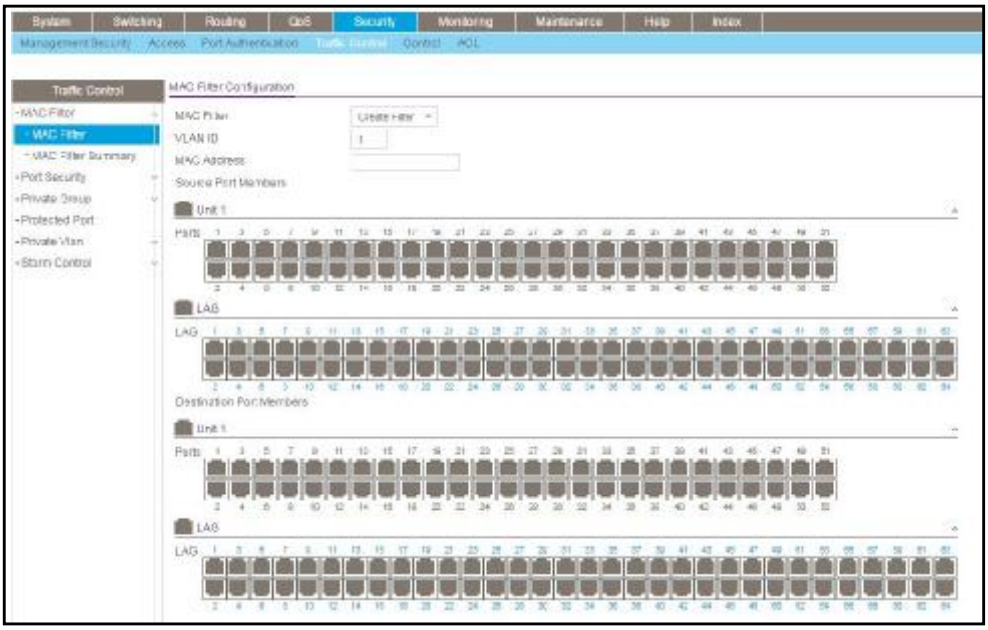
You can configure MAC filters, storm control, port security, and protected port settings.

5.5.1. Configure MAC Filtering

You can create MAC filters that limit the traffic allowed into and out of specified ports on the system.

To configure MAC filter settings:

Security > Traffic Control > MAC Filter.



This is the list of MAC address and VLAN ID pairings for all configured filters.

1. To change the port masks for an existing filter, select the entry.
2. To add a new filter, select **Create Filter** from the **MAC Filter** list.
3. From the **VLAN ID** list, select the VLAN to use with the MAC address to fully identify packets to be filtered.

   You can change this field only when **Create Filter** is selected from the **MAC Filter** list.
4. 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 select the **Create Filte**r 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
5. Use **Source Port Members** to list the ports to be 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 is dropped.
6. Use **Destination Port Members** to list the ports to be included in the outbound filter.

   Packets with the MAC address and VLAN ID you selected are transmitted only from ports that are in the list. Destination ports can be included only in the multicast filter.
7. To delete a configured MAC filter, select it, and then click the **Delete** button.
8. Click the **Apply** button.

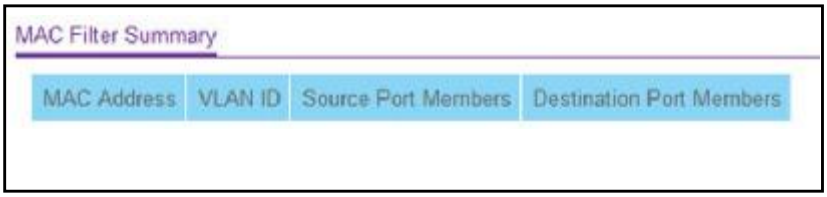
   The updated configuration is sent to the switch. Configuration changes take effect

immediately.

5.5.2. MAC Filter Summary

To view the MAC filter summary:

Security > Traffic Control > MAC Filter > MAC Filter Summary.



The following table describes the information displayed on the screen.

Table92. MAC Filter Summary

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.

Table93. MAC Filter Summary (continued)

Field	Description
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.

5.5.3. Port Security

You can configure port security settings.

5.5.4. Configure the Global Port Security Mode

You can 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 configure the global port security mode:

Security > Traffic Control > Port Security > Port Administration.

1. Select the Port Security Mode **Disable** or **Enable** radio button.

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.

Table94. Port Security Violations

Field	Description
Port	The physical interface.
Last Violation MAC	The source MAC address of the last packet that was discarded at a locked port.
VLAN ID	The VLAN ID corresponding to the last violation MAC address.

5.5.5. Configure a Port Security Interface

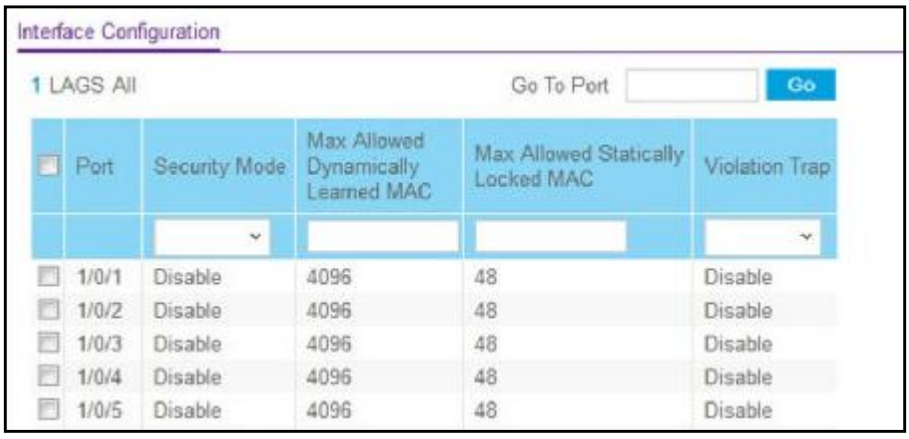
A MAC address can be defined as allowable by one of two methods: dynamically or statically. Both methods are used concurrently when a port is locked.

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 was not 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 configure port security settings:

Security > Traffic Control > Port Security > Interface Configuration.



1. 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.

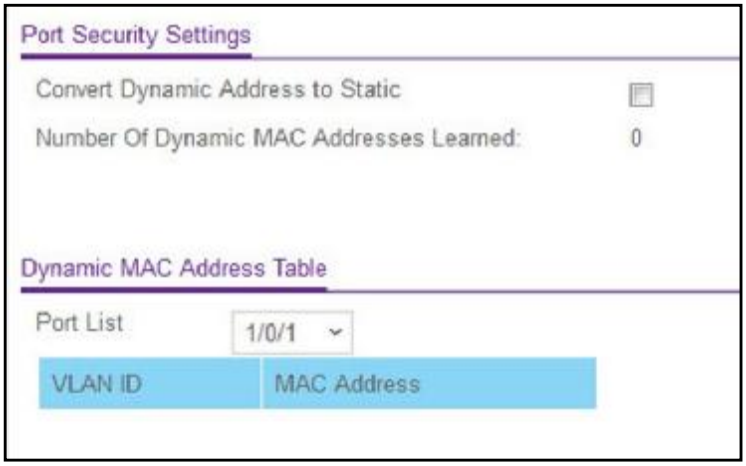
2. Specify the following settings:
   - **Security Mode**. Enables or disables the port security feature for the selected interface.
   - **Max Allowed Dynamically Learned MAC**. Sets the maximum number of dynamically learned MAC addresses on the selected interface.
   - **Max Allowed Statically Locked 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.

5.5.6. Convert Learned MAC Addresses to Static Addresses

You can convert a dynamically learned MAC address to a statically locked address.

To convert learned MAC addresses:

Security > Traffic Control > Port Security > Dynamic MAC Address.



1. Use **Port List** to select the physical interface.
2. Use the **Convert Dynamic Address to Static** check box to convert a dynamically learned MAC address to a statically locked address.

   The dynamic MAC address entries are converted to static MAC address entries in a numerically ascending order until the static limit is reached.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table shows the MAC addresses and their associated VLANs learned on the selected port. Use the **Port List** menu to select the interface.

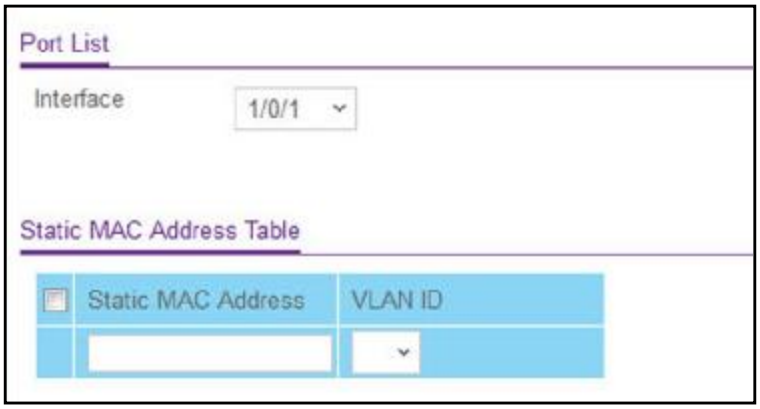
Table95. Dynamic MAC Address

Field	Description
Number of Dynamic MAC Addresses Learned	The number of dynamically learned MAC addresses on a specific port.
VLAN ID	The VLAN ID corresponding to the MAC address.
MAC Address	The MAC addresses learned on a specific port.

5.5.7. Configure a Static MAC Address

To configure a static MAC address:

Security > Traffic Control > Port Security > Static MAC Address.



1. Use **Interface** to select the physical interface.
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 the **Add** button.

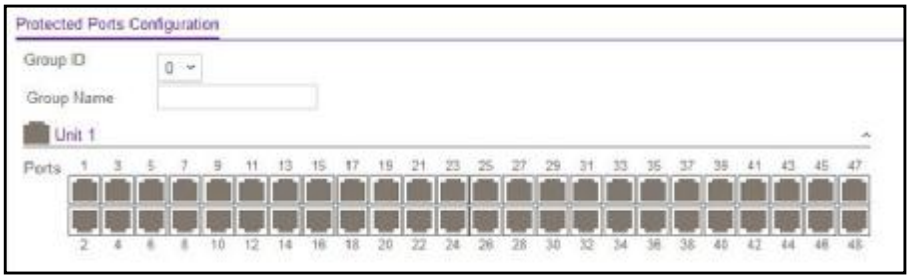
   The static MAC address is added to the switch.
5. To delete a existing static MAC address from the switch, click the **Delete** button.

5.5.8. Configure Protected Ports

If a port is configured as protected, it does not forward traffic to any other protected port on the switch, but it does forward traffic to unprotected ports. You can configure the ports as protected or unprotected. You need read-write access privileges to modify the configuration.

To configure protected ports:

Security > Traffic Control > Protected Ports.



1. In the **Group ID** list, select 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 list includes all the possible protected port group IDs supported for the current platform. The valid range of the gGroup 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. Select the check 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 the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

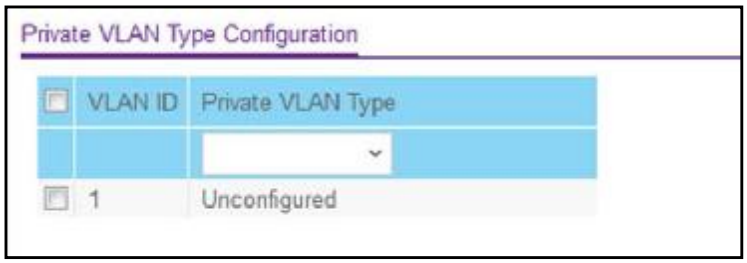
To refresh the screen with the latest information on the switch, click the **Update** button.

5.5.9. Configure a 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.

To configure a private VLAN type:

Security > Traffic Control > Private VLAN > Private VLAN Type Configuration.



1. Use **Private VLAN Type** to select the type of private VLAN.

   The factory default is Unconfigured.

2. Click the **Apply** button.

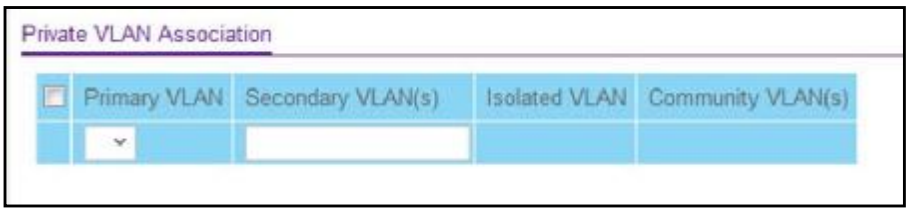
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

   The VLAN ID field specifies the VLAN ID for which the private VLAN type is being set. The factory default is Unconfigured.

5.5.10. Configure Private VLAN Association Settings

To configure private VLAN association:

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 with 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 with the selected primary VLAN.

3. To delete the IP subnet-based VLAN from the switch, click the **Delete** button.
4. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

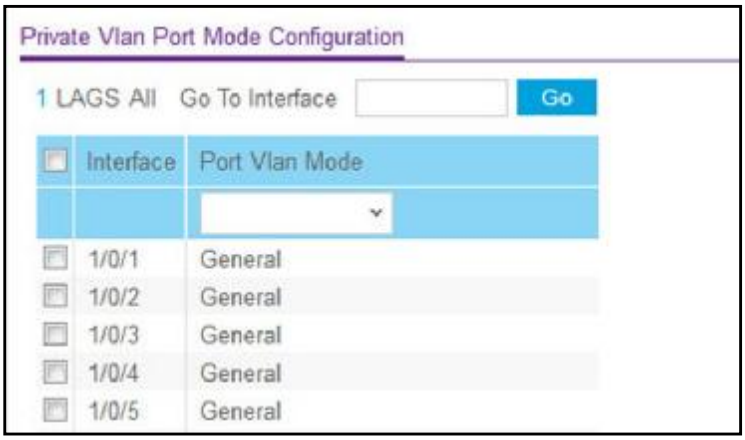
Table96. Private VLAN Association

Field	Description
Isolated VLAN	The isolated VLAN associated with the selected primary VLAN.
Community VLAN(s)	The list of community VLANs associated with the selected primary VLAN.

5.5.11. Configure the Private VLAN Port Mode

To configure the private VLAN port mode:

Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration.



1. Use **Switch Port Mode** to select the switch port mode.
   - **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.

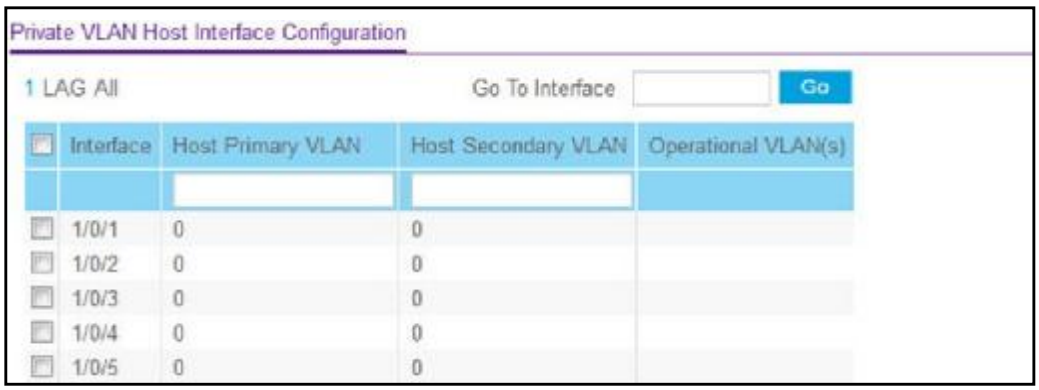
   The factory default is General.
2. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

5.5.12. Configure a Private VLAN Host Interface

To configure a private VLAN host interface:

Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration.



1. In the **Host Primary VLAN** field, 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. To delete the IP subnet-based VLAN from the switch, click the **Delete** button.
4. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

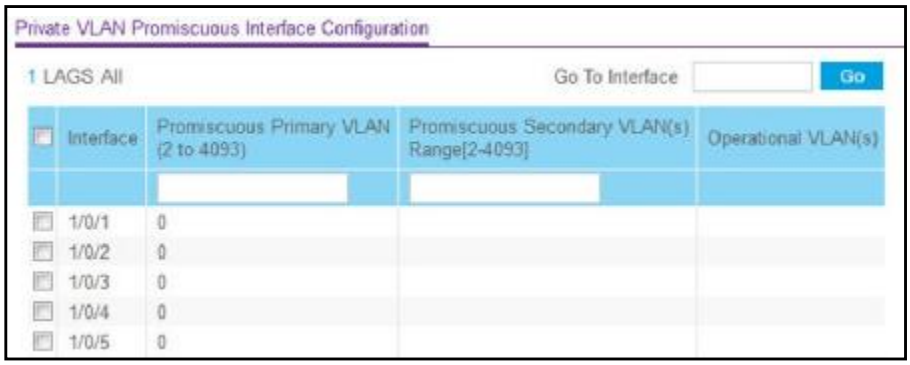
Table97. Private VLAN Host Interface Configuration

Field	Description
Interface	Select the physical or LAG interface.
Operational VLAN(s)	The operational VLANs.

5.5.13. Configure a Private VLAN Promiscuous Interface

To configure a private VLAN promiscuous interface:

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, such as 10. You can specify the VLAN range values separated by a hyphen, for example, 10-13. You can specify the combination of both separated by commas, for example: 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 replaces the configured secondary VLAN list in the association.

3. Click the **Delete** button to delete the IP subnet-based VLAN from the switch.
4. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

Table98. Private VLAN Promiscuous Interface Configuration

Field	Description
Interface	Select the physical or LAG interface
Operational VLAN(s)	The operational VLANs.

5.5.14. 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.

5.5.15. Configure Global Storm Control Settings

To configure global storm control settings:

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 screen.

1. Select the Broadcast Storm Control All **Disable** or **Enable** radio button.

   This enables or disables Broadcast Storm Recovery mode on all ports. When you specify Enable and the broadcast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. The factory default is Enable.

2. Select the Multicast Storm Control All **Disable** or **Enable** radio button.

   This enables or disables Multicast Storm Recovery mode on all ports. When you specify Enable, and the multicast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. The factory default is Disable.

3. Select the Unknown Unicast Storm Control All **Disable** or **Enable** radio button.

   This enables or disables Unicast Storm Recovery mode on all ports. When you specify Enable, and the unicast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. The factory default is Disable.

5.5.16. Configure a Storm Control Interface

To configure a storm control interface:

Security > Traffic Control > Storm Control > Storm Control Interface Configuration.

The following table describes the nonconfigurable information displayed on the screen.

Table99. 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 list. 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 Disable.
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. 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 Disable.

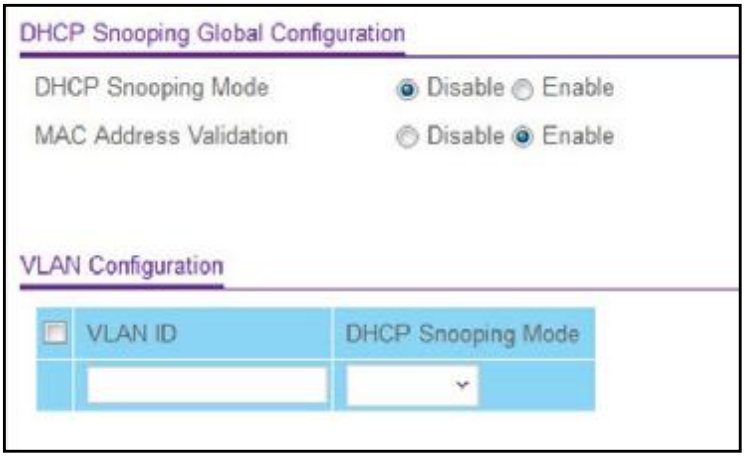
5.6. DHCP Snooping

You can configure DHCP snooping global and interface settings.

5.6.1. Configure DHCP Snooping Global Settings

To configure DHCP snooping global settings:

Security > Control > DHCP Snooping > Global Configuration.



1. Select the DHCP Snooping Mode **Disable** or **Enable** radio button.

   The factory default is Disable.

2. Select the MAC Address Validation **Disable** or **Enable** radio button.

   This enables or disables the validation of sender MAC address for DHCP snooping. The factory default is Enable.

3. Use **VLAN ID** to enter the VLAN for which the DHCP snooping mode is to be enabled.
4. Use **DHCP Snooping Mode** to enable or disable the DHCP snooping feature for the

entered VLAN.

The factory default is Disable.

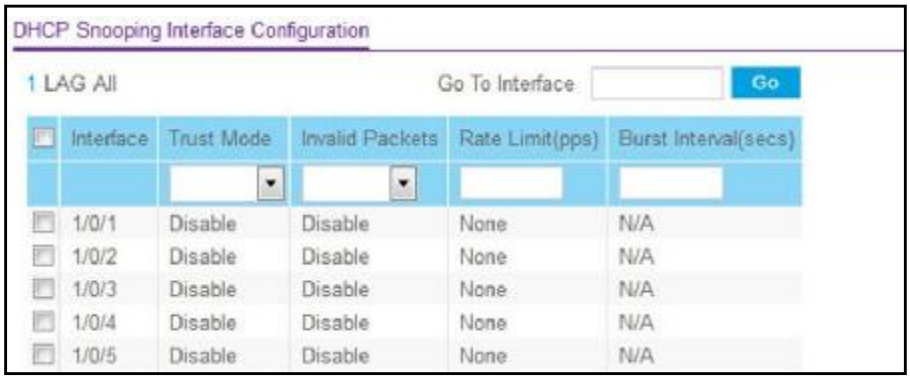
5. Click the **Apply** button.

   The updated configuration is sent to the switch. These changes are not retained across a power cycle unless a save configuration is performed.

5.6.2. Configure a DHCP Snooping Interface

To configure a DHCP snooping interface:

Security > Control > DHCP Snooping > Interface Configuration.



1. Use the **Interface** check boxes to select the interface.
2. If **Trust Mode** is enabled, DHCP snooping application considers the port as trusted.

   The factory default is Disable.

3. If **Invalid Packets** is enabled, DHCP snooping application logs invalid packets on this interface.

   The factory default is Disable.

4. Use **Rate Limit (pps)** to specify rate limit value for DHCP snooping purposes.

   If the incoming rate of DHCP packets exceeds the value of this for consecutive burst interval seconds, the port is shut down. 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.

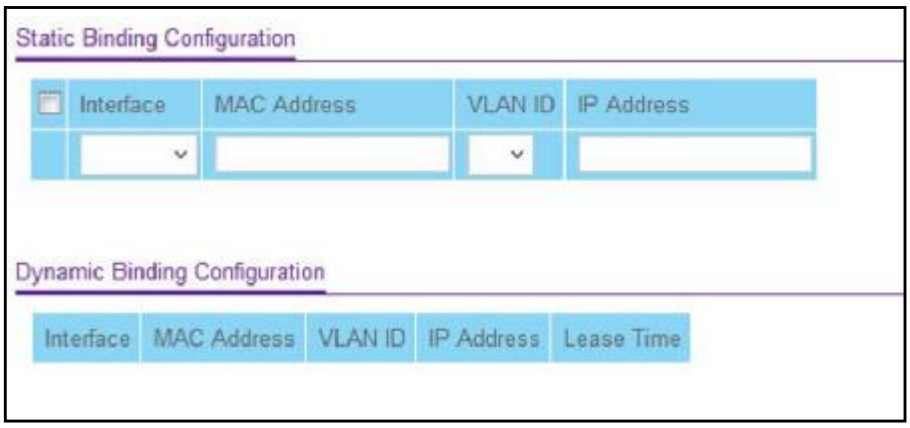
5. Use **Burst Interval (secs)** to specify the burst interval value for rate limiting purpose on this interface.

   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 –1, which means N/A. The range of Burst Interval is 1 to 15.

5.6.3. Configure DHCP SnoopingBinding

To configure snooping binding:

Security > Control > DHCP Snooping > Binding Configuration.



1. To configure static binding, specify the following:
   a. Use the **Interface** check boxes to select the interface.
   b. Use **MAC Address** to specify the MAC address for the binding entry to be added.

      This is the key to the binding database.
   c. Use **VLAN ID** to select the VLAN from the list for the binding rule.

      The range of the VLAN ID is 1 to 4093.
   d. Use **IP Address** to specify valid IP address for the binding rule.
   e. Click the **Add** button.

      The DHCP snooping binding entry is added into the database.
   f. To delete selected static entries from the database, click the **Delete** button.
2. To configure dynamic binding, specify the following:
   a. Use the **Interface** check boxes to select the interface.
   b. Use **MAC Address** to display the MAC address for the binding in the binding database.
   c. 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.
   d. **IP Address**. Displays IP address for the binding entry in the binding database.
   e. **Lease Time**. The remaining lease time for the dynamic entries.
   f. To delete all DHCP snooping binding entries, click the **Clear** button.

5.6.4. Configure Snooping Persistent Settings

To configure snooping persistent settings:

Security > Control > DHCP Snooping > Persistent Configuration.

1. Select the Store **Local** or **Remote** radio button.

   Selecting **Local** disables the remote fields **Remote File Name** and **Remote IP Address**.

2. If you are selected Remote, do the following:

   a. In the **Remote IP Address** field, type the remote IP address on which the snooping database is stored.

   b. In the **Remote File Name** field, enter the remote file name to store the database.

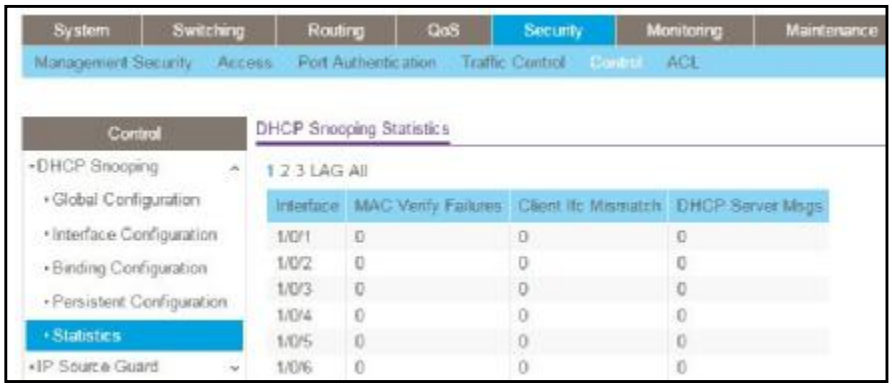
3. In the **Write Delay** field, enter the maximum write time to write the database into local or remote.

   The range is 15 to 86400.

5.6.5. View DHCP SnoopingStatistics

To view DHCP snooping statistics:

Security > Control > DHCP Snooping > Statistics.



To clear all interfaces statistics, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the DHCP snooping statistics.

Table100. DHCP Snooping Statistics

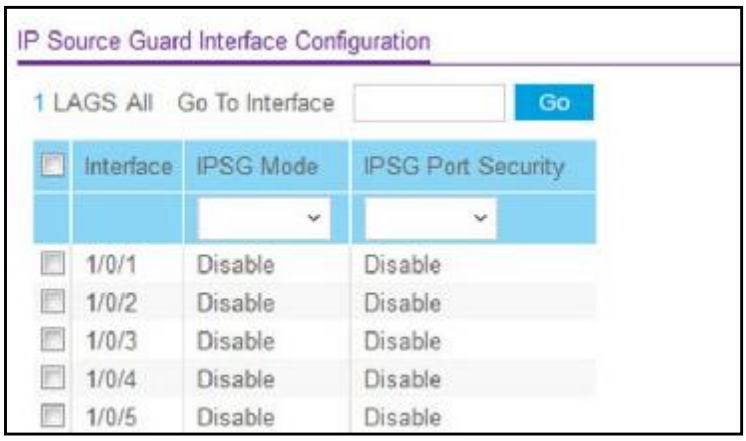
Field	Description
Interface	The untrusted and snooping-enabled interface for which statistics are to be displayed.
MAC Verify Failures	Number of packets that were dropped by DHCP snooping because there is no matching DHCP snooping binding entry found.
Client Ifc Mismatch	The number of DHCP messages that are dropped based on source MAC address and client HW address verification.
DHCP Server Msgs	The number of server messages that are dropped on an untrusted port.

5.6.6. Configure an IP Source Guard Interface

You can configure IP source guard (IPSG) on each interface. IPSG is a security feature that filters IP packets based on source ID. This feature helps protect the network from attacks that use IP address spoofing to compromise or overwhelm the network. The source ID can be either the source IP address or a source IP address and source MAC address pair. The DHCP snooping bindings database, along with IPSG entries in the database, identify authorized source IDs. If you enable IPSG on a port where DHCP snooping is disabled or where DHCP snooping is enabled but the port is trusted, all IP traffic received on that port is dropped depending on the admin-configured IPSG entries. Additionally, IPSG interacts with port security, also known as port MAC locking, to enforce the source MAC address in received packets. Port security controls source MAC address learning in the Layer 2 forwarding database (the MAC address table). When a frame is received with a previously unlearned source MAC address, port security queries the IPSG feature to determine whether the MAC address belongs to a valid binding.

To configure IP Source Guard Interface settings:

Security > Control > IP Source Guard > Interface Configuration.



1. Use the **Interface** check boxes to select the interface.
2. In the **IPSG Mode** list, select **Disable** or **Enable**.

This sets the administrative mode of IPSG on the interface. When IPSG mode is enabled, the sender IP address on this interface is validated against the DHCP snooping binding database. If IPSG is enabled, packets are not forwarded if the sender IP address is not in DHCP snooping binding database. The factory default is Disable.

3. In the **IPSG Port Security** list, select **Disable** or **Enable**.

   This enables or disables the administrative mode of IPSG port security on the selected interface. When this is enabled, the packets are not forwarded if the sender MAC address is not in forwarding database (FDB) table or the DHCP snooping binding database. To enforce filtering based on MAC address other required configurations are as follows:

   - Enable port-security globally.
   - Enable port-security on the interface level.

   IPSG port security cannot be enabled if IPSG is disabled. The factory default is Disable. Also, you cannot turn off IPv6SG port security while IPv6SG is enabled.

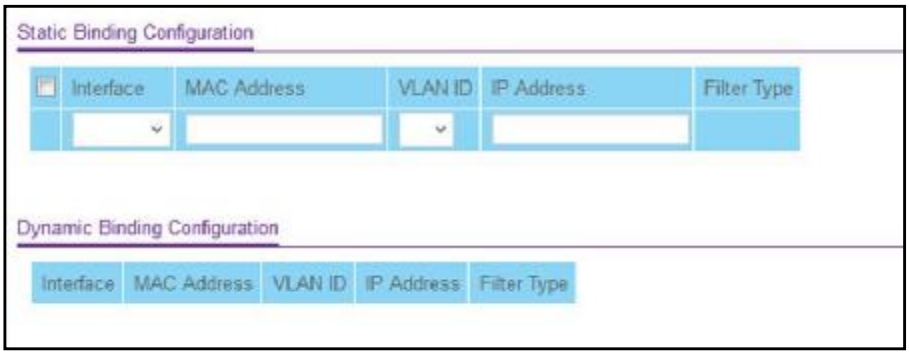
4. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

5.6.7. Configure IP Source Guard Binding Settings

To configure IP source guard static binding settings:

Security > Control > IP Source Guard > Binding Configuration.



1. Use the **Interface** check boxes to select the interface.
2. In the **MAC Address** field, type the MAC address for the binding.
3. In the **VLAN ID** list, select the VLAN for the binding rule.
4. In the **IP Address** field, specify valid IP address for the binding rule.
5. Click the **Add** button.

   The IPSG static binding entry is added into the database.

6. To delete selected static entries from the database, click the **Delete** button.

To clear all the dynamic binding entries, click the **Clear** button.

The following table describes the nonconfigurable IP Source Guard Dynamic Binding Configuration information that is displayed.

Table101. IP Source Guard Dynamic Binding Configuration

Field	Description
Interface	The interface for which to add a binding into the IPSG database.
MAC Address	The MAC address for the binding entry.
VLAN ID	The VLAN for the binding entry.

Table102. IP Source Guard Dynamic Binding Configuration (continued)

Field	Description
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, and the other is source IP address and MAC address filter type.

5.6.8. Configure Dynamic ARPInspection

To configure dynamic ARP inspection (DAI):

Security > Control > Dynamic ARP Inspection > DAI Configuration.

1. Select the Validate Source MAC **Disable** or **Enable** radio button.

   This specifies the DAI source MAC validation mode for the switch. If you select **Enable**, sender MAC validation for the ARP packets is enabled. The factory default is Disable.

2. Select the Validate Destination **MAC Disable** or **Enable** radio button

   This specifies the DAI destination MAC validation mode for the switch. If you select **Enable**, destination MAC validation for the ARP response packets is enabled. The factory default is Disable.

3. Select the Validate IP **Disable** or **Enable** radio button.

   This specifies the DAI IP validation mode for the switch. If you select **Enable**, IP address validation for the ARP packets is enabled. The factory default is Disable.

5.6.9. Configure a DAIVLAN

To configure a DAI VLAN:

Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration.

1. Use the **VLAN ID** check boxes to select the DAI capable VLANs.
2. In the **Admin Mode** list, select **Enable** or **Disable**.

   This indicates whether the dynamic ARP inspection is enabled on this VLAN. If this is set to **Enable**, then dynamic ARP inspection is enabled. If this 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 is set to **Enable,** invalid ARP packets information is logged. If it 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 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.

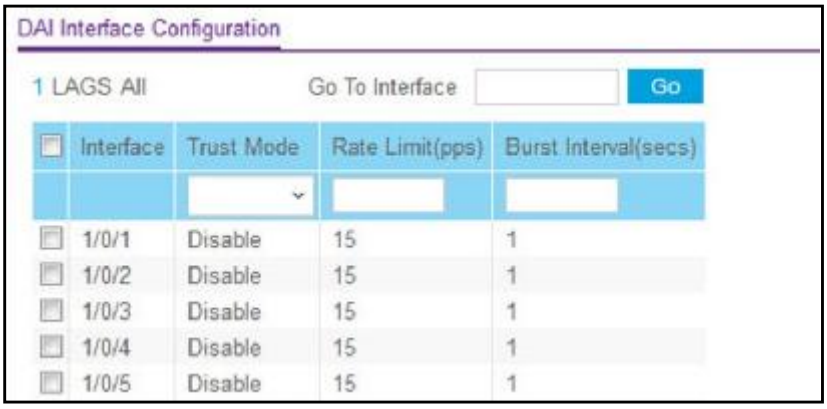
   If the flag is enabled then the ARP packet is validated by the ARP ACL rules only. If the flag is disabled then the ARP packet needs further validation by using the DHCP snooping entries. The factory default is **Disable**.
6. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

5.6.10. Configure the DAI Interface

To configure the DAI interface:

Security > Control > Dynamic ARP Inspection > DAI Interface Configuration.



1. Use the **Interface** check boxes to select the physical interface.
2. Use **Trust Mode** to indicate whether the interface is trusted for dynamic ARP inspection purposes.

   If this is set to Enable, the interface is trusted. ARP packets coming to this interface are forwarded without checking. If this is set to Disable, the interface is not trusted. ARP packets coming to this interface are subjected to ARP inspection. The factory default is Disable.
3. Use **Rate Limit (pps)** to specify rate limit value for dynamic ARP inspection purpose.

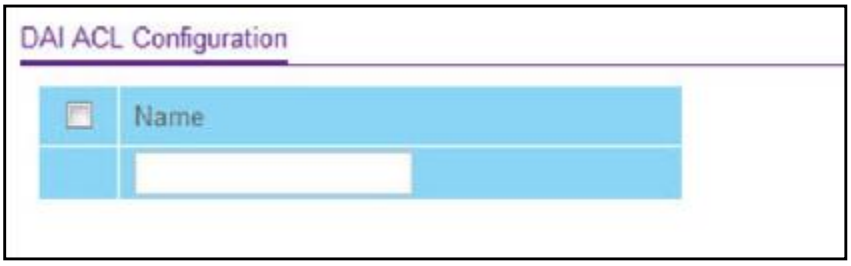
   If the incoming rate of ARP packets exceeds the value of this for consecutive burst interval seconds, ARP packets are dropped. If this value is N/A, there is no limit. The

   value can be set to –1, which means N/A. The range is 0– 300. The factory default is 15 pps (packets per second).
4. Use **Burst Interval (secs)** to specify the burst interval value for rate limiting purposes 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.

5.6.11. Configure a DAI ACL

To configure a DAI ACL:

Security > Control > Dynamic ARP Inspection > DAI ACL Configuration.



1. Use **Name** to create an ARP ACL for DAI.
2. Click the **Add** button.

   The DAI ACL is added to the switch configuration.

3. To remove the currently selected DAI ACL from the switch configuration, click the **Delete** button.

5.6.12. Configure a DAI ACL Rule

To configure a DAI ACL rule:

Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration.

1. In the **ACL Name** field, select the DAI ARP ACL.
2. Click the **Add** button.

   The rule is added to the selected ACL.
3. To remove the currently selected rule from the selected ACL, click the **Delete** button.

The following table describes the nonconfigurable information displayed on the screen.

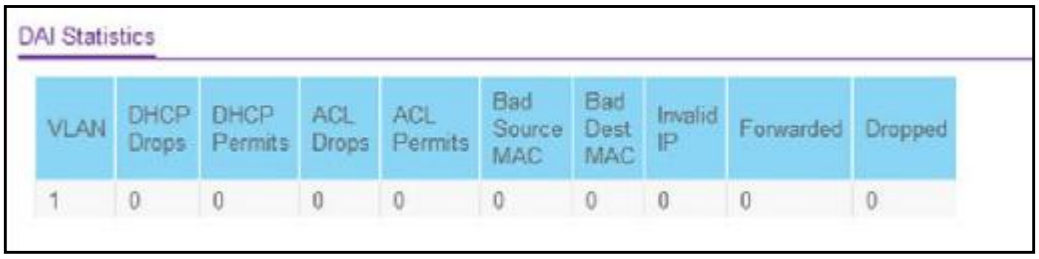
Table103. DAI ACL Rule Configuration

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.

5.6.13. View DAI Statistics

To view the DAI statistics:

Security > Control > Dynamic ARP Inspection > DAI Statistics.



To clear the DAI statistics, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable information displayed on the screen.

Table104. 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 because there is no matching DHCP snooping binding entry found.
DHCP Permits	Number of ARP packets that were forwarded by DAI because there is a matching DHCP snooping binding entry found.
ACL Drops	Number of ARP packets that were dropped by DAI because 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 because there is a matching ARP ACL rule found for this VLAN.
Bad Source MAC	Number of ARP packets that were dropped by DAI because the sender MAC address in ARP packets didn't match the source MAC in Ethernet header.
Bad Dest MAC	Number of ARP packets that were dropped by DAI because the target MAC address in ARP reply packets didn't match the destination MAC in Ethernet header.
Invalid IP	Number of ARP packets that were dropped by DAI because the sender IP address in ARP packets or the target IP address in ARP reply packets 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.

Table105. Storm Control Interface Configuration (continued)

Field	Description
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.

5.7. Configure Access Control Lists

Access control lists (ACLs) ensure that only authorized users can access 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.

5.7.1. Configure a Basic MAC ACL

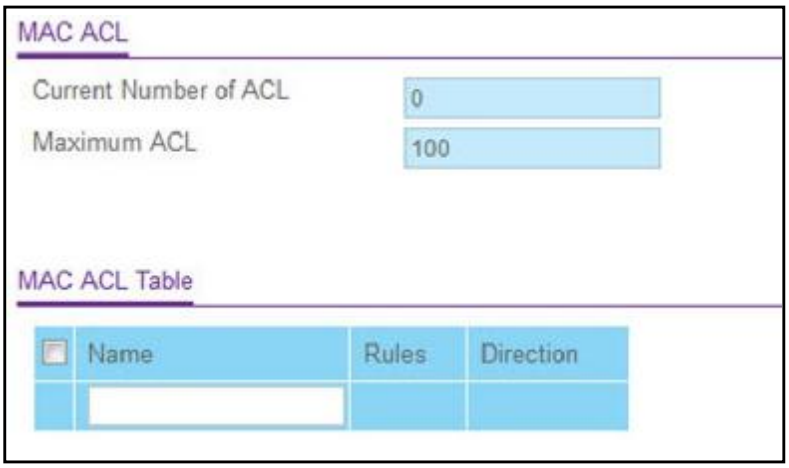
A MAC ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken, and the additional rules are not checked for a match. Rules for the MAC ACL are specified/created using the MAC ACL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

There are multiple steps involved in defining a MAC ACL and applying it to the switch:

1. Create the ACL Name.
2. Create rules for the ACL.
3. Assign the ACL by its name to a port.
4. Optionally, use the *View or Delete MAC ACL Bindings in the MAC Binding Table* screen to view the configurations.

To configure a MAC ACL:

Security > ACL > Basic > MAC ACL.



The MAC ACL screen 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.

1. In the **Name** field, specify a name for the MAC ACL.

   The name string can include alphabetic, numeric, hyphen, underscore, or space characters only. The name must start with an alphabetic character.

   Each configured ACL displays the following information:

   - **Rules**. The number of rules currently configured for the MAC ACL.
   - **Direction**. The direction of packet traffic affected by the MAC ACL, which can be

Inbound or blank.

2. Click the **Add** button.

   The MAC ACL is added to the switch configuration.

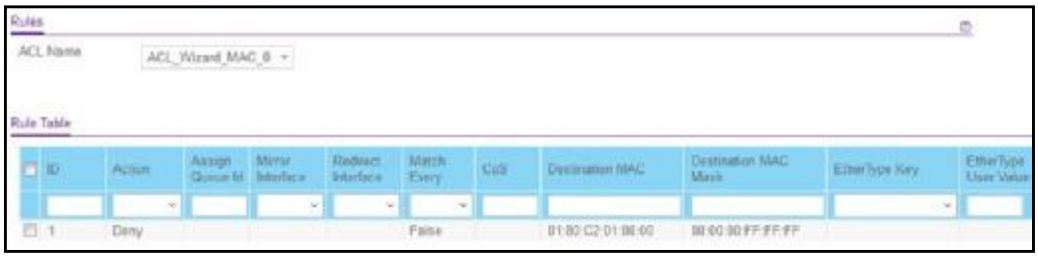
3. To change the name of the MAC ACL, in the **Name** field, update the name, then click the **Apply** button.
4. To delete the selected MAC ACL, click the **Delete** button.

5.7.2. Configure MAC ACL Rules

You can 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 configure MAC ACL rules:

Security > ACL> Basic > MAC Rules.



1. Use **ID** to enter a whole number in the range of 1 to 1023 to identify the rule.
2. Use **Action** to specify what action is 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 as follows:

   - **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 specify 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 can 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 can 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 as follows:

    - 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 you 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. Use **Logging** to enable or disable 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 causes 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. Use **Rate Limit Conform Data Rate** to specify the value of the conforming data rate of MAC ACL rule.

    Valid values are 1 to 4294967295 in Kbps.

17. Use **Rate Limit Burst Size** to specify the burst size of MAC ACL rule.

    Valid values are 1 to 128 in Kbytes.

18. Use **Time Range** to enter the name of the time range associated with the MAC ACL rule.

    The **Rule Status** displays if the ACL rule is active or inactive. If this field is blank, no timer schedules are assigned to the rule.

19. To delete a rule, select the check box associated with the rule and click the **Delete** button.
20. To change a rule, select the check box associated with the rule and change the desired fields.
21. Click the **Apply** button.

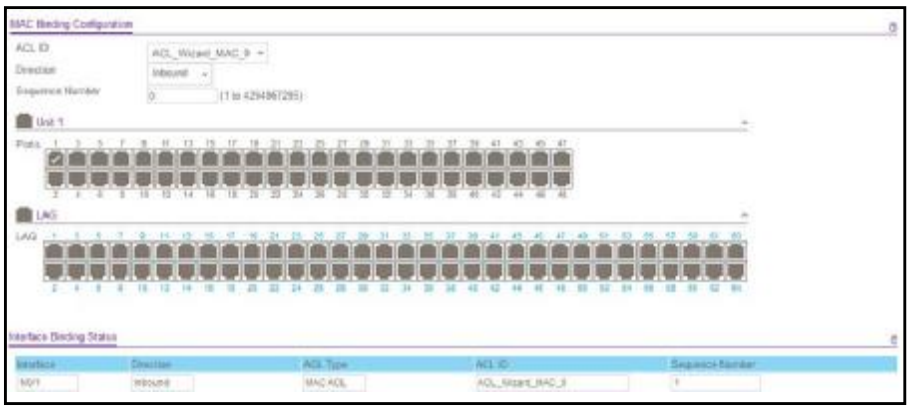
    The updated configuration is sent to the switch. Configuration changes take effect immediately.

5.7.3. Configure MAC Binding

When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface. Use the MAC Binding Configuration screen to assign MAC ACL lists to ACL priorities and interfaces.

To configure MAC binding:

Security > ACL > Basic > MAC Binding Configuration.



1. Select a MAC ACL from the **ACL ID** list.

You can select one and bind it to the interfaces.

The packet filtering **Direction** for ACL is Inbound, which means the MAC ACL rules are applied to traffic entering the port.

2. Specify an optional **Sequence Number** to indicate the order of this access list relative to other access lists already assigned to this interface and direction.

   A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1–4294967295.

3. The **Port Selection Table** provides a list of all available valid interfaces for ACL binding. All nonrouting physical interfaces VLAN interface and interfaces participating in LAGs are listed.
   - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that an X appears in the box.
   - To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. An X in the box indicates that the ACL is applied to the interface.
4. Click the **Apply** button to save any changes to the running configuration.

The following table describes the information displayed in the **Interface Binding Status**.

Table106. Interface Binding Status

Field	Description
Interface	The interface of the ACL assigned.
Direction	Displays selected packet filtering direction for ACL.
ACL Type	The type of ACL assigned to selected interface and direction.
ACL ID	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	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to selected interface and direction.

5.7.4. View or Delete MAC ACL Bindings in the MAC Binding Table

You can view or delete the MAC ACL bindings in the MAC Binding Table.

To view or delete MAC ACL bindings:

Security > ACL > Basic > MAC Binding Table.

To delete a MAC ACL-to-interface binding, select the check box next to the interface and click the **Delete** button.

The following table describes the information displayed in the MAC Binding Table.

Table107. MAC Binding Table

Field	Description
Interface	The interface of the ACL assigned.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to selected interface and direction.
ACL ID	The ACL name identifying the ACL assigned to selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to selected interface and direction.

5.7.5. Configure an IP ACL

An IP or IPv6 ACL consists of a set of rules that 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. You must specify the interfaces to which an IP ACL applies, as well as whether it applies to inbound or outbound traffic. Rules for the IP ACL are specified or created using the IPv6 ACL Rule Configuration screen.

To configure an IP ACL:

Security > ACL > Advanced > IP ACL.

The IP ACL screen 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.

The **Current Number of ACL** field displays the current number of the all ACLs configured on the switch.

The **Maximum ACL** displays the maximum number of IP ACL can be configured on the switch, depending on the hardware.

1. 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 that includes up to 31 alphanumeric characters in length. The name must start with an alphabetic character.

   Each configured ACL displays the following information:

   - **Rules**. 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.
2. To delete an IP ACL, select the check box next to the IP ACL ID field, then click the **Delete** button.
3. Click the **Add** button.

   The IP ACL is added to the switch configuration.
4. Click the **Apply** button.

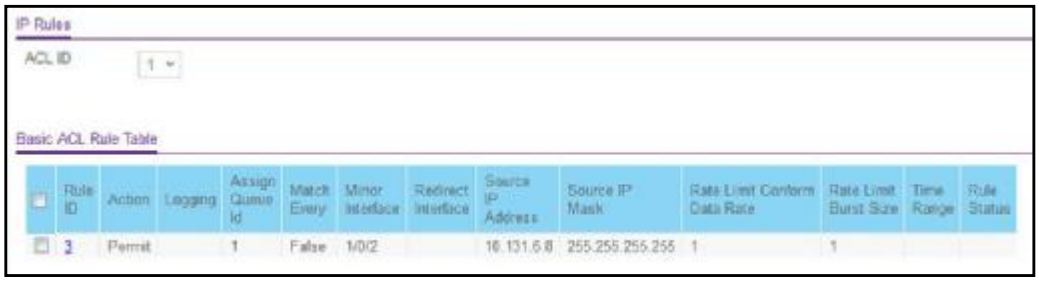
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

5.7.6. Configure Rules for an IP ACL

You can display the rules for the IP access control lists (ACL) that you created. 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 configure rules for an IP ACL:
Security > ACL > Advanced > IP Rules.



1. To add an IP ACL rule, select the **ACL ID**, complete the fields described in the following list, and click the **Add** button.

   (Displays only ACL IDs from 1 to 99.)

   - **Rule ID.** Enter a whole number in the range of 1 to 1023 that is used to identify the rule. An IP ACL can have up to 1023 rules.
   - **Action**. Specify what action is 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 causes 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**. 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 the action.
   - **Match Every.** Select **True** or **False**. True signifies that all packets must match the selected IP ACL and rule and are either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered. To configure specific match criteria for the rule, remove the rule and recreate it, or reconfigure Match Every to False for the other match criteria to be visible.
   - **Mirror Interface.** 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**. 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 the 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 rule check box, and then click the **Delete** button.
3. To update an IP ACL rule, select the rule check box, update the desired fields, and then click the **Apply** button.

   You cannot modify the Rule ID of an existing IP rule.
4. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.
5. To modify an existing IP extended ACL rule, click the **Rule ID**.

   The number is a hyperlink to the Extended ACL Rule Configuration screen.

5.7.7. Configure Rules for an Extended IP ACL

You can view the rules for the IP access control lists that you created. 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 configure rules for an extended IP ACL:

Security > ACL > Advanced > IP Extended Rules.

1. **ACL ID/Name** - 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 is used to identify the rule.

   An IP ACL can have up to 1023 rules.
3. In the **Action** list, specify the action to take if a packet matches the rule's criteria.

The choices are Permit or Deny.

4. Set **Logging** to **Enable**.

   This enables logging for this ACL rule (subject to resource availability in the device). If the access list trap flag is also enabled, this causes 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. In the **Match Every** list, select **True** or **False**.

   True signifies that all packets must match the selected IP ACL and rule and are either permitted or denied. In this case, since all packets match the rule, the option of

   configuring other match criteria is not offered. To configure specific match criteria for the rule, remove the rule and recreate it, or reconfigure **Match Every** to False for the other match criteria to be visible.

9. Use 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 can be set separately. The possible values are as follows:

    - **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 wildcard mask

to apply this criteria. If this field is left empty, it means *any*.

b. When you select the **Host** option, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means *any*.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard 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 values can range 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 are a part of the Layer 4 port range. If these fields are left empty, it means *any*.

    The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard 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 wildcard mask.

    This is 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 wildcard mask to apply this criteria.

If these fields are left empty, it means *any*.

18. When you select the **Host** option, the wildcard 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:

    - **Equa**l. 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 values can range 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 starting port, destination L4 ending port, and all ports in between are a part of the Layer 4 port range. If these fields are left empty, it means *any*.

23. **IGMP Type** - When the IGMP type is specified, the IP ACL rule matches 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 the specified ICMP message type. Possible type numbers are in the range from 0 to 255.

- When the ICMP Code option is specified, IP ACL rule matches 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. The ICMP message is decoded into the 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.

    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 6 bits of the service type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 63. To select the IP DSC, select one of the

      DSCP keywords from the list. If a value is to be selected by specifying its numeric value, then select **Other** and a field displays where you can enter numeric value of the DSCP.
    - **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 8 bits of the service type octet in the IP header. The TOS Bits value is a hexadecimal number from 00 to 09 and to aa 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** - Specify the conforming data rate of IP ACL rule.

    Valid values are 1 to 4294967295 in Kbps.

27. **Rate Limit Burst Size** - Specify the burst size of the IP ACL rule. Valid values are 1 to 128 in Kbytes.

28. **Time Range** - Name of the time range associated with the IP extended ACL rule.

    The **Rule Status** field displays if the ACL rule is active or inactive. Blank means that no timer schedules are assigned to the rule.

29. 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. Click the **Add** button on the IP Extended Rules screen.

30. For standard ACL Rule Configuration (1–99), click the **Add** button on the IP Rules screen.

31. To delete an IP ACL rule, select the rule's check box, and then click the **Delete** button.

5.7.8. Configure IPv6 ACL

An IP or IPv6 ACL consists of a set of rules that 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 screen the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or outbound traffic.

To configure IPv6 ACL:

Security > ACL > Advanced > IPv6 ACL.

1. Specify the **IPv6 ACL**.

   This is the IPv6 ACL name string, which includes up to 31 alphanumeric characters only. The name must start with an alphabetic character.

2. Click the **Add** button.

   The IPv6 ACL is added to the switch configuration.

3. To remove the currently selected IPv6 ACL from the switch configuration, click the **Delete** button.

4. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

Table108. IPv6 ACL

Field	Description
Current Number of ACL	The current number of the IP ACLs configured on the switch.
Maximum ACL	The maximum number of IP ACLs that can be configured on the switch, depending on the hardware.

Table109. IPv6 ACL (continued)

Field	Description
Rules	The number of the rules associated with the IP ACL.
Type	The type is IPv6 ACL.

5.7.9. Configure 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.

Configure ACL IPv6 rules:

Security > ACL > Advanced > IPv6 Rules.

1. Use **Rule ID** to enter a whole number in the range of 1 to 1023 that is used to identify the rule.

   An IP ACL can have up to 1023 rules.

2. Use **Action** to specify what action is 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 causes 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. In the **Match Every** field, select **True** or **False**.

   True signifies that all packets must match the selected IPv6 ACL and rule and are either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered. To configure specific match criteria for the rule, remove the rule and recreate it, or reconfigure *Match Every* to *False* for the other match criteria to be visible.

8. There are two ways to configure IPv6 **Protocol Type**:
   - Specify an integer ranging from 1 to 255 after selecting the protocol keyword other. This number represents the IP protocol.
   - 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 can be set separately. the possible values are as follows:

   - **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:
     - **Protocol**. There are two ways to configure IPv6 protocol.

       Specify an integer ranging from 1 to 255 after selecting protocol keyword *other*. This number represents the IP protocol.

       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).

     - **Src**. Specify a source IPv6 address to match with the selected IPv6 ACL rule.

       When the **IPv6 Address** radio button is selected, enter an IPv6 address with prefix length to match the IPv6 ACL rule. If these fields are left empty, it means *any*.

       When the **Host** radio button is selected, enter a host source IPv6 address to match the 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.
10. **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, select the port key from the list or enter a port number. 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*.
11. **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.

12. **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, select the port key from the list or enter a port number. 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. **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.
14. **Fragments**. The rule to match the packets that are noninitial 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.

15. **Routing**. The rule to match the packets that include a routing extension header.
16. **ICMPv6 Type**. Specifies a match condition for ICMP packets.

    When the *Type* radio button is selected, the IPv6 ACL rule matches the specified ICMPv6 message type. Possible type numbers are in range from 0 to 255. When ICMPv6 code is specified, IP ACL rule matches with the specified ICMPv6 message code. Possible values are in the range from 0 to 255. If this field is left empty, it means *any*.

17. When the *Message* radio button is selected, select the type of the ICMPv6 messages to match the selected IPv6 ACL rule.

    Specifying Message implies that both ICMPv6 type and ICMPv6 code are specified. The ICMPv6 message is decoded into the corresponding ICMPv6 type and ICMPv6 code within that ICMPv6 type. IPv6 ICMPv6 message types are 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.

18. **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.

19. 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. To select the IPv6 DSCP, select one of the DSCP keywords. If a value is to be selected by specifying its numeric value, then select **Other** and a field appears where you can enter the numeric value of the DSCP.

20. **Rate Limit Conform Data Rate**. Specify the conforming data rate of the IPv6 ACL rule.

    Valid values are 1 to 4294967295 in Kbps.

21. **Rate Limit Burst Size**. Specify the burst size of IPv6 ACL rule.

    Valid values are 1 to 128 in Kbytes.

22. **Time Range**. Name of time range associated with the IPv6 ACL rule.
23. **Rule Status**. Displays if the ACL rule is active or inactive.

    Blank means that no timer schedules are assigned to the rule.

24. To modify an IP extended ACL rule, click the **Rule ID**.

    The number is a hyperlink to the Extended IPv6 ACL Rule Configuration (100-199) screen. Click the **Add** button on the IP Extended Rules screen.

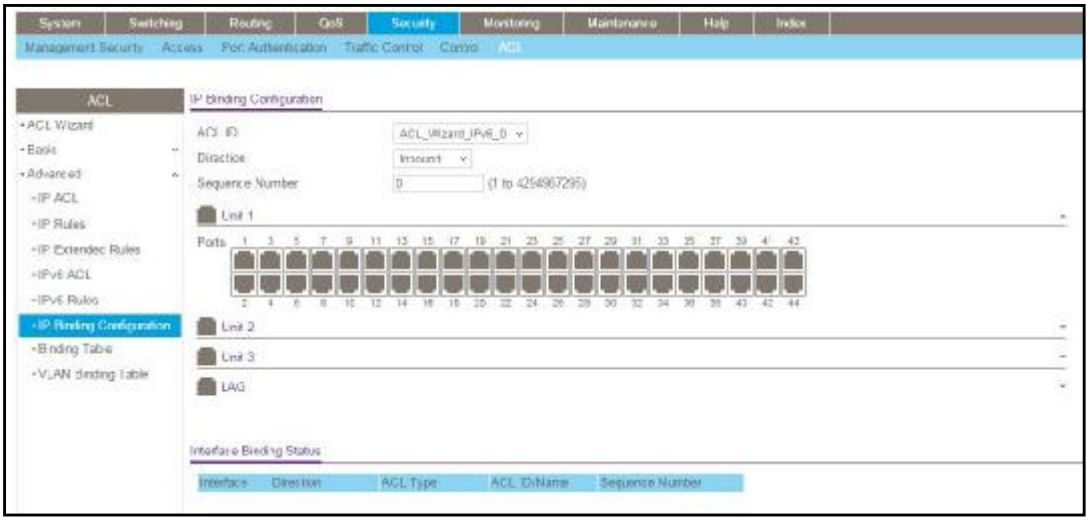
25. For standard ACL rule configuration (1–99), click the **Add** button on the IPv6 Rules screen.
26. To delete a rule, select its check box and click the **Delete** button.

5.7.10. Configure IP ACL Interface Bindings

When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface. You can assign ACL lists to ACL priorities and interfaces.

To configure IP ACL interface bindings:

Security > ACL > Advanced > IP Binding Configuration.



1. In the **ACL ID** menu, select an IP ACL.

   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 you do not specify the sequence number (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 is 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 the **Apply** button to save any changes to the running configuration.

The following table describes the nonconfigurable information displayed on the screen.

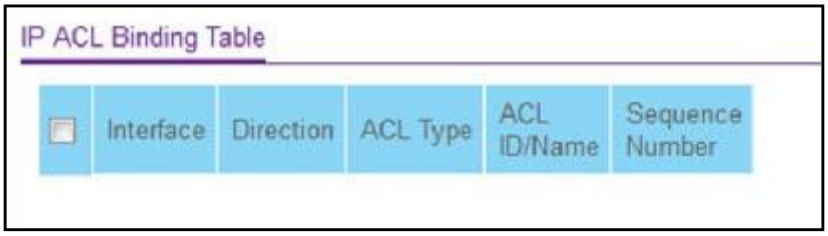
Table110. IP Binding Configuration

Field	Description
Interface	Displays the selected interface.
Direction	Displays the selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID/Name	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	The sequence number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

5.7.11. View or Delete IP ACL Bindings in the IP ACL Binding Table

To view or delete IP ACL bindings:

Security > ACL > Advanced > Binding Table.



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

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

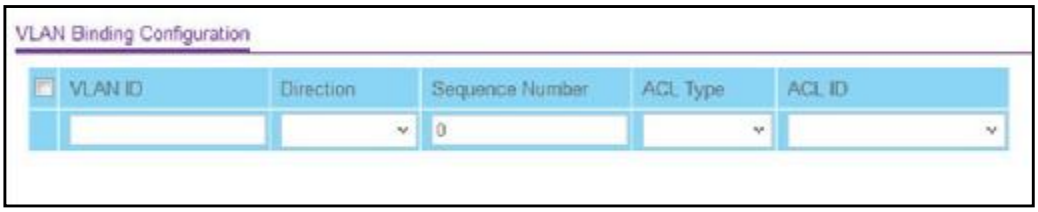
Table111. IP ACL Binding Table

Field	Description
Interface	Displays the selected interface.
Direction	Displays the selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID/Name	The ACL number (in the case of the 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	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to selected interface and direction.

5.7.12. View or Delete VLAN ACL Bindings in the VLAN Binding Table

To view or delete VLAN ACL bindings:

Security > ACL> Advanced > 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.
3. Click the **Add** button to add a VLAN ID to the selected ACL ID.
4. To delete a VLAN ACL-to-interface binding, select the check box for the interface and click the **Delete** button.

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

Table112. ACL VLAN Binding Table

Field	Description
Direction	The packet filtering direction for ACL.
VLAN ID	The VLAN ID for ACL mapping.
Sequence Number	An optional sequence number can 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 (the value is 0), a sequence number that is one greater than the highest sequence number currently in use for this VLAN and direction is used. The valid range is 1 to 4294967295.

6. Monitor the System

This chapter covers the following topics:

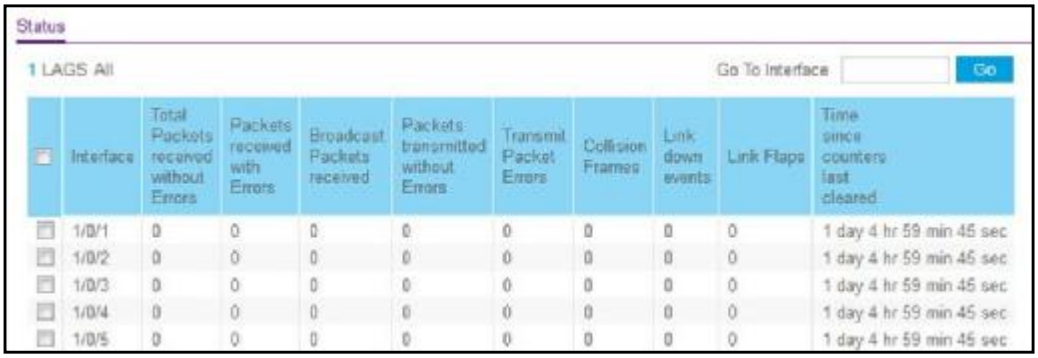
- *View Port Statistics*
- *Manage Logs*
- *Configure Multiple Port Mirroring*
- *Configure RSPAN VLAN*
- *Configure sFlow*

You can view a summary of per-port traffic statistics on the switch.

6.1. Port

To view port statistics:

Monitoring Ports > Port Statistics.



Use the buttons at the bottom of the screen 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 the **Clear** button.
- To clear the counters for a specific port, select the check box for the port and click the **Clear** button.
- To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the per-port statistics displayed on the screen..

Table113. Port Statistics

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. This does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that were 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 events (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.

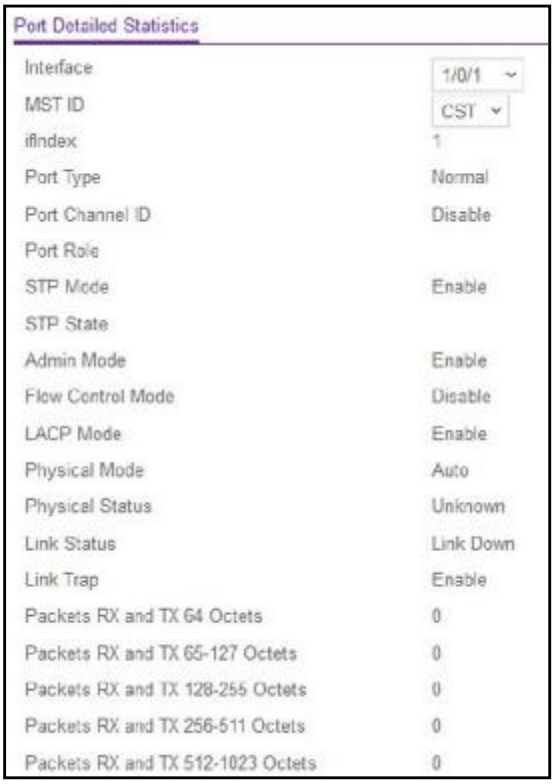
6.1.1. View Detailed Port Statistics

You can view a variety of per-port traffic statistics.

To view detailed port statistics:

Monitoring > Ports > Port Detailed Statistics.

The following figure shows some, but not all, of the fields on the Port Detailed Statistics screen.



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

- To clear all the counters, click the **Clear** button. This resets all statistics for this port to the default values.
- To refresh the screen with the latest information on the switch, click the **Update** button.

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.

Table114. Port Detailed Statistics

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.

Table115. Port Detailed Statistics (continued)

Field	Description
Port Type	For normal ports this field is normal. Otherwise the possible values are as follows: • **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 tole for each spanning tree. The port role is 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 as follows: • 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 places that port into the broken state. The 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 administrative 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 autonegotiation mode the duplex mode and speed are set from the autonegotiation process.
Physical Status	Indicates the port speed and duplex mode.

Link Status	Indicates whether the link is up or down.
Link Trap	Indicates whether or not the port sends a trap when link status changes.

Table116. Port Detailed Statistics (continued)

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

Table117. Port Detailed Statistics (continued)

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. This number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
Receive Packets Discarded	The number of inbound packets that were discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
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 nonintegral number of octets (alignment error). This definition of jabber is different from 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 with 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 nonintegral number of octets.

Table118. Port Detailed Statistics (continued)

Field	Description
Rx FCS Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad frame check sequence (FCS) with an integral number of octets
Overruns	The total number of frames discarded because 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 that were discarded (that is, 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 must 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 to use, including Ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.

Table119. Port Detailed Statistics (continued)

Field	Description
Total Packets Transmitted Successfully	The number of frames that were transmitted by this port to its segment.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
Total Transmit Errors	The sum of single, multiple, and excessive collisions.
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.

Table120. Port Detailed Statistics (continued)

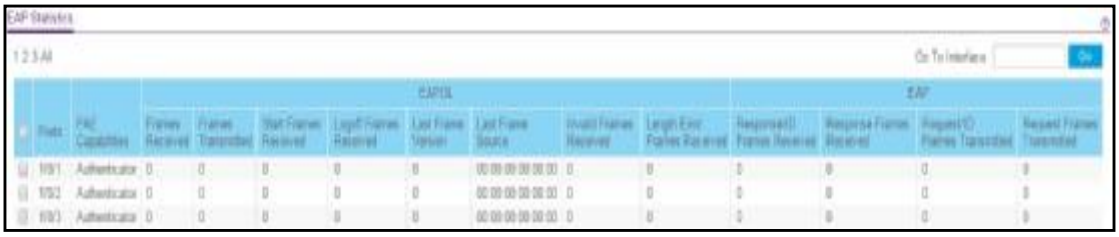
Field	Description
EAPOL Frames Received	The number of valid EAPOL frames of any type that were received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that were transmitted by this authenticator.
Time Since Counters Last Cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for this port were last cleared.

6.1.2. View EAP Statistics

You can display information about EAP packets received on a specific port.

To view EAP statistics:

Monitoring > Ports > EAP Statistics.



Use the buttons at the bottom of the screen 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 the **Clear** button. Clicking 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 the **Clear** button.
- To refresh the screen with the latest information on the switch.

The following table describes the EAP statistics displayed on the screen, click the **Update** button.

Table121. EAP Statistics

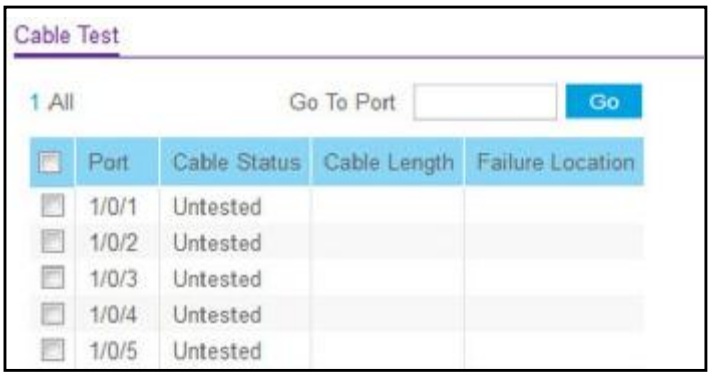
Field	Description
Port	Selects the port to be displayed. When the selection is changed, a screen update occurs causing all fields to be updated for the newly selected port. All physical interfaces are valid.
PAE Capabilities	This displays the PAE capabilities of the selected port.
EAPOL Frames Received	This displays the number of valid EAPOL frames of any type that were received by this authenticator.
EAPOL Frames Transmitted	This displays the number of EAPOL frames of any type that were transmitted by this authenticator.

EAPOL Start Frames Received	This displays the number of EAPOL start frames that were received by this authenticator.
EAPOL Logoff Frames Received	This displays the number of EAPOL logoff frames that were 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 Received	This displays the number of EAPOL frames that were 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 were 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 were received by this authenticator.
EAP Response Frames Received	This displays the number of valid EAP response frames (other than resp/ID frames) that were received by this authenticator.
EAP Request/ID Frames Transmitted	This displays the number of EAP request/identity frames that were transmitted by this authenticator.
EAP Request Frames Transmitted	This displays the number of EAP request frames (other than request/identity frames) that were transmitted by this authenticator.

6.1.3. Perform a Cable Test

To perform a cable test:

Monitoring > Ports > Cable Test.



1. **Port**. Indicates the interface to which the cable to be tested is connected.
2. Click the **Apply** button.

   A cable test is performed on the selected interface. The cable test might take up to two 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 might be *Open* or *Short* because some Ethernet adapters leave unused wire pairs unterminated or grounded.

The following table describes the nonconfigurable information displayed on the screen.

Table122. Cable Test

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 might 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.

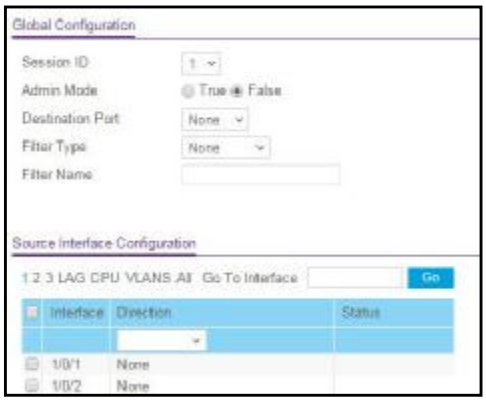
6.2. Configure Multiple Port Mirroring

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 can 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.

To globally configure multiple port mirroring:

Monitoring > Mirroring > Multiple Port Mirroring.



1. Select the number of the session from the **Session ID** list.
2. Select the Admin Mode **True** (enabled) or **False** (disabled) radio button.

   Select the **True** option to enable Admin mode for the selected session. When a particular session is enabled, any traffic entering or leaving the source ports of the session is copied (mirrored) onto the corresponding destination port or a remote switched port analyzer (RSPAN) VLAN. By default, Admin mode is disabled (**False**).
3. From the **Destination Port** list, select the destination interface 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 receives all the traffic from configured mirrored ports. If the value is not configured, it is shown as None. The default value is None.
4. From the **Filter Type** list, select the IP or MAC ACL that can mirror traffic that matches a permit rule.

   Possible values are as follows:

   - **None**. No filter is configured for the session.
   - **IP ACL**. Configure IP ACL.
   - **MAC ACL**. Configure MAC ACL.

   The default value is None.
5. In the **Filter Name** field, enter the name of the filter, if it is configured for the session.
6. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.
7. In the Source Interface Configuration section, use the following selection methods:
   - Select **Unit ID** to display the physical ports of the selected unit.
   - Select **LAG** to display a list of LAGs only.
   - Select **CPU** to display a list of CPUs only.
   - Select **VLANs** to display a list of available VLANs.
   - Select **All** to display a list of all physical ports, LAG, CPU, and VLANs.
   - Select a specific interface by entering its number in the **Go To Interface** field.

- Use **Interface** to specify the configured ports as mirrored ports. Traffic of the configured ports is sent to the probe port.

8. **In the Direction field**, specify the direction of the traffic to be mirrored from the configured mirrored ports.

   If the value is not configured, it is shown as None. The default value is None. Direction options are as follows:

   - **None**. The value is not configured.
   - **Tx and Rx**. Monitors transmitted and received packets.
   - **Tx**. Monitors transmitted packets only.
   - **Rx**. Monitors received packets only.

Note: For VLANs only, the **Tx and Rx** and **None** options are applicable.

- **Tx and Rx**. Specify VLAN as the source VLAN.
- **None**. Remove the specified source VLAN.

If the VLAN is configured as the source VLAN, its direction is displayed as a blank field.

9. Click the **Apply** button.

The settings are applied to the system. If the port is configured as a source port, the **Mirroring Port** field value is Mirrored.

The **Status** field indicates the interface status.

Note: In case of an error dialog having multiple error messages, resolve them to get the remaining set of errors, if any.

6.3. Configure RSPAN VLAN

You can configure the VLAN to use the remote switched port analyzer (RSPAN) VLAN. RSPAN allows you to mirror traffic from multiple source ports (or from all ports that are members of a VLAN) from different network devices and send the mirrored traffic to a destination port (a probe port connected to a network analyzer) on a remote device. The mirrored traffic is tagged with the RSPAN VLAN ID and transmitted over trunk ports in the RSPAN VLAN.

To configure RSPAN VLAN:

Monitoring > Mirroring > RSPAN VLAN.

The **VLAN ID** column lists all VLANs on the device.

1. Select the VLAN to use as the RSPAN VLAN.
2. In the **Admin Mode** list, select to **Enable** or **Disable** RSPAN support on the corresponding VLAN.

The default value is Disable.

3. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

6.3.1. Configure an RSPAN Source Switch

To configure an RSPAN source switch:

Monitoring > Mirroring > RSPAN Source Switch Configuration.

1. Select the **Session ID** number from the list.
2. Select the Admin Mode **True** (enabled) or **False** (disabled) radio button for the selected session.

   When a particular session is enabled, any traffic entering or leaving the source ports of the session is copied (mirrored) onto the corresponding destination port or a remote switched port analyzer (RSPAN) VLAN. By default, Admin mode is False (disabled).
3. Select the **RSPAN Destination VLAN** from the list of available VLAN IDs.
4. Select the **RSPAN Reflector Port** from the list of reflector port interfaces.
5. Select from the **Filter Type** list to configure IP or MAC ACLs that can mirror traffic that matches a permit rule.

   Possible values are as follows:

   - **None.**
   - **IP ACL**. Configure IP ACL.
   - **MAC ACL**. Configure MAC ACL.
6. Enter the **Filter Name**, if a filter is configured for the session.
7. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To configure an RSPAN source interface:

1. Select a Unit ID (**1, 2, 3**) to display a list of physical ports for the selected unit.
2. Select **LAG** to display LAGs only.
3. Select **CPU** to display CPUs only.
4. Select **VLAN** to display a list of available VLAN IDs.
5. Select **All** to display all physical ports, LAGs, CPUs, and VLANs.
6. Select an interface by entering the interface number in the **Go To Interface** field.
7. In the **Interface** list, select an interface to specify the configured ports as mirrored ports.

   Traffic of the configured ports is sent to the probe port.
8. Select from the **Direction** list to specify the direction of the traffic to be mirrored from the configured mirrored ports.

   If the value is not configured, None is displayed. The default value is None.

   - **None**. The value is not configured.
   - **Tx and Rx**. Monitor transmitted and received packets.
   - **Tx**. Monitor transmitted packets only.
   - **Rx**. Monitor received packets only.

The **Status** field indicates the interface status.

6.3.2. Configure the RSPAN Destination Switch

To configure the RSPAN destination switch:

Monitoring > Mirroring > RSPAN Destination Switch Configuration.

1. From the **Session ID** list, select the session ID.
2. Select the Admin Mode **True** (enabled) or **False** (disabled) radio button for the selected session.

   When a particular session is enabled, any traffic entering or leaving the source ports of the session is copied (mirrored) onto the corresponding destination port or a remote switched port analyzer (RSPAN) VLAN. By default, the Admin mode is disabled.
3. Select the **RSPAN Source VLAN** from the list of available VLAN IDs.
4. Select the **RSPAN Destination VLAN** from the list of destination interfaces.
5. Configure the **Filter Type**.

IP or MAC ACLscan mirror traffic that matches a permit rule. Possible values are as follows:

- **None**. No filter is configured for the session.
- **IP ACL**. Configure IP ACL.
- **MAC ACL**. Configure MAC ACL.

6. Enter the **Filter Name**, if it is configured for the session.
7. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

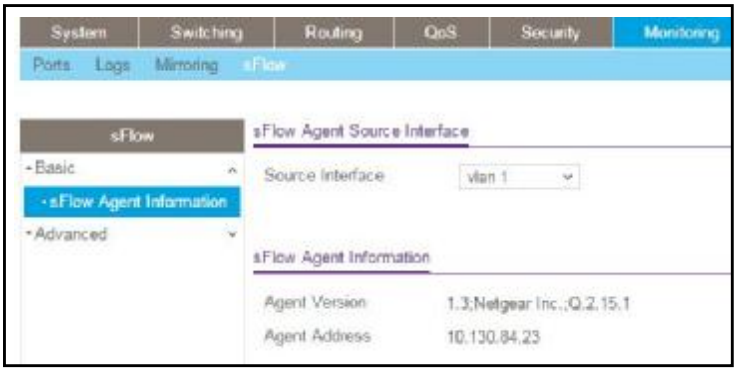
6.4. Configure sFlow

You can configure basic or advanced sFlow settings.

6.4.1. Configure Basic sFlow Agent Information

To configure basic sFlow agent information:

Monitoring > sFlow > Basic > sFlow Agent Information.



1. In the **Source Interface** list, select the management interface that is used for sFlow Agent.

   Possible values are as follows:

   - None
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Tunnel interface
   - Service port

   By default, VLAN 1 is used as the source interface.
2. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect

immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable information.

Table123. sFlow Basic Agent Information

Field	Description
Agent Version	Uniquely identifies the version and implementation of this MIB. The version string must use the following structure: MIB Version;Organization;Software Revision where: • MIB Version: For example, 1.3, the version of this MIB • Organization: Inc. • Revision: 1.0
Agent Address	The IP address associated with this agent.

6.4.2. Configure sFlow Agent Advanced Settings

To configure sFlow agent advanced settings:

Monitoring > sFlow > Advanced > sFlow Agent Information.

1. In the **Source Interface** list, select the management interface to be used for sFlow Agent.

   Possible values are as follows:

   - None
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Tunnel interface
   - Service port

   By default, VLAN 1 is used as the source interface.

2. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable information.

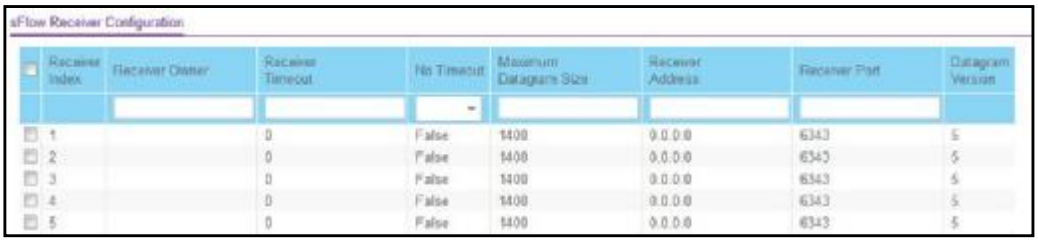
Table124. sFlow Advanced Agent Information

Field	Description
Agent Version	Uniquely identifies the version and implementation of this MIB. The version string must use the following structure: MIB Version;Organization;Software Revision where: • MIB Version: '1.3', the version of this MIB • Organization: Inc. • Revision: 1.0
Agent Address	The IP address associated with this agent.

6.4.3. Configure an sFlow Receiver

To configure an sFlow receiver:

Monitoring > sFlow > Advanced > sFlow Receiver Configuration.



1. Specify the **Receiver Owner**

   This is 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. The 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** to set the no time-out sampling for the receiver.

   Sampling is not stopped until the 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.

   Set this value to avoid fragmentation of the sFlow datagrams. Default Value: 1400. The 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 are sent.

6. **Receiver Port**. The destination port for sFlow datagrams.

   The allowed range is 1 to 65535.

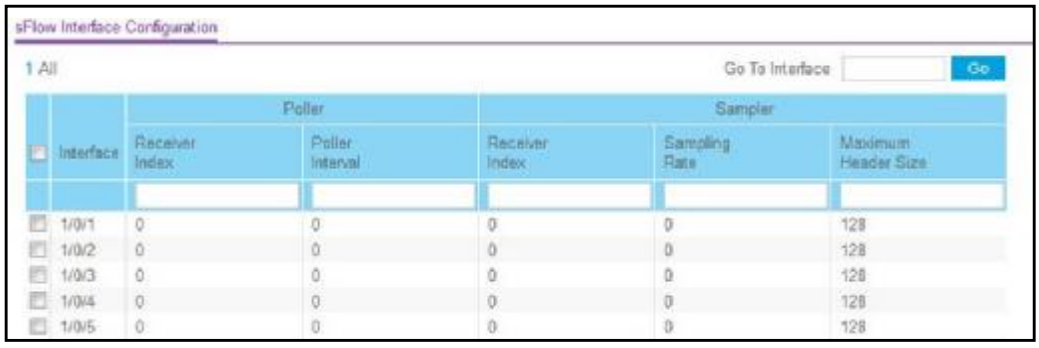
The **Receiver Datagram Version** field displays the version of sFlow datagrams to be sent.

6.4.4. Configure the sFlow Interface

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 configure the sFlow Interface:

Monitoring > sFlow > Advanced > sFlow Interface Configuration.



1. **Interface** displays the interface for this flow poller and sampler.

   This agent supports physical ports only.

2. Use **Poller Receiver Index** to specify the allowed range for the sFlow receiver associated with this counter poller.

   The 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.

   The 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 also expires. The 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. The Allowed range is 1024 to 65536.

6. Use **Maximum Header Size** to specify the maximum number of bytes to be copied from a sampled packet.

   The allowed range is 20 to 256.

6.5. Manage Logs

The switch generates 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.

6.5.1. View Buffered Logs

To view buffered logs:

Monitoring > Logs > Buffered Logs.

6.5.2. Configure Buffered Logs

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.

To configure buffered logs:

1. Select the Admin Status **Enable** or **Disable** radio button.

   A log that is disabled does not log messages.

2. Use **Behavior** to specify the behavior of the log when it is full.

   It can either wrap around or stop when the log space is filled.

3. Select the severity option in the **Severity Filter** list.

A log records messages equal to or above a configured severity threshold. The severity levels are as follows:

- **Emergency (0)**. The 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.

To refresh the screen with the latest information on the switch, click the **Update** button.

4. Click the **Clear** button to clear the buffered log in the memory.
5. Click the **Apply** button.

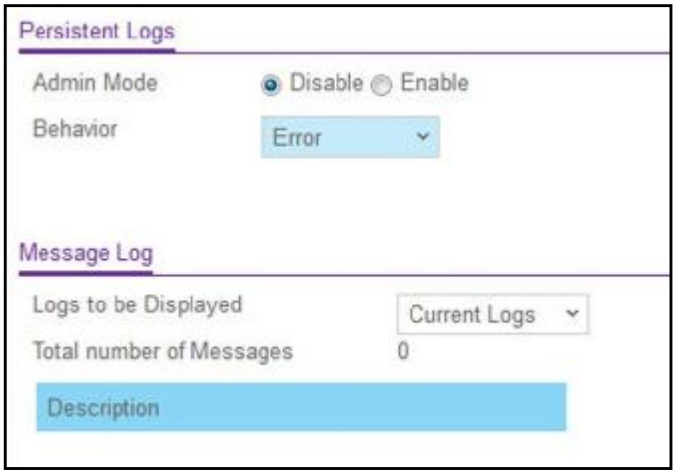
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

6.5.3. Configure Persistent Logs (and only)

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 configure persistent logs:

Monitoring > Logs > Persistent Logs.



A log that is disabled does not log messages.

1. Select the Admin Mode **Disable** or **Enable** radio button.

2. In the **Behavior** list, select the severity level.

   A log records messages equal to or above a configured severity threshold. These severity levels are available:

   - **Emergency (0**). The 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

To refresh the screen with the latest information on the switch, click the **Update** button.

6.5.4. 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

This 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 through syslog use a format identical to the previous message.

6.5.5. Message Log Format

This topic applies to the format of all logged messages that are displayed for the message log, persistent log, or console log.

Messages logged to a collector or relay through syslog use 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.

  This 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.

- <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.

  This 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 through syslog use a format identical to the previous message.

- **Total number of Messages**: For the message log, only the latest 200 entries are displayed on the screen.

6.5.6. Enable or Disable the Command Log

To enable or disable the command log:

Monitoring > Logs > Command Log Configuration.

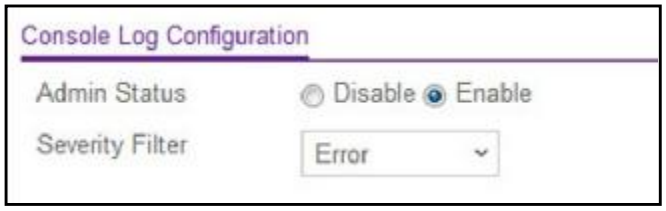
1. Use **Admin Mode** to enable/disable the operation of the CLI command logging by selecting the corresponding radio button.

6.5.7. Enable or Disable Console Logging

This allows logging to any serial device attached to the host.

To enable or disable console logging:

Monitoring > Logs > Console Log Configuration.



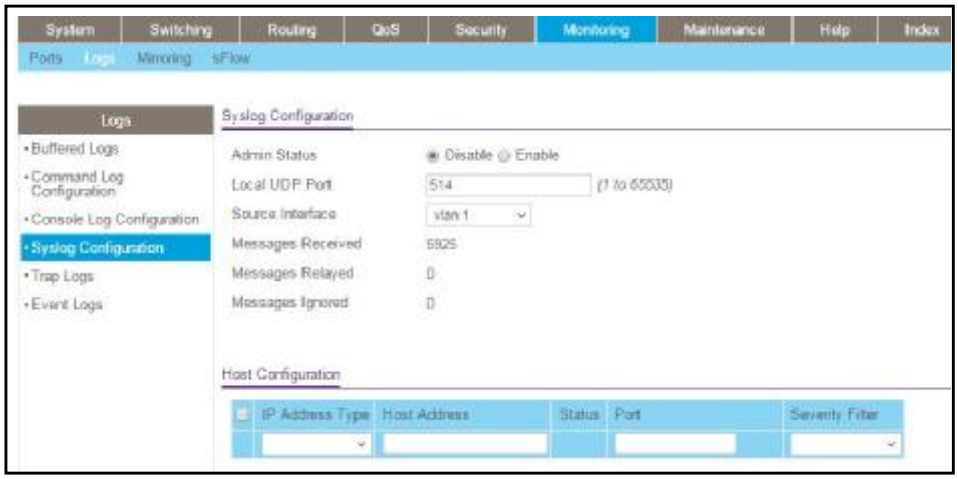
1. Select the Admin Status **Disable** or **Enable** radio button.

   A log that is disabled does not log messages.

6.5.8. Configure Syslog Host Settings

To configure THE syslog:

Monitoring > Logs > Syslog Configuration.



The **Status** field displays whether the host was configure to be actively logging or not.

1. Select the Admin Status **Disable** or **Enable** radio button.

   This enables or disables logging to configured syslog hosts. Setting this to disable stops logging to all syslog hosts so that no messages are sent to any collectors or relays. Enable means messages are sent to configured collectors or relays using the values configured for each collector or relay.

2. Use **Local UDP Port** to specify the port on the local host from which syslog messages are sent.

   The default port is 514.

3. Specify the **Source Interface** to use for syslog.

   Possible values are as follows:

   - None
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Tunnel interface
   - Service port

   By default, VLAN 1 is used as source interface.

4. Use **IP Address Type** to specify the address type of host.

   It can be one of the following:

   - IPv4
   - IPv6
   - DNS

5. iIn the **Host Address** - This is the address of the host configured for THE syslog.
6. In the **Port** field, specify the port on the host to which syslog messages are sent.

   The default port is 514.

7. Select the severity option in the **Severity Filter** list.

   A log records messages equal to or above a configured severity threshold. These severity levels are available:

   - **Emergency (0)**. The 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

The following table describes the nonconfigurable data.

Table125. Syslog Configuration

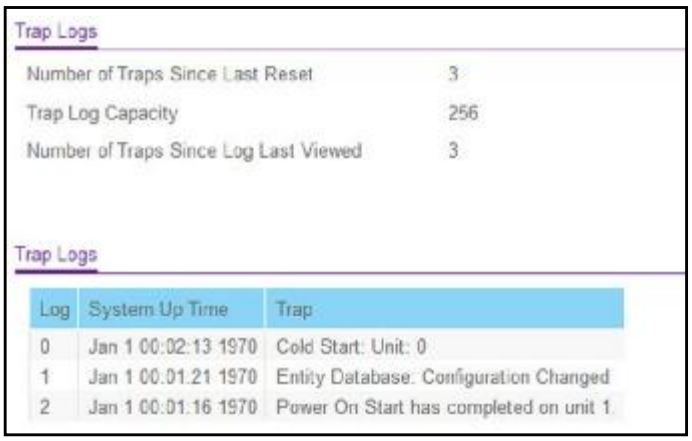
Field	Description
Messages Received	The number of messages received by the log process. This includes messages that are dropped or ignored.
Messages Relayed	The count of syslog messages relayed.
Messages Ignored	The count of syslog messages ignored.

6.5.9. View the Trap Logs

You can view the entries in the trap log. The information can be retrieved as a file.

View the trap logs:

Monitoring > Logs > Trap Logs.



The screen also displays information about the traps that were sent.

Click the **Clear** button to clear all the counters. This resets all statistics for the trap logs to the default values.

The following table describes the Trap Log information displayed on the screen.

Table126. Trap Logs

Field	Description
Number of Traps Since Last Reset	The number of traps that occurred since the switch last rebooted.
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries overwrite the oldest entries.
Number of Traps since log last viewed	The number of traps that occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, web display, upload file from switch, and so on) causes this counter to be cleared to 0.
Log	The sequence number of this trap.
System Up Time	The time when this trap occurred, expressed in days, hours, minutes and seconds, since the last reboot of the switch.
Trap	Information identifying the trap.

6.5.10. View the Event Log

You can view the event log, which contains error messages from the system. The event log is not cleared on a system reset.

To view the event log:

Monitoring > Logs > Event Logs.

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

- To clear the messages out of the Event Log, click the **Clear** button.
- To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the event log information displayed on the screen.

Table127. Event Logs

Field	Description
Entry	The sequence number of the event.
Type	The type of the event.
File Name	The file in which the event originated.

Line	The line number of the event.
Task Id	The task ID of the event.

Table128. Event Logs

Field	Description
Code	The event code.
Time	The time this event occurred.

7. Maintenance

This chapter covers the following topics:

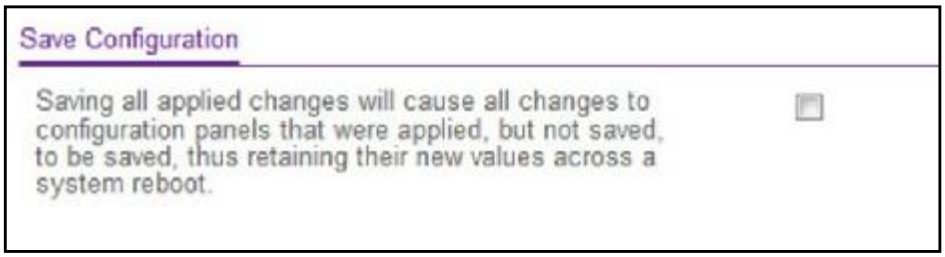
- *Save the Configuration*
- *Configure Auto Save Mode*
- *Reboot the Switch*
- *Power Cycle the Switch*
- *Reset the Switch to Its Factory Default Settings*
- *Reset All User Passwords to Their Default Settings*
- *Upload a File from the Switch*
- *Download a File to the Switch*
- *File Management*
- *Troubleshooting*

7.1. Save the Configuration

When you save the configuration, changes that you made are retained by the switch when it is rebooted. You can manually save the configuration or you can set up autosave.

To save the configuration:

Maintenance > Save Config > Save Configuration.



1. Select the check box.
2. Click the **Apply** button.

   The configuration changes you made are saved across a system reboot. All changes submitted since the previous save or system reboot are retained by the switch.

7.2. Reboot the Switch

To reboot the switch:

Maintenance > Reset > Device Reboot.

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 a radio button:
   - **Save prior to reboot**.The current configuration is saved and the switch reboots.
   - **Don't save prior to reboot**. The switch will reboot without saving the current configuration
3. Click the **Apply** button.

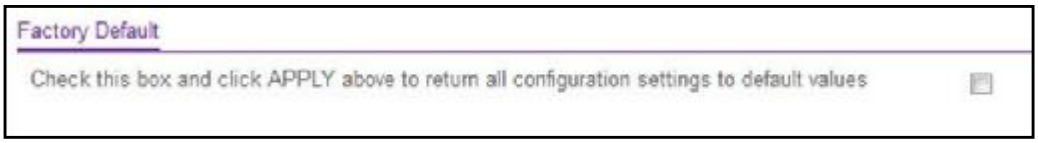
   If you selected the save option, the configuration is saved. The switch reboots.

7.3. Reset the Switch to Its Factory Default Settings

Note: If you reset the switch to the default configuration, the IP address is reset to 192.168.10.12, and the DHCP client is enabled.

To reset the switch to the factory default settings:

Maintenance > Reset > Factory Default.



1. Select the check box.
2. Click the **Apply** button.

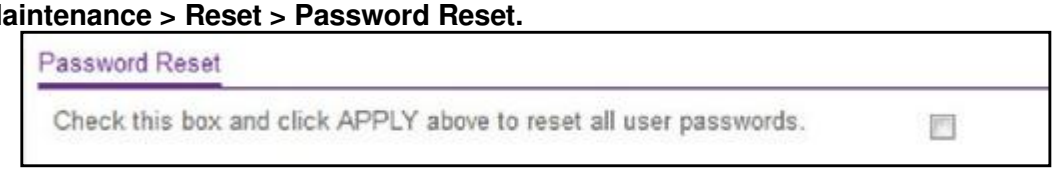
   A confirmation screen displays.
3. Click **Yes** to confirm.

   All configuration parameters are reset to their factory default values. All changes you made are, even if you issued a save.

7.4. Reset All User Passwords to Their Default Settings

To reset all user passwords to their default settings:

Maintenance > Reset > Password Reset.



1. Select the check box.
2. Click the **Apply** button.

   All user passwords are reset to their factory default values.

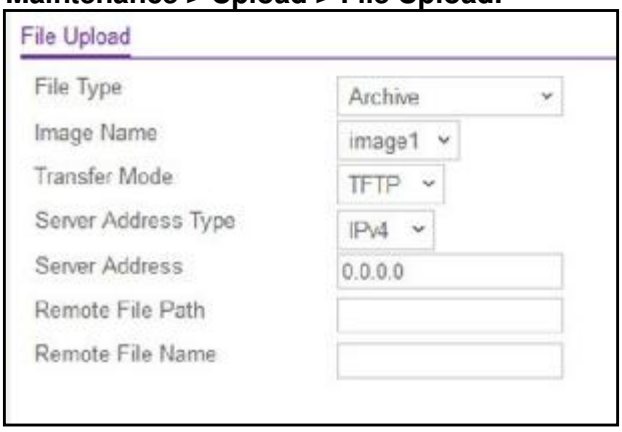
7.5. Upload a File from the Switch

You can upload configuration (ASCII), log (ASCII), and image (binary) files from the switch to the TFTP server.

7.5.1. Upload a File to the TFTP Server

To upload a file from the switch to the TFTP server:

Maintenance > Upload > File Upload.



1. Use **File Type** to specify what type of file to upload:
   - **Archive**. Specify Archive (STK) code to retrieve from the operational flash.

CLI Banner. Specify CLI Banner to **retrieve** the CLI banner file.

- **Text Configuration**. Specify configuration in text mode to retrieve the stored configuration.
- **Script File**. Specify Script file 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 Protocol
   - **SCP**. Secure Copy Protocol
   - **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 to upload the file.

   File path can include alphabetic, numeric, forward slash, dot or underscorecharacters only. You can enter up to 160 characters. The factory default is blank.

7. Use **Remote File Name** to enter the name of the file to download from the server. You can enter up to 32 characters.

   The factory default is blank.

8. Use **Local File Name** to specify the local script file name to upload.

   This field is visible only when File Type is Script File.

9. Use **User Name** to enter the user name for remote login to the SFTP/SCP server where the file is sent.

   This field is visible only when the SFTP or SCP transfer mode is selected.

10. Use **Password** to enter the password for remote login to SFTP/SCP server where the file is sent.

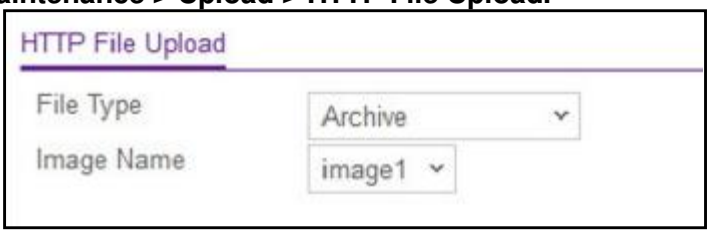
    This field is visible only when the SFTP or SCP transfer mode is selected.

The last row of the table is used to display information about the progress of the file transfer.

7.5.2. HTTP File Upload

To use HTTP rile upload:

Maintenance > Upload > HTTP File Upload.



1. Use **File Type** to specify what type of file to upload:
   - **Archive**. Specify Archive (STK) code to retrieve from the operational flash:
   - **Image Name**. Select one of the images from the list:
     - **Image1**. Specify the code image1 to retrieve.
     - **Image2**. Specify the code image2 to retrieve.
   - **CLI Banner**. Specify CLI Banner to retrieve the CLI banner file.
   - **Text Configuration**. Specify configuration in text mode to retrieve the stored configuration.
   - **Script File**. Specify Script file 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 to upload.

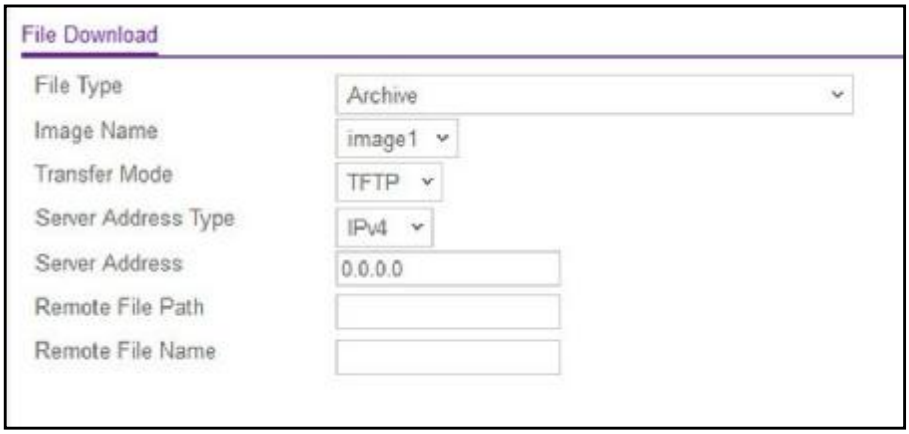
7.6. Download a File to the Switch

The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.

7.6.1. Download a File

To download a file:

Maintenance > File Export > File Export.



1. Use **File Type** to specify what type of file to transfer.
   - **Archive**. Archive (STK) code to upgrade the operational flash.
   - **Text Configuration**. Configuration in text mode to update the switch's configuration. If the file has errors, the update is stopped.
   - **SSH-1 RSA Key File**. SSH-1 Rivest-Shamir-Adelman (RSA) Key File.
   - **SSH-2 RSA Key PEM File**. SSH-2 Rivest-Shamir-Adelman (RSA) Key File (PEM Encoded).
   - **SSH-2 DSA Key PEM File**. 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 **Script File** to specify script configuration file.
- **CLI Banner**. Specify CLI Banner if a banner will to be displayed before the login prompt.
- Use **IAS Users** to specify the Internal Authentication Server Users Database file.

The factory default is Archive.

Note: For you to download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

Note: For you to download SSL PEM files, SSL must be administratively disabled and there can be no active SSH sessions.

The **Image Name** field is visible only when File Type **Archive** is selected.

2. Use **Image Name** to select one of the images from the list:
   - **Image1**. Specify the code image1 to retrieve.
   - **Image2**. Specify the code image2 to retrieve.
3. Use **Transfer Mode** to specify what protocol to use to transfer the file:
   - **TFTP**. Trivial File Transfer Protocol
   - **SFTP**. Secure File Transfer Protocol
   - **SCP**. Secure Copy Protocol
   - **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 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 to download from the server.

   The file path cannot include the following symbols: ' \:*?"<>| '. You can enter up to 32 characters. The factory default is blank.

8. Use **User Name** to enter the user name for remote login to SFTP/SCP server where the file resides.

   This field is visible only when the SFTP or SCP transfer mode is 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 the SFTP or SCP transfer mode is selected.

   The last row of the table displays information about the progress of the file transfer. It is displayed only after the process starts. The screen refreshes automatically until the file transfer completes.

10. Click the **Apply** button.

    The updated configuration is sent to the switch. Configuration changes take effect immediately.

7.6.2. Download a File to the Switch Using HTTP

You can download files of various types to the switch using an HTTP session (for example, through your web browser).

To download a file to the switch using HTTP:

Maintenance > File Export> HTTP File Export..

1. Use **File Type** to specify what type of file to transfer:
   - **Archive**. Archive (STK) code to upgrade the operational flash.
   - The **Image Name** field is visible only when File Type **Archive** is selected. Use **Image Name** to select one of the images from the list:
     - **Image1**. Specify the code image1 to download.

- **Image2**. Specify the code image2 to download.

- **Text Configuration**. Configuration is in text mode to update the switch's configuration. If the file has errors, the update is stopped.
- Use **SSH-1 RSA Key File** to specify SSH-1 Rivest-Shamir-Adelman (RSA) Key File.
- Use **SSH-2 RSA Key PEM File** to specify SSH-2 Rivest-Shamir-Adelman (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 **Config Script** to specify script configuration file.
- **CLI Banner**. Specify CLI Banner if a banner will be displayed before the login prompt.
- Use **IAS Users** to specify the Internal Authentication Server Users Database File.

The factory default is Archive.

Note: For you to download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

Note: For you to download SSL PEM files, SSL must be administratively disabled and there can be no active SSH sessions.

2. Use **Select File** to browse and enter a name along with path for the file to download.

   You can enter up to 80 characters. The factory default is blank.

3. Click **Browse** to locate the file to download.

   The factory default is blank.

4. Click the **Apply** button.

   The download begins.

   The **Download Status** field displays the status during transfer file to the switch.

Note: After a file transfer is started, wait until the screen refreshes. When the screen refreshes, the *Select File* option is blanked out. This indicates that the file transfer is done.

7.7. File Management

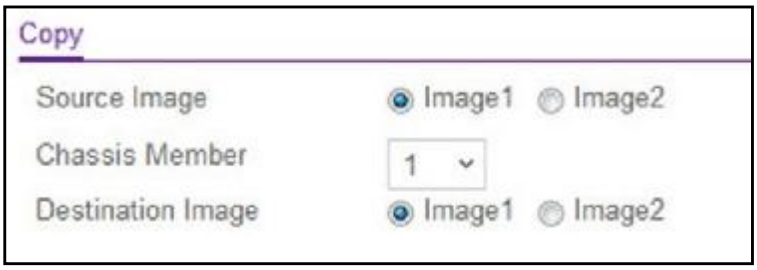
The system maintains two versions of the software in permanent storage. One image is

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 you are upgrading or downgrading the software.

7.7.1. Copy an Image

To copy an image:

Maintenance > File Management > Copy.



1. Use **Source Image** to select the image1 or image2 as the source image (the image to be copied).
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 the destination image.
4. Click the **Apply** button.

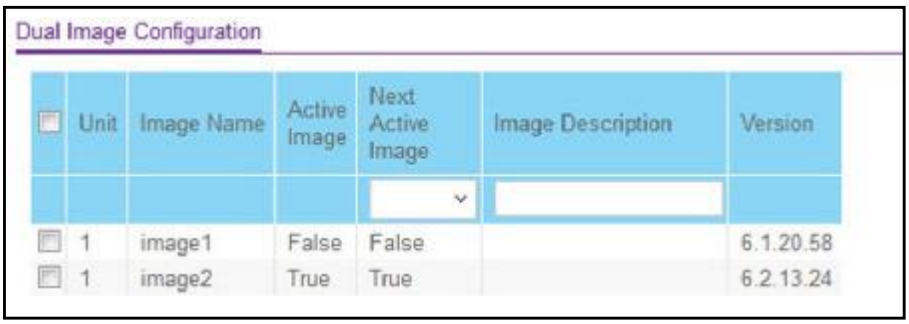
   The updated configuration is sent to the switch. Configuration changes take effect immediately.

7.7.2. Configure Dual Image Settings

The Dual Image feature allows the switch to retain two images in permanent storage. The administrator can designate image1 or image2 as the active image to be loaded during subsequent switch restarts. This feature reduces switch down time when you are upgrading or downgrading the software image.

To configure Dual Image settings:

Maintenance > File Management > Dual Image Configuration.



1. Use **Unit** to select the unit ID whose code image to activate, update, or delete.
2. Use **Next Active Image** to make the selected image the next active image for subsequent reboots of this unit.

3. Use **Image Description** to specify the description for the image that you selected.
4. Click the **Delete** button to delete the selected image from permanent storage on the switch.
5. Click the **Apply** button.

   The updated configuration is sent to the switch. Configuration changes take effect immediately.

Note: After activating an image, you must perform a system reset of the switch to run the new code.

The following table describes the nonconfigurable information displayed on the screen.

Table129. Dual Image Configuration

Field	Description
Image Name	This displays the image name for the selected unit.
Active Image	The current active image of the selected unit.
Version	The version of the image1 code file.

7.8. Troubleshooting

You can use Ping or Traceroute and you can perform a memory dump.

7.8.1. Ping IPv4

You can tell the switch to send a ping request to a specified IP address. You can check whether the switch can communicate with a particular IP station. When you click the **Apply** button, the switch sends a specified number of ping requests and the results are displayed.

If a reply to the ping is not received, the following message displays:

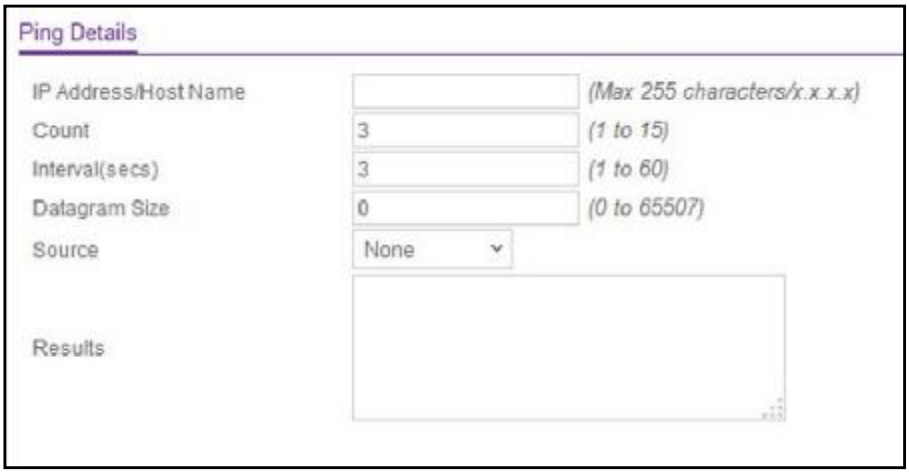
```
Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec
```

If a reply to the ping is received, the following message displays:

```
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 configure the settings and ping a host on the network:

Maintenance > Troubleshooting > Ping IPv4.



1. Use **IP Address/Host Name** to enter the IP address or host name of the station for the switch to ping.

   The initial value is blank.

2. In the **Count field**, enter the number of echo requests to send.

   The default value is 3. The range is 1 to 15.

3. Enter the **Interval** between ping packets in seconds.

   The default value is 3 seconds. The range is 1 to 60.

4. Enter the **Datagram Size** of ping packet.

   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 as follows:

   - **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 on this screen are not saved to the switch. As a result, refreshing the screen sets these fields to the default values.

6. Click the **Apply** button.

The pings are sent 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.

To cancel the operation on the screen and reset the data on the screen to the latest value of the switch, click the **Cancel** button.

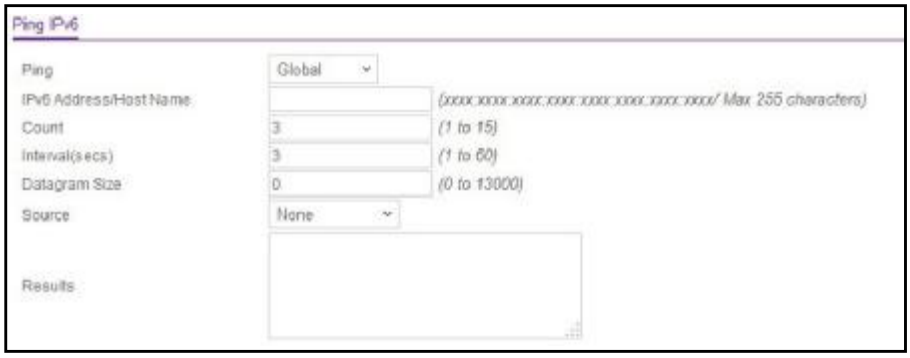
7.8.2. Ping IPv6

This screen is used to send a ping request to a specified host name or IPv6 address. You can use this to check whether the switch can communicate with a particular IPv6 station. When you click the **Apply** button, the switch sends a specified number of ping requests and the results are displayed below the configurable data. The output displays the following:

```
Send count=n, Receive count=n from (IPv6 Address). Average round trip
time = n ms.
```

To use Ping IPv6:

Maintenance > Troubleshooting > Ping IPv6.



1. Select the **Ping** type from the list.

   Possible values are as follows:

   - **Globa**l. 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 host name of the station for 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 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 the source is not required, select None as the source option. Possible values are as follows:

   - **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 in this screen are not saved to the switch. As a result, refreshing the screen sets these fields to the default values.

7. Click the **Apply** button.

   Pings are sent to the specified IPv6 address or host name. 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.

7.8.3. Traceroute IPv4

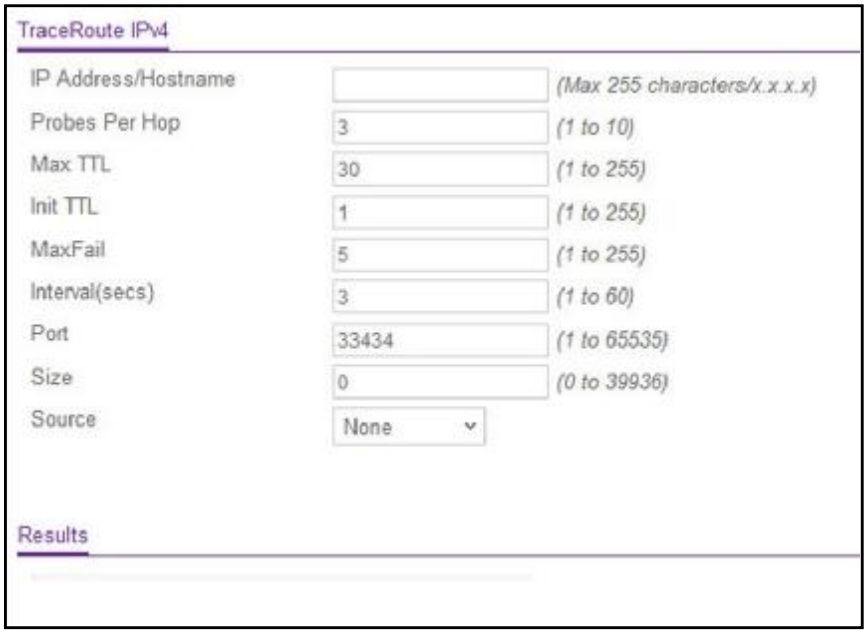
Use this screen to tell the switch to send a traceroute request to a specified IP address or host name. You can use this to discover the paths packets take to a remote destination. Once you click the **Apply** button, the switch sends traceroute and the results are displayed below the configurable data.

If a reply to the traceroute is received, the following message displays:

```
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 configure the traceroute settings and send probe packets to discover the route to a host on the network:

Maintenance > Troubleshooting > Traceroute IPv4.



1. Use **IP Address/Hostname** to enter the IP address or host name of the station to which you want 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 as follows:

   - **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 in this screen are not saved to the switch. As a result, refreshing the screen sets these fields to the default values.

10. Click the **Apply** button.

    A traceroute request is sent to the specified IP address or host name. The results are displayed below the configurable data in the TraceRoute Results area.

    The **Results** field displays the traceroute IPv4 result after the switch sends a traceroute request to the specified IP address or host name.

7.8.4. Traceroute IPv6

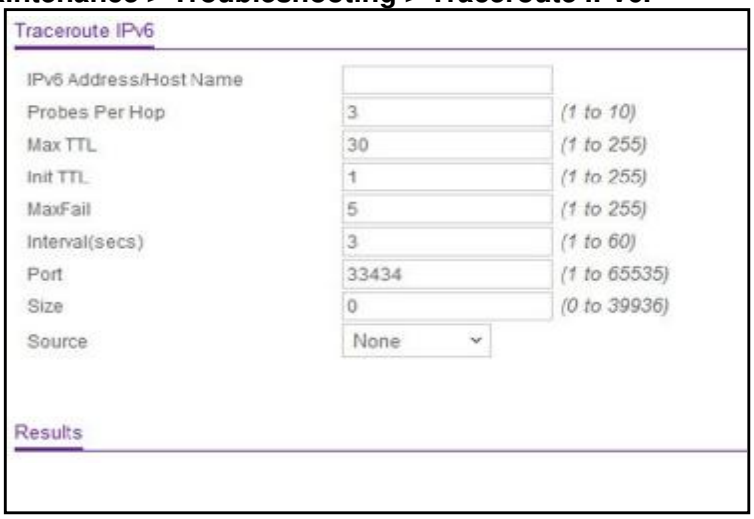
Use this screen to tell the switch to send a traceroute request to a specified IPv6 address or host name. You can use this to discover the paths packets take to a remote destination. Once you click the **Apply** button, the switch sends a traceroute and the results are displayed below the configurable data.

If a reply to the traceroute is received, the following message displays:

```
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 use traceroute IPv6:

Maintenance > Troubleshooting > Traceroute IPv6.



1. In the **IPv6 Address/Hostname** field, enter the IPv6 address or host name of the station to which you want the switch to discover a path.

The initial value is blank. The IPv6 address or host name 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 that 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 as follows:

   - **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 in this screen are not saved to the switch. As a result, refreshing the screen sets these fields to the default values.

10. Click the **Apply** button.

    The traceroute begins. The results display in the TraceRoute area.

    The **Results** field displays the traceroute IPv6 result after the switch sends a traceroute request to the specified IP address or host name.

8. Default Settings

This appendix describes the default settings for many of the managed switch software features.

Table130. Default Settings

Feature	Default
IP address	192.168.10.12
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

Table131. Default Settings (continued)

Feature	Default
sFlow	Enabled
ISDP	Enabled (Versions 1 and 2)
RMON	Enabled
TACACS	Not configured
RADIUS	Not configured
SSH/SSL	Disabled
Telnet	Enabled
Denial of Service Protection	Disabled
Captive Portal	Disabled
Dot1x Authentication (IEEE 802.1X)	Disabled
MAC-based port security	All ports are unlocked
Access control lists (ACL)	None configured
IP source guard (IPSG)	Disabled
DHCP snooping	Disabled
Dynamic ARP inspection	Disabled
Protected ports	None
Private groups	None
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)

Table132. Default Settings (continued)

Feature	Default
DHCP Layer 2 relay	Disabled
Default VLAN ID	1
Default VLAN name	Default
GVRP	Disabled
GARP timers	Leave: 60 centiseconds Leave All: 1000 centiseconds Join: 20 centiseconds
Voice VLAN	Disabled
Guest VLAN	Disabled
RADIUS-assigned VLANs	Disabled
Double VLANs	Disabled
Spanning Tree Protocol (STP)	Enabled
STP operation mode	IEEE 802.1s 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

9. Configuration Examples

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

- *Virtual Local Area Networks (VLANs)*
- *Access Control Lists (ACLs)*
- *Differentiated Services (DiffServ)*
- *802.1X*
- *MSTP*

9.1. 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 present 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 *Configure Port PVID Settings* on page 204.
- 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 is not a member of the VLAN as 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.

9.1.1. VLAN Configuration Examples

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 *Configure VLANs* on page 195), create the following VLANs:
   - A VLAN with VLAN ID 10.
   - A VLAN with VLAN ID 20.
2. In the VLAN Membership screen (see *Configure VLAN Membership* on page 201) 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 *Configure Port PVID Settings* on page 204), 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.

9.2. Access Control Lists(ACLs)

ACLs ensure that only authorized users can access 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.

allow ACLs to be bound to physical ports and LAGs. The switch software supports MAC ACLs and IP ACLs.

9.2.1. MAC ACL Sample 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 *Configure a Basic MAC ACL* on page 649).

   By default, this ACL is 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 *Configure MAC ACL Rules* on page 651.

3. From the MAC Binding Configuration screen, assign the Sales_ACL to the interface gigabit ports 6, 7, and 8, and then click the **Apply** button. (See *Configure MAC Binding* on page 654.)

   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 *View or Delete MAC ACL Bindings in the MAC Binding Table* on page 655).

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.

9.2.2. Standard IP ACL Sample 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 *Configure an IP ACL* on page 656).
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 *Configure Rules for an IP ACL* on page 658.

3. Click the **Add** button.
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 the **Add** button.
6. From the IP Binding Configuration screen, assign ACL ID 1 to the interface gigabit ports 2, 3, and 4, and assign a sequence number of 1 (See *Configure IP ACL Interface Bindings* on page 671).

   By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch.
7. Click the **Apply** button.
8. Use the IP Binding Table screen to view the interfaces and IP ACL binding information (See *View or Delete IP ACL Bindings in the IP ACL Binding Table* on page 673).

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.

9.3. 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 might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email 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 with 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 cannot 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.

managed switch 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 (the assignment of a policy to a directional interface)

9.3.1. 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 and so on)
- 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

9.3.2. 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 (*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.

9.3.3. 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.

9.3.3.1. 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 (such as the 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 can 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 can also be specified along with a QoS queue assignment.

9.3.4. 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 *Configure a DiffServ Class* on page 526.
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 *Configure a DiffServ Class* on page 526.
4. Click the **Apply** button.
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 *Configure DiffServ Policy* on page 533.

6. Click the **Add** button.

   The policy is added.

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 *Configure DiffServ Policy* on page 533.

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 the **Apply** button. (See *Configure the DiffServ Service Interface* on page 536.)

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 include 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.

9.4. 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 you might want 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 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 managed switch switches support a guest VLAN, which allows unauthenticated users 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 through the LAN. Port-based network access control allows the operation of a switch's ports to be controlled 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 when you 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 accesscontrol interaction:

1. **Authenticator**: A Port that enforces authentication before allowing access to services available through 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 for you to complete an authentication exchange.

managed switch 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.

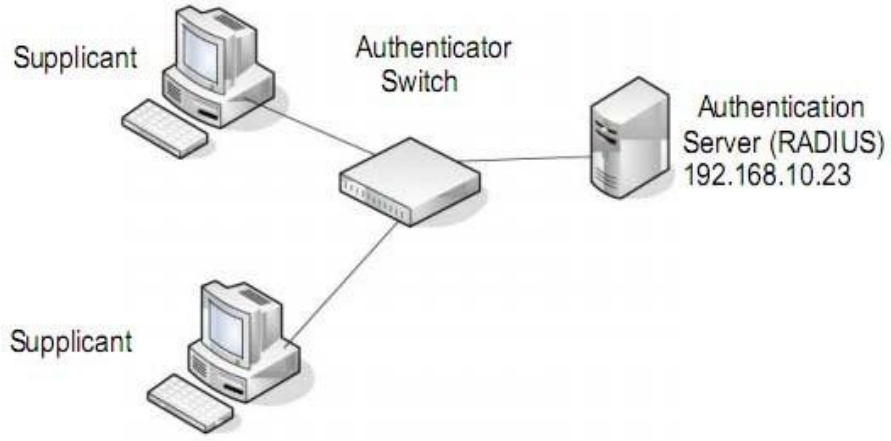


Figure 1. 802.1X Authentication Roles

9.4.1. 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 must 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 be Authorized. When the Port Control setting is Authorized, the port is unconditionally put in a force-Authorized state and does not require any authentication. When the Port Control setting is Auto, the authenticator PAE sets the controlled port mode
3. In the Guest VLAN field for ports 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 *Configure a Port Security Interface* on page 598 for information about the settings.
4. Click the **Apply** button.
5. From the 802.1X Configuration screen, set the Port Based Authentication State and Guest VLAN mode to Enable, and then the **Apply** button (See *Configure the Global Port Security Mode* on page 597).

   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 Overview* on page 545.
7. Click the **Add** button.
8. From the Authentication List screen, configure the default List to use RADIUS as the first authentication method (See *Configure a Login Authentication List* on page 555).

This example enables 802.1X-based port security on 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.

9.5. 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 through 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 without any 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 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 might 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.

9.5.1. MSTP Example Configuration

This example shows how to create an MSTP instance from the switch. The example network has three different 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.

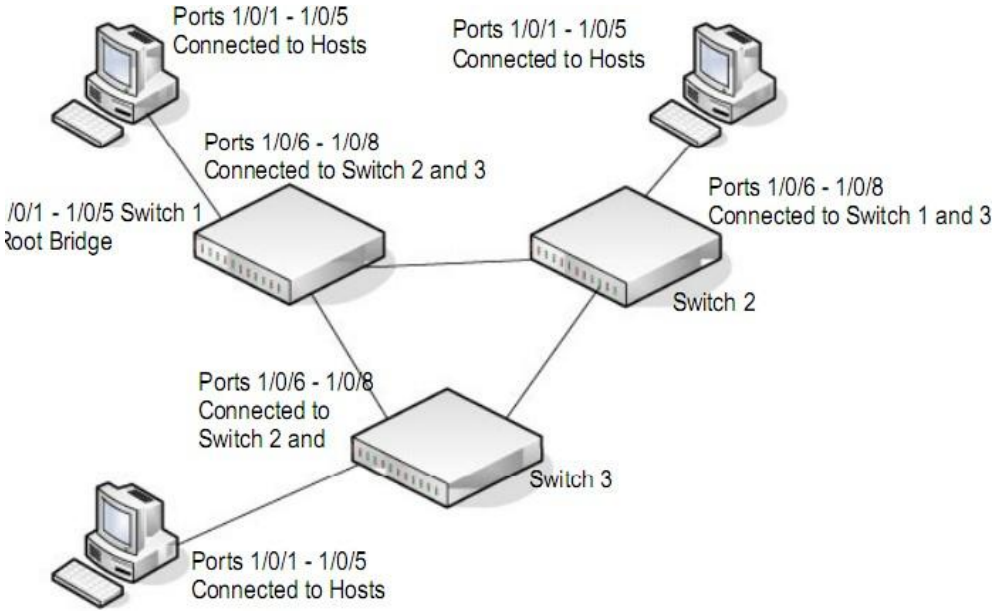


Figure 2. MSTP sample configuration

Perform the following procedures on each switch to configure MSTP:

1. Use the VLAN Configuration screen to create VLANs 300 and 500 (see *Configure Basic VLAN Settings* on page 195).
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 *Configure Basic VLAN Settings* on page 195).
3. From the STP Configuration screen, enable the Spanning Tree State option (see *Configure Advanced STP Settings* on page 231).

   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 are assigned the same bridge priority value, the switch with the lowest MAC address is elected as the root bridge (see *Configure CST Settings* on page 234).
5. From the CST Port Configuration screen, select ports 1/0/1–1/0/8 and select **Enable** from the **STP Status** menu (see *Configure CST Port Settings* on page 236).
6. Click the **Apply** button.
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 the **Apply** button.

   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 *Configure MST Settings* on page 240.
10. Click the **Add** button.
11. Create a second MST instance with the following settings
    - MST ID: 2
    - Priority: 49152
    - VLAN ID: 500
12. Click the **Add** button.

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 include 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.

10. Acronyms and Abbreviations

In most cases, acronyms and abbreviations are defined on first use in this document. Acronyms and abbreviations are also defined in the following table.

Table133. Acronyms and Abbreviations

Acronym	Definition
802.1x	IEEE 802.1x Authentication Protocol Standard
ACE	Access Control Entry
ACL	Access Control List
API	Application Programming Interface
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CLI	Command Line Interface
CoS	Class of Service
Default Gateway	The IP address of a router that a host can use as its first hop when the host does not know a more specific route to a given destination.
Default Route	A manually configured (*static*) route whose destination is 0.0.0.0/0.0.0.0 and therefore matches every packet's destination. A router uses a default route to forward packets that do not match a more specific route.
DHCP	Dynamic Host Configuration Protocol (RFC 2131, RFC3315). A mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DHCP Server	Dynamic Host Configuration Protocol Servers are servers that grant the address and do parameter assignment to requested clients in the network. Current interest is that these servers provide TFTP server and boot file information.
DLL	Data Link Layer
DNS Server	Domain Name System servers that provide the IP address mapping to the name of the hosts.
DSCP	Differentiated Services Code Point

Table134. Acronyms and Abbreviations (continued)

Acronym	Definition
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
ECMP	Equal Cost Multiple Paths
EEE	Energy Efficient Ethernet (from the IEEE 802.3az Energy Efficient Ethernet Task Force and IEEE 802.3az Energy Efficient Ethernet Study Group).
Host Interface	An IP interface that is not a routing interface. Only locally-originated packets are sent on a host interface. Only packets with a local destination are received. Host interfaces do not participate in dynamic routing protocols.
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internal Authentication Server
IGMP	Internet Group Management Protocol
In-band Interface	An IP interface that could be used for in-band management. Any IP interface other than the Out-of-Band port.
IP	Internet Protocol
IP Address Owner	The VRRP router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, and so on
IP Interface	An interface configured as an IP interface rather than a Layer 2 switching interface. An IP interface must be assigned one or more IP addresses. Also called a *Layer 3 interface*.
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDP	Industry Standard Discovery Protocol
ISID	Initiator-defined session identifier
L2	Layer 2 (networking)
L2	Layer 3 (networking)
LAG	Link Aggregation Group (IEEE standard)
LLDP	Link Layer Discovery Protocol
Local Route	A route to an attached subnet. A router creates a local route for each active, locally-configured IP address and uses the local route to reach other stations on the attached subnet.
LPI	Low-power Idle
MAB	MAC Authentication Bypass

Table135. Acronyms and Abbreviations (continued)

Acronym	Definition
MAC	Media Access Control
Management Interface	An external IP interface used to send and receive IP packets to configure and monitor the device.
Management VLAN	A VLAN configured to be used for management rather than control or data traffic.
MFDB	Multicast Forwarding Database
MIB	Management Information Base
MLAG	Multi-chassis Link Aggregation
MPLS	Multiprotocol Label Switching: A standard involving IP quality.
MVR	Multicast VLAN Registration
N/A	not applicable
NSF	Nonstop Forwarding
PAE	Port Access Entity
PDU	Protocol Data Unit
PIM-DM	Protocol-Independent Multicast Dense mode
PIM-SM	Protocol-Independent Multicast Sparse mode
Primary IP Address	An IP address selected from the set of real interface addresses. One possible selection algorithm is to always select the first address. VRRP advertisements are always sent using the primary IP address as the source of the IP packet.
PoE	Power over Ethernet. Corresponds to the IEEE 802.3AF standard which supports power delivery of up to 15.4W per port.
PoE+	Power over Ethernet Plus. Corresponds to the IEEE 802.3AT standard which supports power delivery of up to 34.2W per port.
PSE	Power Sourcing Equipment
QoS	Quality of Service
RADIUS	Remote Authentication Dial-in User Service
Routing Interface	An IP interface whose physical ports are front panel ports and associated with a VLAN. Packets received on a routing interface can be transmitted on a different VLAN than they were received on.
SDM	Switch Database Management
Service Port	An IP interface on an Ethernet interface that is separate from the front panel ports. The service port is dedicated to management. The service port has its own independent interface to the IP stack. The service port is a host interface.
SM	state machine

Table136. Acronyms and Abbreviations (continued)

Acronym	Definition
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
TFTP	Trivial File Transfer Protocol
TFTP Server	Trivial File Transfer Protocol Servers are servers that hold the requested configuration and/or image files for requested clients.
TLV	Type-Length-Value
UDLD	Uni-Directional Link Detection
UI	User Interface
UPoE	Universal Power over Ethernet. No IEEE standard exists yet for UPoE. UPoE supports power delivery of up to 60W per port.
USB	Universal Serial Bus
Virtual Router	An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a virtual router identifier and a set of associated IP address(es) across a common LAN. A VRRP router can backup one or more virtual routers
Virtual Router Backup	The set of VRRP routers available to assume forwarding responsibility for a virtual router if the current Master fails.
Virtual Router Master	The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP requests for these IP addresses. Note that if the IP address owner is available, then it will always become the Master.
VLAN	Virtual Local Area Network
VRRP Router	A router running the Virtual Router Redundancy Protocol. It can participate in one or more virtual routers.