NETGEAR ®

User Manual

S3300 Gigabit Ethernet Stackable Smart Switch

Model
GS728TX
GS728TXP
GS752TX
GS752TXP

Firmware Version 6.6.4

Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/download/.

(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/download/.)

For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.

See the regulatory compliance document before connecting the power supply.

For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.

By using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions. If you do not agree, return the device to your place of purchase within your return period.

Do not use this device outdoors. The PoE source is intended for intra building connection only.

Applicable to 6 GHz devices only: Only use the device indoors. The operation of 6 GHz devices is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

This switch is designed for indoor use only. If you want to connect to a device located outdoors, the outdoor device must be properly grounded and surge protected, and you must install an Ethernet surge protector inline between the switch and the outdoor device. Failure to do so can damage the switch.

WARNING: Before connecting this switch to outdoor cables or devices, see https://kb.netgear.com/000057103 for safety and warranty information.

Trademarks

© NETGEAR, Inc., NETGEAR, and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

Publication Part Number	Publish Date	Comments
202-12612-01	March 2022	Revised Mirroring. Updated the manual to the latest format.
202-11377-03	September 2017	Updated manual for release 6.6.4.
202-11377-02	June 2016	Updated manual to conform to firmware release v6.6.0.x.
202-11377-01	July 2014	First publication

Contents

Chapter 4   Configuring Routing

Chapter 7   Maintenance

Chapter 8   Monitoring the System

1
Getting Started

This manual describes how to configure and operate the S3300 Smart Switch family by using the web-based graphical user interface (GUI). The manual describes the software configuration procedures and explains the options available within those procedures. The S3300 switches are referred to as the NETGEAR switch throughout this document. The individual switches are:

- GS728TX (also referred to as S3300-28X)
- GS728TXP (also referred to as S3300-28X-PoE+)
- GS752TX (also referred to as S3300-52X)
- GS752TXP (also referred to as S3300-52X-PoE+)

This chapter contains the following sections:

> **Note:** The information in this manual applies to all switch models unless otherwise noted.

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

Note: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download. 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.

Enhanced Stacking Capability

In Release 6.6.4, two M4300 product series are added to enhance the stacking capability of S3300.

- The M4300-12X12F (XSM4324S) is a stackable, fully-managed L2+ Gigabit switch. This 24-port Gigabit Ethernet Layer 2 switch provides 12 * 10G Copper ports and 12 * 10G Fiber ports.

- The M4300-24X (XSM4324CS) is a stackable, fully-managed L2+ Gigabit switch. It has 24 port 10GBASE-T with 4 shared SFP+.

These are the existing M4300 series switches that have been re-configured to act as S3300 switches. The capabilities of the switches will match the S3300 capabilities.

S3300 models can stack, up to six switches high. On S3300 models, any of the four 10G ports can be configured as stacking ports. Two M4300 24-port 10G switches offer mixed stacking, respecting the same rules for consistency:

- Six-switches total height

- On M4300 10G models, a maximum of four 10G ports (any four from below the eight available ports) can be configured as stacking ports concurrently.

  - M4300-12X12F: port 9–12 and port 21–24
  - M4300-24X: port 17–24

In order to stack M4300 models with the S3300 models, you will need to procure standard version M4300 switches, and apply a special firmware image to downgrade them to S3300 software for compatibility and mixed stacking. If you later want to go back to M4300 software on the M4300 models running S3300 firmware, you can upgrade the M4300 models using the standard M4300 firmware image. For the procedure to upgrade the M4300/S3300 firmware, see Smart M4300/S3300 Firmware Upgrade Procedure on page 338.

Getting Started with the NETGEAR Switch

This chapter provides an overview of starting your NETGEAR switch and accessing the user interface. It also leads you through the steps to use the Smart Control Center (SCC) application, which can be downloaded to your computer.

This guide does not document the SCC application. Full documentation for SCC is found at http://docs.netgear.com/scc/enu/202-10685-01/index.htm.

Switch Management Interface

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

NETGEAR provides the Smart Control Center utility with this product. This program runs on a Windows-based computer and provides a front end that discovers the switches on your network segment (L2 broadcast domain). When you power up your switch for the first time, use the Smart Control Center to discover the switch and view the network information that has been automatically assigned to the switch by a DHCP server; or, if no DHCP server is present on the network, use the Smart Control Center to discover the switch and assign static network information.

In addition to enabling NETGEAR switch discovery, the Smart Control Center provides several utilities to help you maintain the NETGEAR switch on your network, such as password management, firmware upgrade, and configuration file backup. For more about the Smart Control Center utilities, see the *Smart Control Center User Guide at* http://docs.netgear.com/scc/enu/202-10685-01/index.htm.

Connect the Switch to the Network

To enable remote management of the switch through a web browser or SNMP, you must connect the switch to the network and configure it with network information (an IP address, subnet mask, and default gateway). The switch has a default IP address of 192.168.0.239 and a default subnet mask of 255.255.255.0.

To change the default network information on the switch, use one of the following three methods:

- **Dynamic assignment through DHCP**. DHCP is enabled by default on the switch. If you connect the switch to a network with a DHCP server, the switch obtains its network information automatically. You can use the Smart Control Center to discover the automatically assigned network information. For more information, see Discover a Switch in a Network with a DHCP Server on page 13.

- **Static assignment through the Smart Control Center**. If you connect the switch to a network that does not have a DHCP server, you can use the Smart Control Center to assign a static IP address, subnet mask, and default gateway. For more information, see Discover a Switch in a Network without a DHCP Server on page 14.

- **Static assignment by connecting from a local host**. If you do not want to use the Smart Control Center to assign a static address, you can connect to the switch from a host (administrative system) in the 192.168.0.0/24 network and change the settings by using the web management interface on the switch. For information about how to set the IP address on the administrative system so it is in the same subnet as the default IP address of the switch, see Configure the Network Settings on the Administrative System on page 16.

Discover a Switch in a Network with a DHCP Server

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

To install the switch in a network with a DHCP server:

1. Connect the switch to a network with a DHCP server.
2. Power on the switch by connecting its power cord.
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click the **Discover** button for the Smart Control Center to find your switch.

   A screen similar to the one shown in the following figure displays.
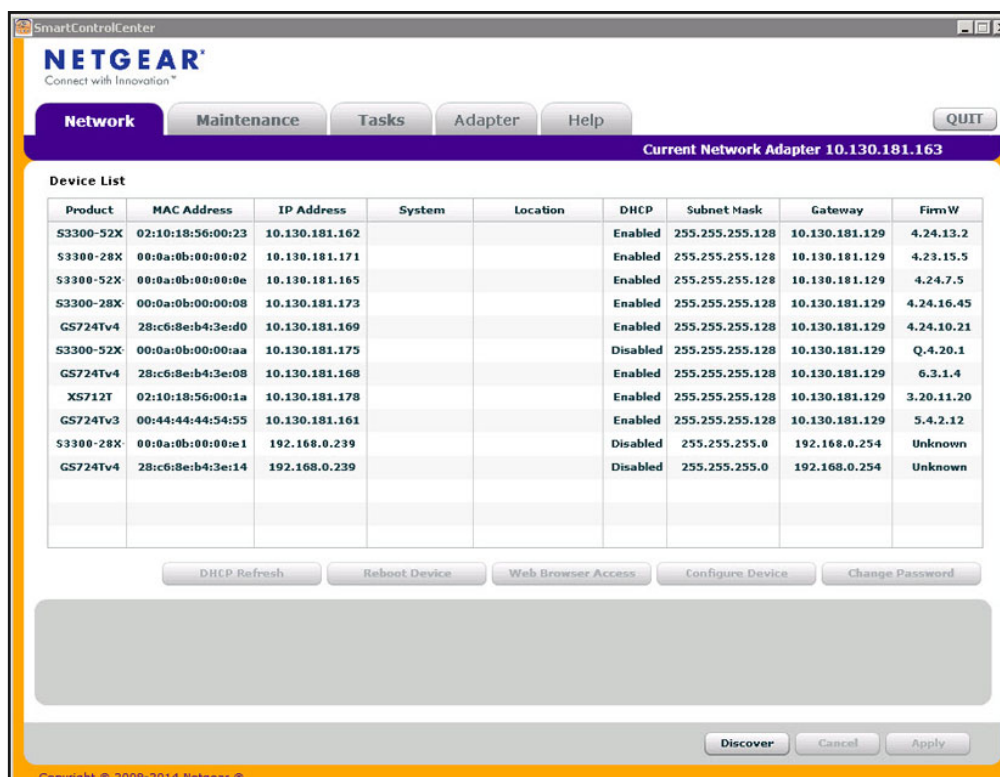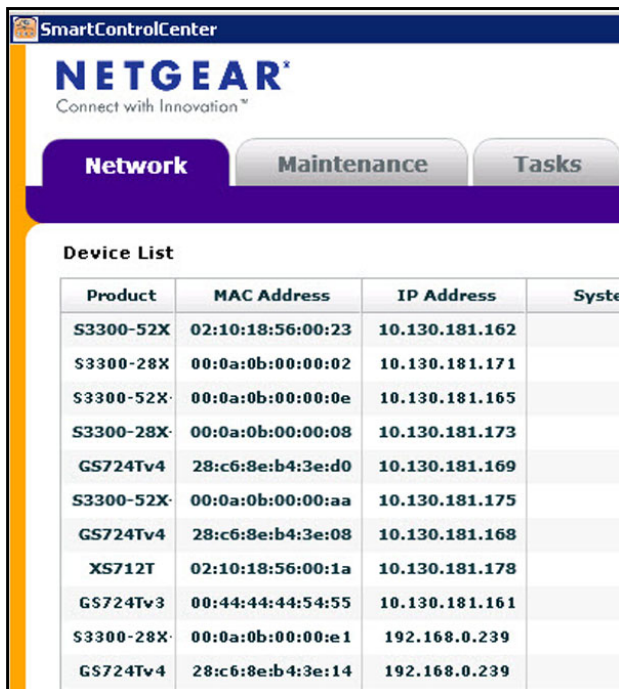
Figure 1. Smart Control Center - Discover

6. Make a note of the displayed IP address assigned by the DHCP server.

You will need this value to access the switch directly from a web browser (without using the Smart Control Center).

Figure 2. Smart Control Center - Device List

7. Select your switch by clicking the line that displays the switch, then click the **Web Browser Access** button.

   The Smart Control Center launches a browser that displays the login screen of the selected device.

   Use your web browser to manage your switch. The default password is *password*. For more information about the screen layout and options, see <u>Use the Web Interface on page 19</u>.

Discover a Switch in a Network without a DHCP Server

This section describes how to use the Smart Control Center to set up your switch in a network without a DHCP server. If your network has no DHCP service, you must assign a static IP address to your switch. If you choose, you can assign it a static IP address, even if your network has DHCP service.

To assign a static IP address:

1. Connect the switch to your existing network.
2. Power on the switch by connecting its power cord.

3. Install the Smart Control Center on your computer.

4. Start the Smart Control Center.

5. Click the **Discover** button for the Smart Control Center to find your S3300 switch.

   The utility broadcasts Layer 2 discovery packets within the broadcast domain to discover the switch.

6. Select the switch, then click the **Configure Device** button.

   The screen expands to display additional fields at the bottom.

7. Select the **Disabled** radio button to disable DHCP.

8. Enter the static switch IP address, gateway IP address, and subnet mask for the switch.
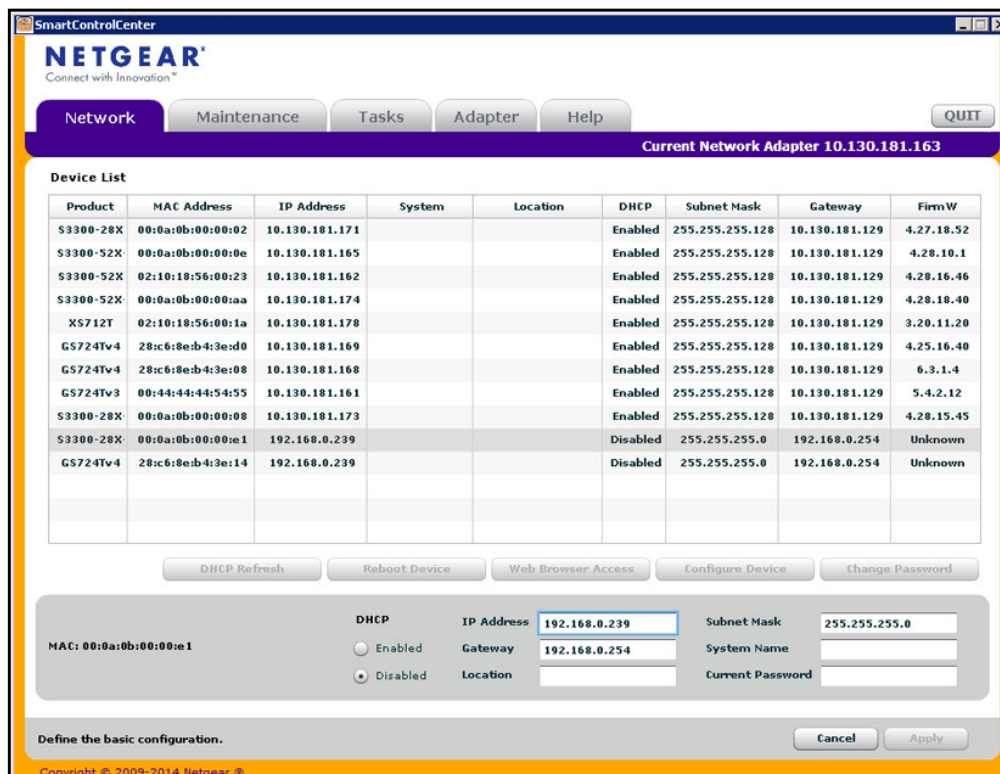
Figure 3. Smart Control Center - Configure Device

9. Type your password to continue with the configuration change.

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

10. Click the **Apply** button to configure the switch with the network settings.

Ensure that your computer and the switch are in the same subnet. Make a note of these settings for later use.

Configure the Network Settings on the Administrative System

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

The method to change the IP address on an administrative system varies depending on the operating system version. You need Windows Administrator privileges to change these settings. The following procedures show how to change the static IP address on a computer running a Microsoft Windows 7.

To modify the network settings on your administrative system:

1. Open the Control Panel and click the **Network and Sharing Center** option.
2. Click the **Local Area Connection** link.
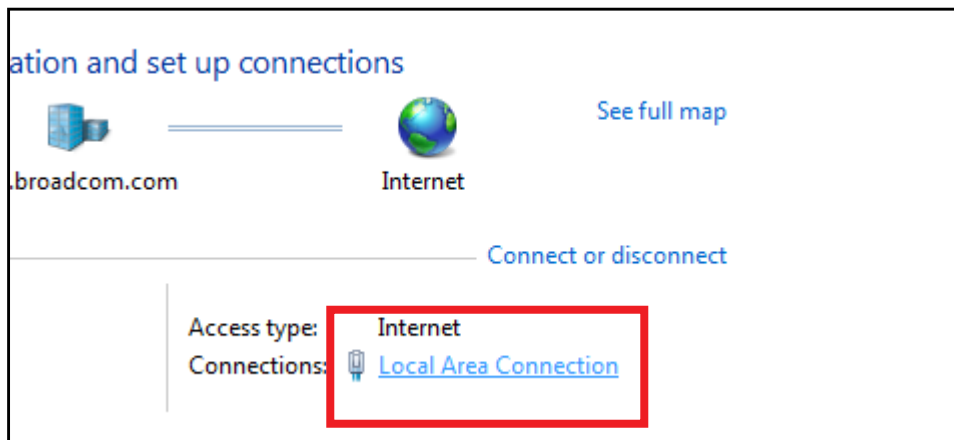
Figure 4. Local Area Connection

3. In the Local Area Connection Status window, click the **Properties** button.

    The Local Area Connection Properties window displays.
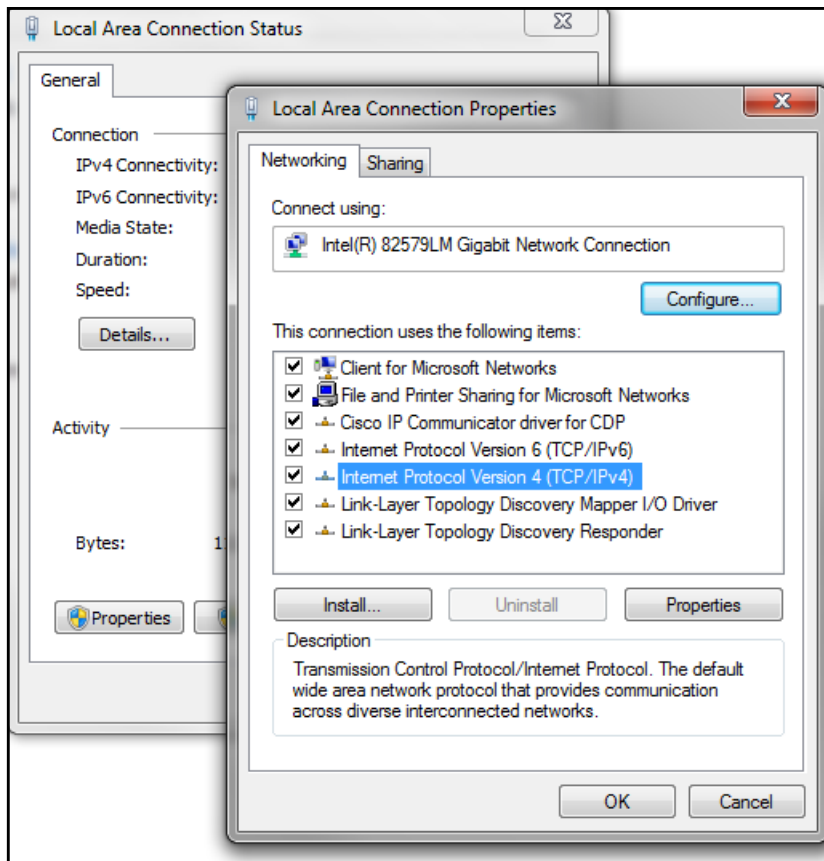
Figure 5. Local Area Connection Properties Window

4. Select the **Internet Protocol Version 4 (TCP/IPv4)** option, and then click the **Properties** button.

The Internet Protocol Version 4 (TCP/IPv4) Properties window appears.

5. Select the **Use the following IP address** option and set the IP address of the administrative system to an address in the 192.168.0.0 network, such as 192.168.0.200.

The IP address must be different from that of the switch but within the same subnet.

⚠️ **WARNING:**

When you change the IP address of your administrative system, you lose your connection to the rest of the network. Be sure to write down your current network address settings before you change them.
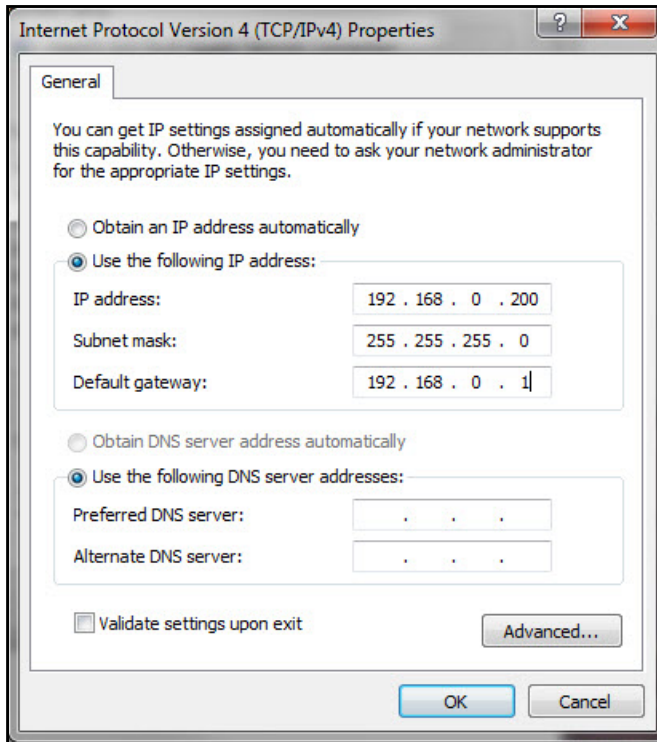
Figure 6. IP Address Settings

6. Click the **OK** button.

To configure a static address on the switch:

1. Use a straight-through cable to connect the Ethernet port on the administrative system directly to any port on the switch.

2. Open a web browser on your computer and connect to the management interface.

For more information, see Access the Management Interface from a Web Browser on page 19.

3. Change the network settings on the switch to match those of your network.

For more information, see IP Configuration on page 44.

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

Access the Management Interface from a Web Browser

To access the switch management interface, use one of the following methods:

- From the Smart Control Center, select the switch and click the **Web Browser Access** button. For more information, see the *Smart Control Center User Guide at* netgear.com/support/product/Smart%20Control%20Center%20(SCC).
- Open a web browser and enter the IP address of the switch in the address field.

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

Clicking the **Web Browser Access** button on the Smart Control Center or accessing the switch directly from your web browser displays the Login screen.

User Interfaces

The 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)

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

This manual describes how to use the web interface to manage and monitor the system.

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

Supported web browsers:

The following browsers were tested and support the web browser–based management interface. Later browser versions might function fine but were not tested. The supported web browsers include the following:

- Microsoft Internet Explorer (IE) versions 10-11
- Microsoft Edge
- Mozilla Firefox versions 40, 46.0.1
- Chrome version 45
- Safari on Windows OS 5.1, 6.0
- Safari on Mac OS 8.0

To log on to the web interface:

1. Open a web browser and enter the IP address of the switch in the web browser address field.

   The login screen displays.

2. Type the password in the Password field.

   The factory default password is **password**. Passwords are case-sensitive.

3. Click the **Login button**.

   After the system authenticates you, the System Information screen displays.

   The following figure shows the layout of the web interface.
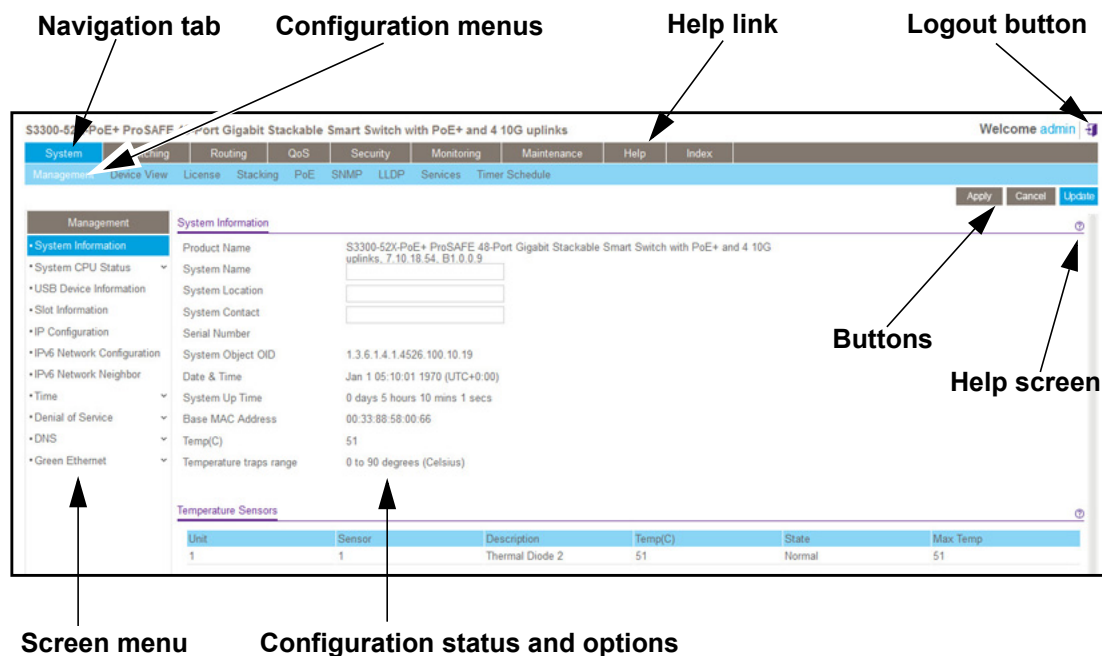
Figure 7. Smart Switch Web Interface

Navigation Tabs, Configuration Menus, and Screen Menu

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

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

The configuration screens for each feature are available as submenu links in the screen menu on the left side of the screen. Some items in the menu expand to reveal multiple submenu links, as the following figure shows.
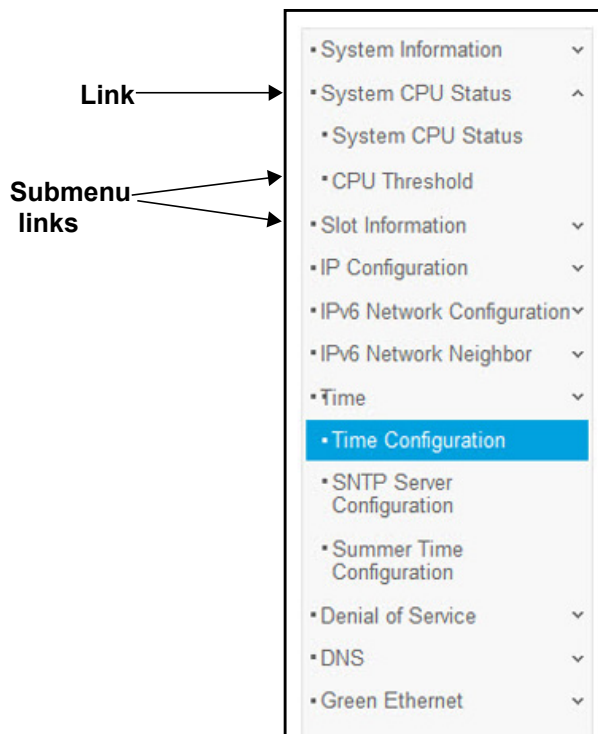
Figure 8. Submenu Links

When you click a menu item that includes multiple configuration screens, the item becomes preceded by a down arrow symbol and expands to display the additional submenu links.

Configuration and Status Options

The area directly under the configuration menus and to the right of the links displays the configuration information or status for the screen you select. On screens that contain configuration options, you can input information into fields or select options from drop-down lists.

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

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

Table 1. Command buttons

Button	Function
Add	Places the new item configured in the heading row of a table.
Apply	Sends the updated configuration to the switch. Configuration changes take effect immediately.
Cancel	Abandons the configuration changes on the screen and resets the data to the previous values.
Delete	Removes the selected item.
Refresh/Update	Refreshes/updates the screen with the latest information from the device.
Logout	Ends the session.
Clear	Clears all information and returns the switch to its default settings.

Device View

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

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

The following image shows the Device View of the S3300-28X.
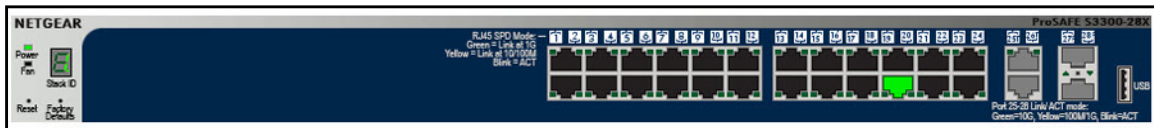
Figure 9. S3300-28X

The following image shows the Device View of the S3300-28X-PoE+.
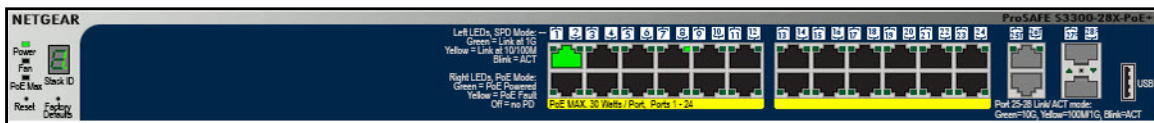
Figure 10. S3300-28X-PoE+

The following image shows the Device View of the S3300-52X.
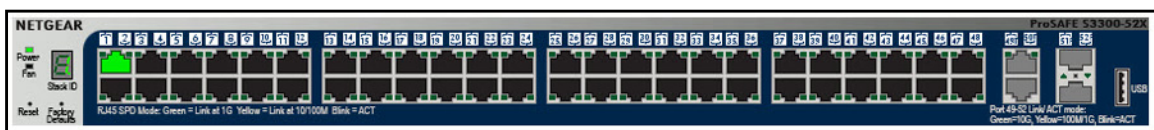
Figure 11. S3300-52X

The following image shows the Device View of the S3300-52X-PoE+.
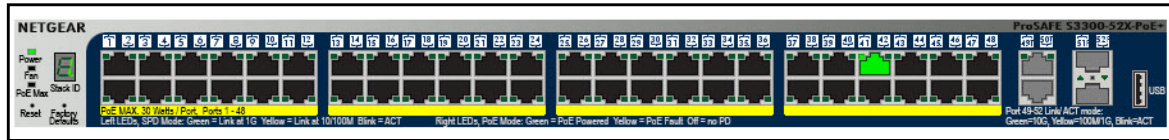
Figure 12. S3300-52X-PoE+

In the S3300, the four uplink ports can work in either Stacking mode or in Ethernet mode.

- By default those ports are in Stacking mode, and their color is gray.
- When these ports are configured in Ethernet mode, then their color is blank (not connected).

Depending upon the status of the port, the port color in Device View is either red, green, yellow, gray or black.

- Green and yellow indicate that the port is enabled.
- Red indicates that an error has occurred on the port or that the port is administratively disabled.
- Black indicates that no link is present.

When a link is present, the color of the port in the device view is either green or yellow:

- A green speed LED indicates operational ports at the following link speed:
    - 10G copper ports—10 Gbps
    - 1G copper ports—1000 Mbps (1 Gbps)
    - Fiber SFP+ ports—10 Gbps
- A yellow speed LED indicates operational ports at the following link speed:
    - 1G copper ports—10/100 Mbps
    - Fiber SFP+ ports—1000 Mbps

Click the port you want to view or configure to see a menu that displays statistics and configuration options, as shown in Figure 13 on page 24. Select the menu option to access the page that contains the configuration or monitoring options.
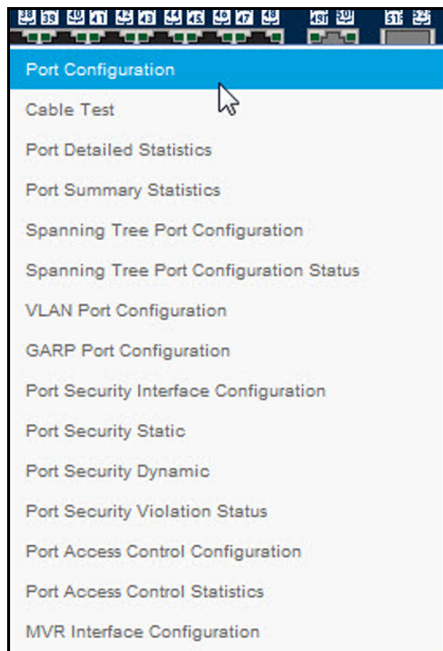
Figure 13. Device View S3300-52X Port Menu

If you click the graphic but do not click a specific port, the main menu appears, as Figure 14, Device View Main Menu shows. This menu contains the same option as the navigation menu at the top of the screen.
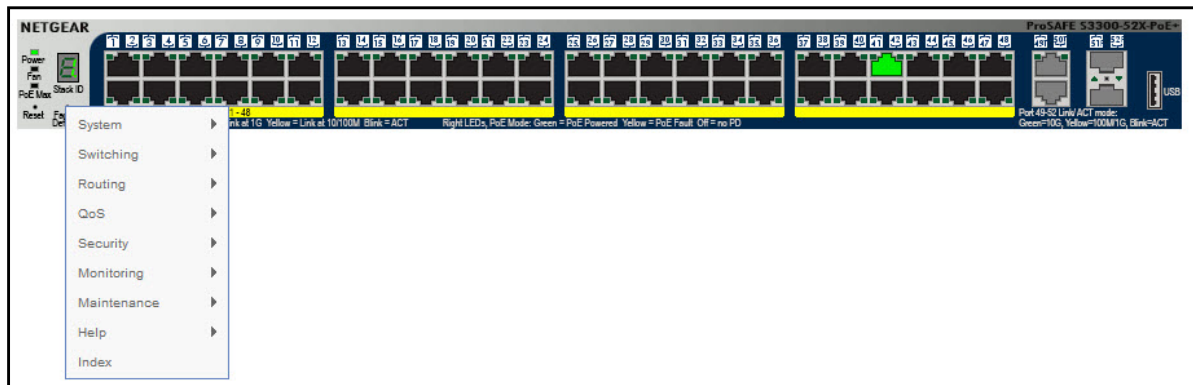
Figure 14. Device View Main Menu

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

Power/Status LED

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

• A solid green LED indicates that the power is supplied to the switch and operating normally.

- A solid yellow LED indicates that system is in the boot-up stage.
- No lit LED indicates that power is disconnected.

FAN Status LED

FAN status is indicated as follows:

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

Stack ID LED

The seven Segment LED displays the unit number in green. The dot LED on the bottom right glows when either the unit is a Stack Manager or Standalone (meaning that it is not connected in a Stack).

PoE Max LED

The PoE Max LED is for the S3300-28X-PoE+ and S3300-52X-PoE+ devices.

- Off indicates the system has more than 7 watts (W) of PoE power available for another PD device.
- A steady yellow LED indicates that less than 7W of PoE power is available.
- A blinking yellow LED indicates the device was active in the past two minutes.

Help Access

Every screen contains a button to launch online help, which contains information to assist in configuring and managing the switch. The online help screens are context-sensitive. For example, if the IP Addressing screen is open, the help topic for that screen displays if you click Help. Figure 7, Smart Switch Web Interface on page 20 shows the location of the Help link on the web interface.

User-Defined Fields

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

Table 2. Disallowed characters in user-defined fields

Character	Definition
\	Backslash
/	Forward slash
*	Asterisk
?	Question mark

Table 2. Disallowed characters in user-defined fields

Character	Definition
<	Less than
>	Greater than
|	Pipe

Use SNMPv3

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

The switch uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. All private MIBs begin with a hyphen (-) 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 after a successful login, displays the information you need to configure an SNMP manager to access the switch. To configure information for SNMPv1 or SNMPv2, see SNMP on page 91.

Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, the switch supports only one user which is **admin**; therefore there is only one profile that can be created or modified.

To configure authentication and encryption settings for the SNMPv3 admin profile by using the web interface:

1. Select **System** > **SNMP** > **SNMPv3** > **User Configuration**. The User Configuration screen displays.
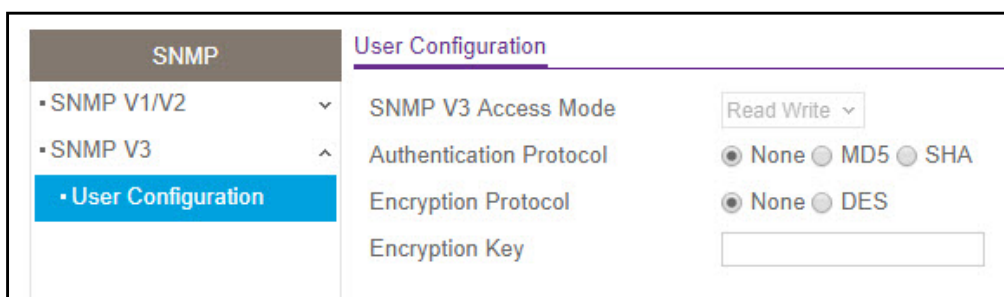
Figure 15. SNMPv3 User Configuration

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

2. To enable authentication, select an Authentication Protocol option.

If the authentication protocol is MD5 or SHA, the user login password will be used as SNMPv3 authentication password. To configure the login password, see Change Password on page 228.

3. To enable encryption:

    a. In the Encryption Protocol field, select the **DES** option to encrypt SNMPv3 packets using the DES encryption protocol.

    b. In the Encryption Key field, enter an encryption code of eight or more alphanumeric characters.

4. Click the **Apply** button.

Interface Naming Convention

The switch supports physical and logical interfaces. Interfaces are identified by their type and the interface number. All the physical ports are as follows:

- **GS728TX (S3300-28X)**: The S3300-28X Smart switch is a stackable small/medium business class switch.This 28-port Gigabit Ethernet Layer 2 switch provides ports as follows:
  - Ports 1–24 are 1GBaseT ports (RJ45)
  - Ports 25–26 are two dedicated 10GBaseT ports supporting 10G/1G/100M speeds
  - Ports 27-28 are two dedicated SFP+ ports supporting 10G and 1000M speeds

  The dedicated 10GBaseT and SFP+ ports can be configured as Ethernet ports or as stacking links. Up to six S3300 switches can be stacked together to form a larger device which can be managed at a single IP address. This switch supports management via IPv4 and IPv6, supports 32 Static Routes, and provides Green Ethernet (EEE) capability.

- **GS728TXP (S3300-28X-PoE+)**: The S3300-28X-PoE+ switch is identical to the S3300-28X except it supports PoE+ on the 24 1G ports.

- **GS752TX (S3300-52X)**: The S3300-52X Smart switch is a stackable small/medium business class switch. This 52-port Gigabit Ethernet Layer 2 switch provides the following:
  - Ports 1–48 are 1GBaseT ports (RJ45)
  - Ports 49–50 are two dedicated 10GBaseT ports supporting 10G/1G/100M speeds
  - Ports 51-52 are two dedicated SFP+ ports supporting both 10G and 1000M speeds

  The dedicated 10GBaseT and SFP+ ports can be configured as Ethernet ports or as stacking links. Up to six S3300 switches can be stacked together to form a larger device which can be managed at a single IP address. This switch supports management via IPv4 and IPv6, supports 32 Static Routes, and provides Green Ethernet (EEE) capability.

- **GS752TX (S3300-52X-PoE+)**: The S3300-52X-PoE+ Smart switch is identical to the S3300-52X except it supports PoE+ on the 48 1G ports.

The number of the port is identified on the front panel. You can configure the logical interfaces by using the software. The following table describes the naming convention for all interfaces available on the switch.

Table 3. Interface naming conventions

Interface	Description	Example
Physical	The physical ports include Gigabit ports and are numbered sequentially starting from one using the following format: X/gY or X/xgY. X for the unit ID, g is for a 1G port, xg is for a 10G port, and Y is the port number.	1/g1, 1/g2, 2/xg27
Link aggregation group (LAG)	LAG interfaces are logical interfaces that are only used for bridging functions.	l1, l2, l3
CPU management interface	This is the internal switch interface responsible for the switch base MAC address. This interface is not configurable and is always listed in the MAC Address Table.	c1

Configuring Interface Settings

For some features that allow you to configure interface settings, you can apply the same settings simultaneously to any of the following:

- A single port
- Multiple ports
- All ports
- A single LAG
- Multiple LAGs
- All LAGs
- Multiple ports and LAGs
- All ports and LAGs

Many of the screens that allow you to configure or view interface settings include links to display all ports, all LAGs, or all ports and LAGs on the screen.
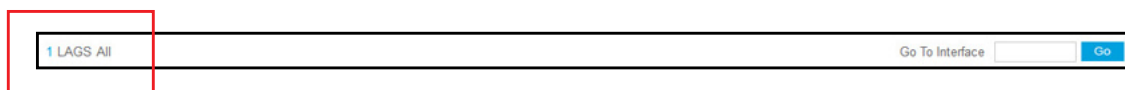
Figure 16. Links to Display Interfaces

Use these links as follows:

- To display all ports, click the **1** link.
- To display all LAGs, click the **LAGS** link.
- To display all ports and LAGs, click the **All** link.

The procedures in this section describe how to select the ports and LAGs to configure.

To configure a single port by using the Go To Interface field:

1. Ensure that the screen is displaying all ports, and not only the LAGs.
2. In the Go To Interface field, type the port number, for example g4.
3. Click the **Go** button.

   The check box associated with the interface is selected, the row for the selected interface is highlighted, and the interface number appears in the heading row.

Figure 17. Go To Interface Example

4. Configure the desired settings.
5. Click the **Apply** button.

   The settings you configure in the heading row are applied to the selected interface.

To configure a single LAG by using the Go To Interface field:

1. Click the **LAGS** link or the **All** link to display the LAGs.
2. In the Go To Interface field, type the LAG number, for example l3.
3. Click the **Go** button.

   The check box associated with the interface is selected, the row for the selected interface is highlighted, and the interface number appears in the heading row.

4. Configure the desired settings.
5. Click the **Apply** button.

   The settings you configure in the heading row are applied to the selected interface.

To configure a single port:

1. Ensure that the screen is displaying all ports, and not only the LAGs.
2. Select the check box next to the port number.

   The row for the selected interface is highlighted, and the interface number appears in the heading row.

3. Configure the desired settings.
4. Click the **Apply** button.

   The settings you configure in the heading row are applied to the selected interface.

To configure a single LAG:

1. Click the **LAGS** link or the **All** link to display the LAGs.
2. Select the check box next to the LAG number.

    The row for the selected interface is highlighted, and the interface number appears in the heading row.

3. Configure the desired settings.
4. Click the **Apply** button.

    The settings you configure in the heading row are applied to the selected interface.

To configure multiple ports:

1. Ensure that the screen is displaying all ports, and not only the LAGs.
2. Select the check box next to each port to configure.

    The row for each selected interface is highlighted.

Figure 18. Select Multiple Ports

3. Configure the desired settings.
4. Click the **Apply** button.

    The settings you configure in the heading row are applied to all selected interfaces.

To configure multiple LAGs:

1. Click the **LAGS** link or the **All** link to display the LAGs.
2. Select the check box next to each LAG to configure.

    The check box associated with each interface is selected, and the row for each selected interface is highlighted.

3. Configure the desired settings.
4. Click the **Apply** button.

    The settings you configure in the heading row are applied to all selected interfaces.

To configure all ports:

1. Ensure that the screen is displaying only ports, and not LAGs.
2. Select the check box in the heading row.

   The check box associated with every port is selected, and the rows for all ports are highlighted.

Figure 19. Select All Ports

3. Configure the desired settings.
4. Click the **Apply** button.

   The settings you configure in the heading row are applied to all ports.

To configure all LAGs:

1. Click the **LAGS** link to display only the LAG interfaces.
2. Select the check box in the heading row.

   The check box associated with every LAG is selected, and the rows for all LAGs are highlighted.

3. Configure the desired settings.
4. Click the **Apply** button.

   The settings you configure in the heading row are applied to all LAGs.

To configure multiple ports and LAGs:

1. Click the **All** link to display all ports and LAGs.
2. Select the check box associated with each port and LAG to configure.

   The rows for the selected ports and LAGs are highlighted.

3. Configure the desired settings.
4. Click the **Apply** button.

   The settings you configure in the heading row are applied to the selected ports and LAGs.

To configure all ports and LAGs:

1. Click the **All** link to display all ports and LAGs.
2. Select the check box in the heading row.

   The check box associated with every port and LAG is selected, and the rows for all ports and LAGs are highlighted.

3. Configure the desired settings.
4. Click the **Apply** button.

   The settings you configure in the heading row are applied to all ports and LAGs.

Online Help

The Help main navigation tab of the web management interface provides access to the menus that are described in the following sections:

- Support on page 32
- User Guide on page 32

Support

The Support screen provides access to the NETGEAR support website at support.netgear.com.

To access the support website from the web management interface:

1. Select **Help** > **Support**.

   The Support screen displays.

2. Click the **Apply** button to access the NETGEAR support site for the switch.

User Guide

The *S3300 Gigabit Ethernet Stackable Smart Switch User Manual* (the guide you are now reading) is available at the NETGEAR download center at https://www.netgear.com/support/download/.

To access the reference manual online from the web management interface:

1. Select **Help** > **User Guide**.
2. Click the **Apply** button to access the NETGEAR download center.
3. Enter the model number of the switch.
4. Locate the *S3300 Gigabit Ethernet Stackable Smart Switch User Manual* on the product support web screen.

Registration

To qualify for product updates and product warranty, NETGEAR encourages you to register your product. The first time that you connect to the switch while it is connected to the Internet, you have the option to register your product. At any time, you can register your product from the web management interface, or you can visit the NETGEAR website for registration at my.netgear.com/home.aspx.

To register the switch with NETGEAR:

1. Select **Help > Register**.

   The Registration screen displays.

2. Click the **Register** button.

   A pop-up window opens and displays the NETGEAR product registration web screen.

3. Follow the on-screen instructions to complete the product registration process.

2

Configure System Information

Use the features you access from the **System** navigation tab to define the switch's relationship to its environment. The **System** navigation tab provides access to the configuration menus described in the following sections:

- Management on page 35
- Device View on page 72
- License on page 72
- Switch Stack Configuration on page 73
- PoE on page 86
- SNMP on page 91
- LLDP on page 94
- Services on page 108
- Timer Schedule on page 127

Management

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

- System Information on page 35
- System CPU Status on page 39
- USB Device Information on page 42
- Slot Information on page 43
- IP Configuration on page 44
- IPv6 Network Configuration on page 46
- IPv6 Network Neighbor on page 48
- Time on page 49
- Denial of Service on page 58
- DNS on page 61
- Green Ethernet on page 63

System Information

After a successful login, the System Information screen displays. Use this screen to configure and view general device information.

To define a system name, location, and contact:

1. **Select System > Management > System Information.**

   The **System Information** screen displays.

System Information	
Product Name	S3300-28X-PoE+ ProSAFE 24-Port Gigabit Stackable Smart Switch with PoE+ and 4 10G uplinks, 6.4.0.11, B1.0.0.9
System Name	
System Location	
System Contact	
Serial Number	3TM1447X8004B
System Object OID	1.3.6.1.4.1.4526.100.10.17
Date & Time	Jan 1 00:21:29 1970 (UTC+0:00)
System Up Time	0 days 0 hours 21 mins 29 secs
Base MAC Address	08:BD:43:6B:61:5C
Temp(C)	48
Temperature traps range	0 to 90 degrees (Celsius)

   Figure 20. Management - System Information

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

3. Click the **Apply** button.

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

The following table describes the status information the System Information screen displays.

Table 4. System Information Screen Status Fields

Field	Description
Product Name	The product name that describes the switch.
Serial Number	The serial number of the switch.
System Object OID	The base object ID for the switch's enterprise MIB.
Date & Time	The current date and time.
System Up Time	The number of days, hours, and minutes since the last system restart.
Base MAC Address	The universally assigned network address.
Temp (C)	The general temperature of the switch in degrees Celsius.
Temperature Traps Range	Identifies the minimum and maximum degrees of the temperature traps range.

Note: NSDP supports TLV for Serial Number.

TLV	Value	Description
Serial Number	1…21	For Smart Switch: 1 Byte: 0-Invalid 1-Valid Next 20 bytes: Serial number string

Temperature Sensors

This screen shows the temperature of different system sensors. The temperature is instant and can be refreshed when you press the **Update** button.

Temperature Sensors					⑦
Unit	Sensor	Description	Temp(C)	State	Max Temp
1	1	Thermal Diode 1	48	Normal	48

Figure 21. System Information - Temperature Sensors Status

The following table describes the status information displayed in the Temperature Sensors section of the System Information screen.

Table 5. System Information - Temperature Sensors Status Fields

Field	Description
Unit	The unit number in the stack.
Sensor	The temperature sensor for the given unit.
Description	The description of the temperature sensor.
Temp (C)	The current temperature of the specified sensor of the switch in degrees Celsius.
State	The unit temperature state.
Max Temp	The maximum temperature of the CPU and MACs. The maximum temperature depends on the actual hardware.

Fans

The screen shows the status of the fans. These fans remove the heat generated by the power, CPU and other chipsets.

Fans							⑦
Unit	FAN	Description	Type	Speed	Duty level	State	
1	1	FAN-1	Fixed	Not Supported	27	Not Applicable	
1	2	FAN-2	Fixed	Not Supported	27	Not Applicable	

Figure 22. System Information - Fan Status

The following table describes the status information displayed in the Fans section of the System Information screen.

Table 6. System Information - Fans Status Fields
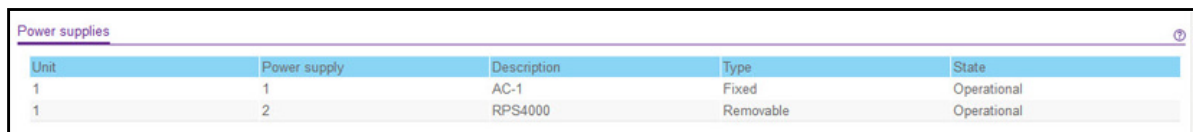
Field	Description
Unit	The unit number in the stack.
Fan	The fan index used to identify the fan for the given stack member.
Description	The description of the temperature sensor.

Table 6. System Information - Fans Status Fields (continued)

Field	Description
Type	Specifies whether the fan module is fixed or removable.
Speed	The fan speed.
Duty Level	The duty level of the fan.
State	Specifies whether the fan is running or stopped.

Power Supplies

This screen shows the power supplies status.

Figure 23. System Information - Power Supplies Status
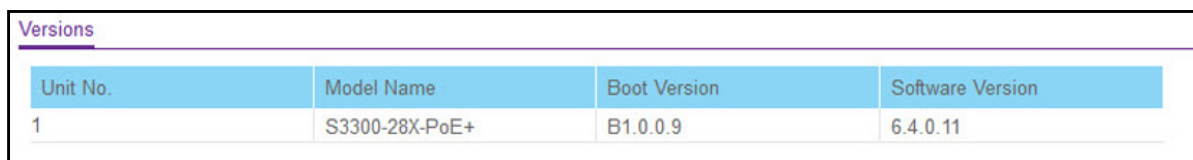
The following table describes the status information displayed in the Power Supplies section of the System Information screen.

Table 7. System Information - Power Supplies Status Fields

Field	Description
Unit	The unit number in the stack.
Power Supply	The power supply index used for the given stack member.
Description	The description of the power supply.
Type	Indicates whether the power supply is fixed or removable.
State	Specifies whether the power modules is operational or stopped.

Versions

This screen displays the software version of each device.

Figure 24. System Information - Versions Information

The following table describes the information displayed in the Versions section of the System Information screen.

Table 8. System Information - Versions Information Fields

Field	Description
Unit No.	The unit number of the switch.
Model Name	The model name of the switch.
Boot Version	The version of the boot code on the switch.
Software Version	The software version currently running on the switch.

System CPU Status

Use the **System CPU Status** screen to monitor the CPU, memory resources, and utilization patterns across various intervals to assess the performance, load, and stability parameters of member units.

To display the System CPU Status information:

Select System > Management > System CPU Status > System CPU Status

The **System CPU Status** screen displays **CPU Memory Status** and **CPU Utilization** information.

To display a member unit's CPU status information:

1. **Select System > Management > System CPU Status > System CPU Status**
2. In the **CPU Utilization > Unit No.** field, select a unit number. Select **All** to run CPU Utilization information for all units.
3. The unit's Memory Utilization Report is displayed.

The **CPU Utilization** screen displays the memory information, task-related information and percentage of CPU utilization per task.
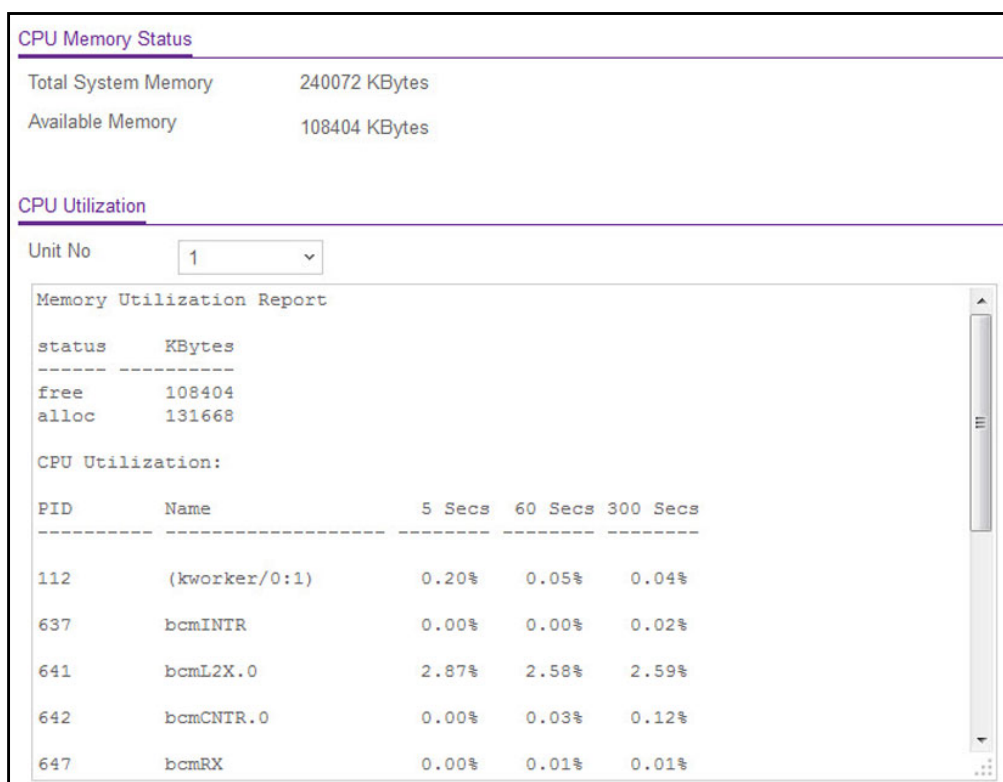
Figure 25. System CPU Status - Unit CPU Utilization

Table 9 describes the information that the System CPU Status screen displays.

Table 9. System CPU Status > CPU Memory Status

Field	Description
CPU Memory Status	
Total System Memory	The total memory of the switch in KBytes.
Available Memory	The available memory space for the switch in KBytes.
CPU Utilization	
Unit No	Select the Unit to display the CPU Utilization information. Select All to display the CPU Utilization information for all units.

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

To configure the CPU Threshold information:

Select System > Management > System CPU Status > CPU Threshold.

Figure 26. CPU Threshold

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

1. Define the CPU Threshold fields listed in <u>Table 10</u>.

Table 10. System CPU Status > CPU Threshold

Field	Description
Rising Threshold	Notification is generated when the total CPU utilization exceeds this threshold value over the configured time period. The range is 1 to 100.
Rising Interval	The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds.
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 or less than Rising threshold value. The Falling utilization threshold notification is made only if previously a Rising threshold notification was done. 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. Range is 1 to 100.
Falling Interval	The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiple of 5 seconds.
Free Memory Threshold	This is non-configurable data and is the CPU Free Memory Threshold value.

2. Click the **Apply** button.

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

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

USB Device Information

Use the **USB Device Information** screen to display the USB device status, memory statistics, and directory details.

To display the USB Device Information page:

1. **Select System > Management >** USB Device Information.
2. The **USB Device Information** screen displays as shown in Figure 27, USB Device Information.
3. Click **Update** to update the information on the page to the latest data on the switch.

Note: The system only detects and manages the USB device installed in the master unit.

The limitations for the USB Device supported on the S3300 are as follows:

- The USB disk should comply for USB 2.0.
- The USB disk should have a filetype of FAT32 or VFAT. NTFS is not supported.
- The write/read speed is about 1 Mbps due to a hardware limitation.

USB Device Information		
USB Device Details		
Device Status		
USB Memory Statistics		
Total Size		
Bytes Used		
Bytes Free		
USB Directory Details		
File Name	File Size	Modification Time

Figure 27. USB Device Information

Table 11 describes the nonconfigurable information that the USB Device Information screen displays.

Table 11. USB Device Information

Field	Description
USB Device Details	
Device Status	Specifies the current status of device. • **Active** if the device is USB plugged in and recognized by the switch. • **Inactive** if the device is not mounted. • **Invalid** if the device is not present or an invalid device is plugged in.
USB Memory Statistics	
Total Size	Displays the USB flash device storage size in bytes.
Bytes Used	Displays the size of memory used on the USB flash device.
Bytes Free	Displays the size of memory free on the USB flash device.
USB Directory Details	
File Name	Displays the name of the file stored in the USB flash drive.
File Size	Displays the size, in bytes, of the file stored in the USB flash drive.
Modification Time	Displays the last modification time of the file stored in the USB flash drive.

Slot Information

Use the Slot Information screen to display details about the different slots in the different units in the switch stack.

To display the slot Information:

Select System > Management > Slot Information.

Table 12 describes the information that the Slot Information screen displays.

Table 12. Slot Information

Field	Description
Slot Summary	
Slot	Identifies the slot using the format unit/slot.
Status	Displays whether the slot is empty or full.
Administrative State	Displays whether the slot is administratively enabled or disabled.
Power State	Displays whether the slot is powered on or not.
Configured Card Model ID	Displays the model ID of the card configured for the slot.

Table 12. Slot Information (continued)

Field	Description
Configured Card Description	Displays the description of the card configured for the slot.
Inserted Card Model ID	Displays the model ID of the card inserted into the slot.
Inserted Card Description	Displays the description of the card inserted into the slot.
Card Power Down	Displays whether the card in the slot is powered down.
Card Pluggable	Displays whether the inserted card is pluggable or not.
Supported Card	
Card Model	Displays the list of models of all cards that can be supported.
Card Index	Displays the index assigned to the selected card type.
Card Type	Displays the hardware type of this supported card. This is a 32-bit data field.
Card Descriptor	Displays a data field used to identify the supported card.
Supported Switch	
Switch Model ID	Displays the list of models of all supported switches.
Switch Index	Displays the index assigned to the selected switch.
Management Preference	Displays management preference of the supported switch.

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

IP Configuration

Use the IP Configuration screen to configure network information for the management interface, which is the logical interface used for in-band connectivity with the switch through any of the switch's front-panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

To configure the network information for the management interface:

1. Select **System > Management > IP Configuration**.

Figure 28. IP Configuration

2. Select the appropriate radio button to determine how to configure the network information for the switch management interface:

- **Dynamic IP Address (DHCP)**. Specifies that the switch must obtain the IP address through a DHCP server.

- **Dynamic IP Address (BOOTP)**. Specifies that the switch must obtain the IP address through a BootP server.

- **Static IP Address**. Specifies that the IP address, subnet mask, and default gateway must be manually configured. Enter this information in the fields below this radio button.

3. If you selected the Static IP Address option, configure the following network information:

- **IP Address**. The IP address of the network interface. The factory default value is 192.168.0.239. Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.

- **Subnet Mask**. The IP subnet mask for the interface. The factory default value is 255.255.255.0.

- **Default Gateway**. The default gateway for the IP interface. The factory default value is 192.168.0.254.

4. Specify the VLAN ID for the management VLAN.

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

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

Note: Make sure that the VLAN to be configured as the management VLAN exists, and make sure that the PVID of at least one port that is a port of the VLAN is the same as the management VLAN ID. For information about creating VLANs and configuring the PVID for a port, see VLANs on page 139.

The management VLAN has the following requirements:

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

5. Click the **Apply** button.

IPv6 Network Configuration

Use the IPv6 Network Configuration screen to configure the IPv6 network interface, which is the logical interface used for in-band connectivity with the switch through all of the switch's front-panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

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

- IPv6 auto configuration
- DHCPv6

When in-band connectivity is established, IPv6 information can be changed using SNMP-based management or web-based management

To configure the network information for an IPv6 network:

1. Select **System** > **Management** > **IPv6 Network Configuration**.

Figure 29. IPv6 Network Configuration
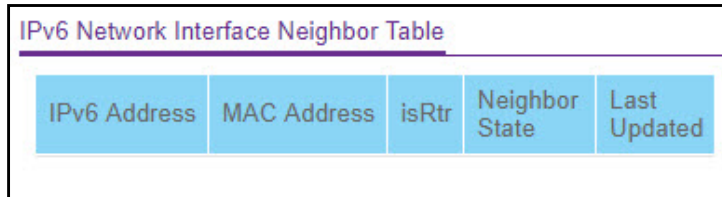
2. Next to **Admin Mode**, ensure that the **Enable** radio button is selected.

3. Determine how the switch acquires an IPv6 address:

   - **IPv6 Address Auto Configuration Mode**. When this mode is enabled, the network interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of router advertisement messages. When this mode is disabled, the network interface will not use the native IPv6 address auto configuration features to acquire an IPv6 address. Auto configuration can be enabled only when DHCPv6 is not enabled on any of the management interfaces.

   - **DHCPv6**. Next to Current Network Configuration Protocol, select **DHCPv6** to enable the DHCPv6 client on the interface. The switch attempts to acquire network information from a DHCPv6 server. Selecting None disables the DHCPv6 client on the network interface. When DHCPv6 is enabled, the DHCPv6 Client DUID field displays the client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.

4. In the IPv6 Gateway field, specify the default gateway for the IPv6 network interface.

   The gateway address is in IPv6 global or link-local address format.

5. (Optional) Configure one or more static IPv6 addresses for the management interface.

   a. In the IPv6 Prefix/Prefix Length field, specify the static IPv6 prefix and prefix to the IPv6 network interface.

      The address is in the global address format.

   b. In the EUI64 list, select **True** to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or select **False** to omit the EUI flag.

   c. Click the **Add** button.

6. Click the **Apply** button.

IPv6 Network Neighbor

Use the IPv6 Network Neighbor screen to view information about the IPv6 neighbors the device has discovered through the network interface by using the Neighbor Discovery Protocol (NDP).

To display the IPv6 Network Neighbor screen:

Select **System** > **Management** > **IPv6 Network Neighbor**.

Figure 30. IPv6 Network Neighbor

Table 13 describes the information the IPv6 Network Neighbor screen displays about each IPv6 neighbor that the switch has discovered.

Table 13. IPv6 neighbor table fields

Field	Description
IPv6 Address	The IPv6 address of the neighbor.
MAC Address	The MAC address associated with an interface.
IsRtr	Indicates whether the neighbor is a router. If the neighbor is a router, the value is True. If the neighbor is not a router, the value is False.
Neighbor State	The state of the neighbor cache entry. The following are the states for dynamic entries in the IPv6 neighbor discovery cache: • Reach. The neighbor is reachable through the network interface. • Stale. The neighbor is not known to be reachable, and the switch will begin the process to reach the neighbor. • Delay. The neighbor is not known to be reachable, and upper-layer protocols are attempting to provide reachability information. • Probe. The neighbor is not known to be reachable, and the device is attempting to probe for this neighbor. • Unknown. The reachability status cannot be determined.
Last Updated	The amount of time that has passed since the neighbor entry was last updated.

Time

The switch supports the Simple Network Time Protocol (SNTP). You can also set the system time manually.

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

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

Information received from SNTP servers is evaluated based on the time level and server type. SNTP time definitions are assessed and determined by the following time levels:

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

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

Polling for unicast information is used for contacting a server for which the IP address is known. SNTP servers that have been configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the SNTP Server Configuration screen.

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

Time Configuration

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

To manually configure the time:

1. Select **System** > **Management** > **Time** > **Time Configuration**.

Figure 31. Time Configuration

2. Next to Clock Source, select **Local**.

---

3. In the Date field, enter the date in the DD/MM/YYYY format.

4. In the Time field, enter the time in HH:MM:SS format.

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

---

5. Click the **Apply** button.

To configure the time by using SNTP:

1. Select **System** > **Management** > **Time** > **Time Configuration**.

2. Next to Clock Source, select the **SNTP** radio button.

   The screen refreshes and displays the SNTP Global Configuration screen.

Figure 32. Time > SNTP Global Configuration

3. Next to Client Mode, select the mode of operation of the SNTP client:
   - Disable. SNTP is not operational. No SNTP requests are sent from the client nor will any received SNTP messages be 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 **Disable.**

4. If the SNTP client mode is **Unicast**, use the SNTP Server Configuration screen to add the IP address or DNS name of one or more SNTP servers for the switch to poll.

   For more information, see SNTP Server Configuration on page 54.

5. 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 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 OS.

6. In the Unicast Poll Interval field, specify 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.

7. In the Broadcast Poll Interval field, specify the number of seconds between broadcast poll requests expressed as a power of two when configured in broadcast mode. Broadcasts received prior to the expiry of this interval are discarded. The allowed range is 6 to 10. The default value is 6.

8. In the Unicast Poll Timeout field, specify 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.

9. In the Unicast Poll Retry field, specify the number of times to retry a request to an SNTP server after the first timeout 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.

10. When using SNTP/NTP time servers to update the switch's clock, the time data received from the server is based on Coordinated Universal Time (UTC) which is the same as Greenwich Mean Time (GMT). This may not be the time zone in which the switch is located. Use the Time Zone Name field to configure a time zone specifying the number of hours, and optionally the number of minutes, difference from UTC with Offset Hours and Offset Minutes. The time zone can affect the display of the current system time. The default value is UTC.

11. Use the Offset Hours field to specify the number of hours difference from UTC. See the description for Time Zone Name in Step 10 above for more information. The allowed range is –12 to 13. The default value is 0.

12. In the Offset Minutes field, specify the number of minutes difference from UTC. See the description for Time Zone Name in Step 10 above for more information. The allowed range is 0 to 59. The default value is 0.

13. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

The **SNTP Global Status** table on the **System** > **Management** > **Time** > **Time Configuration** screen displays information about the system's SNTP client.

SNTP Global Status

Version	4
Supported Mode	Unicast and Broadcast
Last Update Time	Jan 1 00:00:00 1970 (UTC+0:00)
Last Attempt Time	Jan 1 00:00:00 1970 (UTC+0:00)
Last Attempt Status	Other
Server IP Address	
Address Type	Unknown
Server Stratum	0
Reference Clock Id	
Server Mode	Reserved
Unicast Server Max Entries	3
Unicast Server Current Entries	0
Broadcast Count	0

Figure 33. Time > SNTP Global Status

The following table describes the SNTP Global Status fields.

Table 14. Time Configuration status fields

Field	Description
Version	Specifies the SNTP version the client supports.
Supported Mode	Specifies the SNTP modes the client supports. Multiple modes can be supported by a client.
Last Update Time	Specifies the local date and time (UTC) the SNTP client last updated the system clock.
Last Attempt Time	Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.

Table 14. Time Configuration status fields (continued)

Field	Description
Last Attempt Status	Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes: • Other. The status of the last request is unknown. • Success. The SNTP operation was successful, and the system time was updated. • Request Timed Out. After an SNTP request was sent to an SNTP server, the response timer expired before a response from the server was received. • 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 by the leap indicator field on the SNTP message. • Server Kiss Of Death. The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Server IP Address	Specifies the IP address of the server for the last received valid packet. If no message has been received from any server, an empty string is shown.
Address Type	Specifies the address type of the SNTP server address for the last received valid packet.
Server Stratum	Specifies the claimed stratum of the server for the last received valid packet.
Reference Clock Id	Specifies the reference clock identifier of the server for the last received valid packet.
Server Mode	Specifies the mode of the server for the last received valid packet.
Unicast Sever Max Entries	Specifies the maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	Specifies the number of current valid unicast server entries configured for this client.
Broadcast Count	–

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

SNTP Server Configuration

Use the SNTP Server Configuration screen to view and modify information for adding and modifying Simple Network Time Protocol SNTP servers.

To configure a new SNTP server:

1. Select **System** > **Management** > **Time** > **SNTP Server Configuration**.

Figure 34. SNTP Server Configuration

2. From the Server Type list, select the type of SNTP address to enter in the Address field, which is either an IP address (IPv4) or hostname (DNS).

3. In the Address field, specify the IP address or the host name of the SNTP server.

4. If the UDP port on the SNTP server to which SNTP requests are sent is not the standard port (123), specify the port number.

5. In the Priority field, specify the order in which to query the servers.

   The SNTP client on the device continues sending SNTP requests to different servers until a successful response is received or all servers are exhausted. The request is sent to an SNTP server with a priority value of 1 first, then to a server with a priority value of 2, and so on. If more than one server has the same priority, the SNTP client contacts the servers in the order that they appear in the table.

6. In the Version field, specify the NTP version running on the server.

7. Click the **Add** button.

8. Repeat the previous steps to add additional SNTP servers.

   You can configure up to three SNTP servers.

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

Table 15. SNTP Server Status Fields

Field	Description
Address	Specifies all the existing server addresses.
Last Update Time	Specifies the local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	Specifies the local date and time (UTC) that this SNTP server was last queried.
Last Attempt Status	Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes: • Other. The status of the last request is unknown, or no SNTP responses have been received. • Success. The SNTP operation was successful, and the system time was updated. • Request Timed Out. After an SNTP request was sent to an SNTP server, the response timer expired before a response from the server was received. • 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 by the leap indicator field on the SNTP message. • Server Kiss Of Death. The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Requests	Specifies the number of SNTP requests made to this server since the last reboot.
Failed Requests	Specifies the number of failed SNTP requests made to this server since the last reboot.

To remove an SNTP server:

1. Select the check box next to the configured server to remove.
2. Click the **Delete** button.

To change the settings for an existing SNTP server:

1. Select the check box next to the configured server.
2. Specify new values in the available fields.
3. Click the **Apply** button.

Daylight Saving Configuration

Use the Daylight Saving Time (DST) Configuration screen to configure settings for daylight saving time. Used in some countries around the world, daylight saving time is the practice of temporarily advancing clocks during the summer months. Typically clocks are adjusted forward one or more hours near the start of spring and are adjusted backward in autumn.

To configure the daylight saving settings:

1. Select **System** > **Management** > **Time** > **Daylight Saving Configuration**.

Figure 35. Daylight Saving Configuration

2. Next to **Daylight Saving**, select one of the following options:
   - Disable. Use this option to disable Daylight Saving Time (DST).
   - **Recurring**. Use this option to configure Recurring Daylight Saving. Summer time occurs at the same time every year. The start and end times and dates for the time shift must be manually configured.
   - **Recurring EU**. Use this option to configure Recurring EU Daylight Saving. The system clock uses the standard recurring summer time settings used in countries in the European Union. When this field is selected, the rest of the applicable fields on the screen are automatically populated and cannot be edited.
   - **Recurring USA**. Use this option to configure Recurring USA Daylight Saving. The system clock uses the standard recurring daylight saving time settings used in the United States. When this field is selected, the rest of the applicable fields on the screen are automatically populated and cannot be edited.
   - **Non Recurring**. Use this option to configure Non-recurring Daylight Saving. Summer time settings are in effect only between the start date and end date of the specified year. When this mode is selected, the summer time settings do not repeat on an annual basis.

3. The following fields are displayed only when Daylight Saving is **Recurring**, or **Recurring EU,** or **Recurring USA**. Use the fields to set the start and end times for the time shift:
   - **Begins At**. From the appropriate lists, select the Start values of date and time on which Daylight Saving begins:
     - **Week**. Use this field to configure the start week.
     - **Day**. Use this field to configure the start day.

- **Month**. Use this field to configure the start month.

- **Hours**. Use this field to configure the start hours.

- **Minutes**. Use this field to configure the start minutes.

- **Ends At**. From the appropriate lists, select the End values of date and time on which Daylight Saving ends.

  - **Week**. Use this field to configure the end week.

  - **Day**. Use this field to configure the end day.

  - **Month**. Use this field to configure the end month.

  - **Hours**. Use this field to configure the end hours.

  - **Minutes**. Use this field to configure the end minutes.

4. In the **Offset** field, specify the number of minutes to shift the daylight saving time from the standard time. The valid range is 1 to 1440 minutes.

5. In the **Zone** field, specify the acronym associated with the time zone when daylight saving time is in effect.

    This field is not validated against an official list of time zone acronyms.

6. The fields below are visible only when Daylight Saving (DST) is **Non Recurring**. Use the fields to configure the start and end values of date and time:

    - **Begins At**. From the appropriate lists, select the Start values of date and time:

      - **Month**. Use this field to configure the start month.

      - **Date**. Use this field to configure the start date.

      - **Year**. Use this field to configure the start year.

      - **Hours**. Use this field to configure the start hours.

      - **Minutes**. Use this field to configure the start minutes.

    - **Ends At**. From the appropriate lists, select the End values of date and time.

      - **Month**. Use this field to configure the end month.

      - **Date**. Use this field to configure the end date.

      - **Year**. Use this field to configure the end year.

      - **Hours**. Use this field to configure the end hours.

      - **Minutes**. Use this field to configure the end minutes.

7. In the **Offset** field, specify the number of minutes to shift the daylight saving time from the standard time. The valid range is 1 to 1440 minutes.

8. In the **Zone** field, specify the acronym associated with the time zone when daylight saving time is in effect. This field is not validated against an official list of time zone acronyms.

9. Click the **Apply** button.

The Daylight Saving (DST) Status table shows information about the daylight saving time settings, and whether the time shift for daylight saving time is currently in effect or not.

Note: When **Daylight Saving (DST)** is **Disabled**, the following fields will not be displayed: **Begins At**, **Ends At**, **Offset (in Minutes)**, and **Zone**.

Denial of Service

Use the Denial of Service (DoS) feature to configure DoS control. The switch software provides support for classifying and blocking specific types of DoS attacks.

Configure Auto-DoS

The Auto-**DoS Configuration** screen lets you automatically enable all the DoS features available on the switch, except for the L4 Port attack. For information about the types of DoS attacks the switch can monitor and block, see <u>Configure Denial of Service on page 58</u>.

To enable the Auto-DoS feature:

1. Select **System** > **Management** > **Denial of Service** > **Auto-DoS Configuration**.
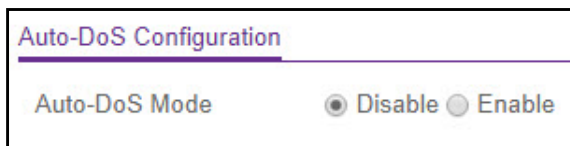
   Figure 36. Auto-DoS Configuration

2. Next to Auto-DoS Mode, select **Enable**.

   When an attack is detected, a warning message is logged to the buffered log and is sent to the syslog server. At the same time, the port is shut down and can be enabled only manually by the admin user.

3. Click the **Apply** button.

Configure Denial of Service

The **Denial of Service Configuration** screen allows you to select which types of DoS attacks the switch monitors and blocks.

To configure individual DoS settings:

1. Select **System** > **Management** > **Denial of Service** > **Denial of Service Configuration**.

Figure 37. Denial of Service Configuration

2. Select the types of DoS attacks for the switch to monitor and block and configure any associated values:

- **Denial of Service Min TCP Header Size**. Specify the minimum TCP header size allowed. If DoS TCP Fragment is enabled, the switch will drop packets that have a TCP header smaller than the configured value.

- **Denial of Service ICMPv4**. Enabling ICMPv4 DoS prevention causes the switch to drop ICMPv4 packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 packet size. The factory default is disabled.

- **Denial of Service Max ICMPv4 Packet Size**. Specify the maximum ICMPv4 packet size allowed. If ICMPv4 DoS prevention is enabled, the switch will drop IPv4 ICMP ping packets that have a size greater than the configured value.

- **Denial of Service ICMPv6**. Enabling ICMPv6 DoS prevention causes the switch to drop ICMPv6 packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 packet size.

- **Denial of Service Max ICMPv6 Packet Size**. Specify the maximum IPv6 ICMP packet size allowed. If ICMPv6 DoS prevention is enabled, the switch will drop IPv6

ICMP ping packets that have a size greater than this configured maximum ICMPv6 packet size.

- **Denial of Service First Fragment**. Enabling First Fragment DoS prevention causes the switch to check DoS options on first fragment IP packets when switch are receiving fragmented IP packets. Otherwise, the switch ignores the first fragment IP packages.

- **Denial of Service ICMP Fragment**. Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP fragmented packets.

- **Denial of Service SIP=DIP**. Enabling SIP=DIP DoS prevention causes the switch to drop packets that have a source IP address equal to the destination IP address.

- **Denial of Service SMAC=DMAC**. Enabling SMAC=DMAC DoS prevention causes the switch to drop packets that have a source MAC address equal to the destination MAC address.

- **Denial of Service TCP FIN&URG&PSH**. Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets that have TCP Flags FIN, URG, and PSH set and TCP sequence number equal to 0.

- **Denial of Service TCP Flag&Sequence**. Enabling TCP Flag DoS prevention causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0.

- **Denial of Service TCP Fragment**. Enabling TCP Fragment DoS prevention causes the switch to drop packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size.

- **Denial of Service TCP Offset**. Enabling TCP Offset DoS prevention causes the switch to drop packets that have a TCP header offset set to 1.

- **Denial of Service TCP Port**. Enabling TCP Port DoS prevention causes the switch to drop packets that have TCP source port equal to TCP destination port.

- **Denial of Service TCP SYN**. Enabling TCP SYN DoS prevention causes the switch to drop packets that have TCP flags SYN set.

- **Denial of Service TCP SYN&FIN**. Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets that have TCP flags SYN and FIN set.

- **Denial of Service UDP**. Enabling UDP Port DoS prevention causes the switch to drop packets that have UDP source port equal to UDP destination port. The factory default is disabled.

3. Click the **Apply** button.

DNS

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

Configure DNS

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

To configure the global DNS settings:

1. Select **System** > **Management** > **DNS** > **DNS Configuration**.

Figure 38. DNS Configuration

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

    When the system is performing a lookup on an unqualified hostname, this field is provided as the domain name (for example, if default domain name is netgear.com and the user enters test, then test is changed to test.netgear.com to resolve the name).

4. In the DNS Server field, specify the IPv4 address to which the switch sends DNS queries.
5. Click the **Add** button.

    You can specify up to eight DNS servers. The **Preference** field displays the server preference order. The preference is set in the order created.

6. Click the **Apply** button. The updated configuration is sent to the switch, and configuration changes take effect immediately.

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

Table 16. Dynamically learned host name mapping information

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

Click **Clear** to delete dynamic host entries. The table will be repopulated with entries as they are learned.

Configure and View Host Name-to-IP Address Information

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

To add a static entry to the local DNS table:

1. Select **System** > **Management** > **DNS** > **Host Configuration**.

Figure 39. DNS Host Configuration

2. In the Host Name field, specify the static host name to add.
3. In the IPv4/IPv6 Address field, specify the IP address to associate with the host name.
4. Click the **Add** button.

To remove an entry from the static DNS table:

1. Select the check box next to the entry to remove.
2. Click the **Delete** button.

To change the host name or IP address in an entry:

1. Select the check box next to the entry to update.

2. Enter the new information in the appropriate field.

3. Click the **Apply** button.

Green Ethernet

Use this screen to configure Green Ethernet features. Using the Green Ethernet Configuration features allows for power consumption savings.

To configure the Green Ethernet settings:

1. Select **System** > **Management** > **Green Ethernet** > **Green Ethernet Configuration**.
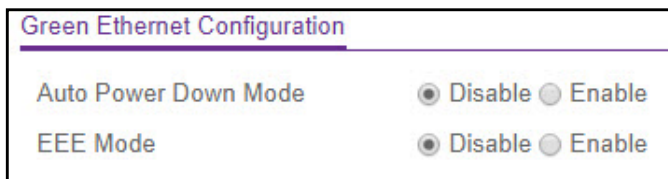
Figure 40. Green Ethernet Configuration

2. Enable or disable the **Auto Power Down Mode**.

   - **Enable**. When the port link is down, the PHY (physical layer device) will automatically go down for a short period of time and then wake up to check link pulses. This allows the port to continue to perform autonegotiation while consuming less power when no link partner is present.

   - **Disable**. Provide full power to the PHY even if the port link is down. The default is Disable.

3. Enable or disable the **EEE Mode**.

   - **Enable**. When the send and receive sides of a link are lightly loaded, the port can transition to low power mode to save power.

   - **Disable**. Provide full power to the PHY regardless of the link load. The default is Disable.

4. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

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

Green Ethernet Interface Configuration

Use this screen to configure per-port Green Ethernet settings.

To configure the Green Ethernet Interface settings:

1. Select **System** > **Management** > **Green Ethernet** > **Green Ethernet Interface Configuration**.

Figure 41. Green Ethernet Interface Configuration

2. Select one or more ports to configure.
   - To configure a single port, select the check box associated with it, or type the port number in the Go To Interface field and click the **Go** button.
   - To configure multiple ports with the same settings, select the check box associated with each port to configure.
   - To configure all ports with the same settings, select the check box in the heading row.
3. Use the lists to enable or disable the Green Ethernet features for the selected ports:
   - **Auto Power Down Mode**. The factory default is **Disable**. If Auto Power Down Mode is not supported, then **N/A** (not applicable) is displayed. When this mode is enabled and a port link is down, the PHY will automatically go down for short period of time, and then wake up to check link pulses. This will allow performing auto-negotiation and saving power consumption when no link partner is present.
   - **EEE Mode**. The factory default is **Disable**. If the EEE Mode is not supported, then **N/A** (not applicable) is displayed. 'When this mode is enabled and the send and receive sides of a link are lightly loaded, the port can transition to low-power mode. The EEE and the Short Cable modes are not supposed to be active simultaneously.
4. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

Green Ethernet Detail

Use this screen to view detailed per-port Green Ethernet information and to enable or disable Green Ethernet settings on a single port. Using the Green Ethernet features allows for power consumption savings.

To configure Green Ethernet mode settings for a port:

1. Click **System** > **Management** > **Green Ethernet** > **Green Ethernet Detail**.

Figure 42. Green Ethernet Detail

2. From the **Interface** list, select the interface to configure the Green Ethernet mode settings.

3. Enable or disable the **Energy Detect Admin Mode** on the port. When energy detect mode enabled, and a port link is down, the PHY automatically goes down for a short period of time, and then wakes up to check link pulses. This will allow performing auto-negotiation and saving power consumption when no link partner is present. The default value is **Disabled**. If **Energy Detect Admin Mode** is not supported, then **N/A** is displayed.

4. **EEE Admin Mode**. Enable or disable the **Energy Efficient Ethernet (EEE) Admin Mode** on the port. When EEE mode is enabled, the port transitions to low-power mode during link idle conditions. The default value is **Disabled**. If **EEE Admin Mode** is not supported, then **N/A** is displayed.

5. **EEE Transmit Idle Time**. Enter the time for which the condition to move to LPI state is satisfied, at the end of which MAC TX transitions to LPI state. The range is 600 to 4294967295. The default value is 600.

6. **EEE Transmit Wake Time**. Enter the time for which the MAC/switch has to wait to go back to Active state from the LPI state when it receives a packet for transmission. The range is 8 to 65535. The default value is 17.

7. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

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

9. Click **Refresh** to refresh the data on the screen with the current data on the switch.

10. Click **Clear** to clear the configuration and reset all statistics for the selected interface to the default values.

The **Local Device Information** table displays the following non-configurable information about the Green Ethernet status and statistics on the port.

Table 17. Green Ethernet Local Device Information

Field	Description
Cumulative Energy Saved on this port due to Green Mode(s) (Watts * Hours)	The energy savings per port, per hour.
Energy Detect Operational Status	Indicates whether the Energy Detect Admin Mode is currently operational (Active) or inactive.
Reason	The reason for the current operational status of Energy Detect Admin Mode.
Rx Low Power Idle Event Count	This field is incremented each time MAC RX enters LP Idle state. Shows the number of times the local interface has entered a low-power idle state (i.e. shows the total number of Rx LPI Events) since EEE counters were last cleared.
Rx Low Power Idle Duration (uSec)	Indicates the duration of Rx LPI state in 10 microsecond increments. Shows the total duration of Rx LPI (i.e. the amount of time the local interface has spent in a low-power idle state) since the EEE counters were last cleared.
Tx Low Power Idle Event Count	The number of times the link partner has entered a low-power idle state.
Tx Low Power Idle Duration (uSec)	The duration of Tx LPI state (i.e. amount of time) in 10 microsecond increments. Shows the total duration the link partner has spent in a Tx low-power idle state since the EEE counters were last cleared.
Tw_sys_tx (uSec)	An integer that indicates the value of Tw_sys that the local system can support. This value is updated by the EEE DLL Transmitter state diagram.
Tw_sys_tx Echo (uSec)	An integer that indicates the remote system's transmit Tw_sys that was used by the local system to compute the Tw_sys that it wants to request from the remote system.
Tw_sys_rx (uSec)	An integer that indicates the value of Tw_sys that the local system requests from the remote system. This value is updated by the EEE Receiver L2 state diagram.

Table 17. Green Ethernet Local Device Information (continued)

Field	Description
Tw_sys_rx Echo (uSec)	An integer that indicates the value of the remote system's receive Tw_sys that was used by the local system to compute the Tw_sys that it can support.
Fallback Tw_sys (uSec)	An integer that indicates the value of fallback Tw_sys that the local system requests from the remote system. This value is updated by the local system software.
Tx_dll_enabled	The initialization status of the EEE transmit Data Link Layer management function on the local system.
Tx_dll_ready	The transmit Data Link Layer ready status. This variable indicates that the tx system initialization is complete and is ready to update/receive LLDPDU containing EEE TLV. This variable is updated by the local system software.
Rx_dll_enabled	The status of the EEE capability negotiation on the local system.
Rx_dll_ready	The receive Data Link Layer ready status. This variable indicates that the rx system initialization is complete and is ready to update/receive LLDPDU containing EEE TLV. This variable is updated by the local system software.
Time Since Counters Last Cleared	The amount of time that has passed since the Green Ethernet information for this port was last cleared (since the time of power up, or after EEE counters were cleared).

To display Green Ethernet mode settings for a Remote Device:

1. Click **System** > **Management** > **Green Ethernet** > **Green Ethernet Detail**.
2. Scroll down to the Remote Device Information section.
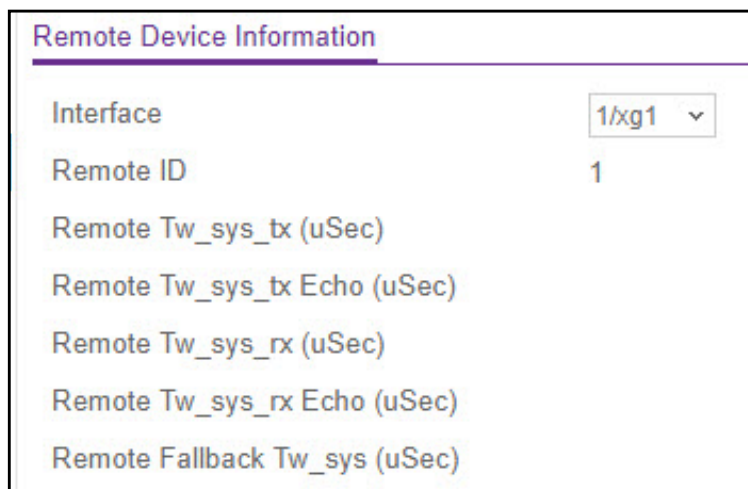
Figure 43. Remote Device Information

3. From the **Interface** list, select the interface.

<u>Table 18, Green Ethernet Local Device Information</u> displays the following non-configurable information about the Green Ethernet status and statistics on the local device.

Table 18. Green Ethernet Local Device Information

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

4. Click **Clear** to clear the configuration and reset all statistics for the selected interface to the default values.

Green Ethernet Summary

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

To access the Green Ethernet Summary screen, select **System** > **Management** > **Green Ethernet** > **Green Ethernet Summary**.

Figure 44. Green Ethernet Summary

Table 19, Green Ethernet statistics summary describes the information the Green Ethernet Statistics Summary table displays.

Table 19. Green Ethernet statistics summary

Field	Description
Current Power Consumption	The estimated power consumption (in mWatts) by all the ports on the switch.
Percentage Power Saving/Stack	The percentage of power saved on all ports due to the Green Ethernet mode(s) being enabled.
Cumulative Energy Saving per Stack (Watts*Hours)	The cumulative energy saved in (Watts * Hour) due to all Green Ethernet features being enabled.

Table 20, Green Ethernet feature summary describes the information in the Green Ethernet feature summary table.

Table 20. Green Ethernet feature summary

Field	Description
Unit	The unit ID number, which is always 1.
Green Features supported on this unit	The Green Ethernet features the switch supports.

Table 21, Green Ethernet interface summary describes the information in the Green Ethernet interface summary table.

Table 21. Green Ethernet interface summary

Field	Description
Interface	The interface associated with the rest of the data in the row.
Energy Detect Admin Mode	The administrative status of the Energy Detect feature on the interface.
Energy Detect Operational Status	The operational status of the Energy Detect feature on the interface.
EEE Admin Mode	The administrative status of the **EEE** feature on the interface.

Click **Refresh** to refresh the data on the screen with the current data on the switch.

View and Configure Green Ethernet LPI History

Use this screen to configure and view the Green Ethernet low power idle (LPI) history. Viewing the Green Ethernet LPI History feature allows you to view the Green Ethernet history for the switch.

To configure the LPI settings:

1. Select **System** > **Management** > **Green Ethernet** > **Green Ethernet LPI History**.

Figure 45. Green Ethernet LPI History

2. In the Sampling Interval field, specify the frequency, in seconds, at which EEE LPI history.

3. In the Max Samples to keep field, specify the maximum number of LPI samples to keep in the history buffer.

4. Click the **Apply** button.

To view per-interface LPI history information, select the interface with the information to view from the Interface list. The screen refreshes and displays the LPI history for the selected interface.

The following table describes the status fields on the screen.

Table 22. LPI history information

Field	Description
Percentage LPI time	The percentage of time the switch spent in LPI mode.
Sample No.	The current sample number. When the number increases to the maximum, it rolls over and begins at 1.
Time Since The Sample Was Recorded	The amount of time that has passed since the last LPI history sample was recorded. Each time the screen is refreshed it shows a different time as it reflects the difference in current time and time at which the sample was recorded.

Table 22. LPI history information (continued)

Field	Description
Percentage Time spent in LPI mode since last sample	The percentage of time spent in LPI mode since the last sample was recorded.
Percentage Time spent in LPI mode since last reset	The percentage of time spent in LPI mode since the switch was reset.

Device View

For Device View information, see .

License

Some switch features require a special license in order to be active. If a license is not active, the feature associated with the license is not available and cannot be configured.

To view information about the license key, click **System** > **License** > **License Key**.

The following table describes the non-configurable fields on the License Key page.

Table 23. License Key information

Field	Description
License Date	The date the license is purchased.
License Copy	The number of licenses that exist on the switch.
License Status	Indicates whether the license is active or inactive. If a license is inactive, a license should be purchased and downloaded to the switch. The license is not activated until the switch reboots.
Description	A description of the license key status. If the license is inactive, this field provides information about why it is inactive.

To view a list of features on the device that require an active license, click **System** > **License** > **License Features**.

Switch Stack Configuration

Stacking Overview

A stackable switch is a switch that is a fully functional operating standalone, but can also be set-up to operate together with up to six switches, with this group of switches showing the characteristics of a single switch while having the port capacity of the sum of the combined switches.

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

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

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

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack manager. Every stack member is uniquely identified by its own stack member number.

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

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

All stack members must run the same software version to ensure compatibility between stack members. The software versions on all stack members, including the stack manager, must be the same. This helps ensure full compatibility in the stack protocol version among the stack members. If a stack member is running a software version that is not the same as the stack manager, then the stack member is not allowed to join the stack.

The stack manager contains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes.

If the manager is removed from the stack, another member will be elected manager, and will then run from that saved configuration.

The stack manager switch performs a consistency check to ensure that all units in the stack are running the same version of agent. Using the information gathered during topology discovery, the stack manager can determine whether all units are running the same version of agent. If the versions do not match, then the ports on the subordinate switch will not

become valid for operation. This condition is known as the special stacking mode. You have the ability to synchronize the software on the stack unit with the software that is running on the stack manager. Normally, the software is automatically distributed to all units in the stack after downloading new code, but there can be instances where a unit with older code is plugged in to the stack. In this scenario, use the stack firmware synchronization feature to push the code from the stack manager to the stack members. This ensures that the stack members are in sync with the rest of the participating switches in the stack. For more information, see .

The stack manager will automatically distribute firmware to subordinate switches when you upgrade the firmware so that all stack members are synchronized when reloading the stack.

Stack Features

The primary stacking features are as follows:

- Up to 6 switches in a stack
- Single IP Address management through web and SCC
- Manager-member configuration
  - Configuration for all units is stored on the manager
  - Auto-detection for new members, with synchronization of firmware (upgrade or downgrade as needed).
- Configuration updates download is supported across the stack through single operation.
- Automatic master fail-over. Fully resilient stack with chain and ring topology.
- Hot swappable (insertion and removal) of stack units
- Stack number information and automatic stacking set-up options

Factory Defaults Reset Behavior

The configurations applied on S3300 would be automatically saved to the flash. The stack manager automatically distributes the configuration to the stack members. If the stack manager becomes unavailable, a stack member can become the new stack manager and apply the configuration that was saved on the original stack manager.

The stack manager initializes the stack using the last saved system configuration that is stored in its local FLASH. When the stack manager is reset to the factory default settings, the stack manager applies default settings to all the stack members and resets the stack including the participating stack members.

Stack Manager Election and Re-Election

The stack manager is elected or re-elected based on one of these factors and in the order listed:

- The switch that is currently the stack manager
- The switch with the highest stack member priority value

Note: NETGEAR recommends assigning the highest priority value to the switch that you prefer to be the stack manager. This ensures that the switch is re-elected as stack manager if a re-election occurs.

- The switch with the higher MAC address

A stack manager retains its role unless one of these events occurs:

- The stack manager is removed from the switch stack
- The stack manager is reset or powered off
- The stack manager has failed
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks

In the case of a manager re-election, the new stack manager becomes available after a few seconds.

If a new stack manager is elected and the previous stack manager becomes available, the previous stack manager does not resume its role as stack manager.

Smart M4300/S3300 Stacking Notes and Restrictions

In release 6.6.4, two M4300 models (M4300-12X12F/M4300-24X) are able to be stacked with S3300 models. This section describes the notes and restrictions when M4300 is mixed stacking with S3300 running 6.6.4.x firmware.

- M4300-12X12F/M4300-24X (hereafter referred to as M4300) and S3300 have separate 6.6.4.x images to support this mixed stacking.
  - These switches need to be upgraded to their respective new images before they can be put into stacking.
  - In order to load the 6.6.4.x image into an M4300 unit running firmware 12.0.0.x/12.0.2.x older than 12.0.2.17, the M4300 should be loaded with a new 12.0.2.x image (12.0.2.17 or newer) first.
  - Once an S3300 unit is running with a 6.6.4 image, it can be brought back to the M4300 family by directly downloading and activating a 12.0.0.x/12.0.2.x image into it.

  For the procedures regarding upgrading M4300/S3300 firmware, see Smart M4300/S3300 Firmware Upgrade Procedure on page 338.

- On the two M4300 models, a maximum of four 10G ports (any four from the eight available ports below) can be configured as stacking ports.
  - M4300-24X: port 17–24
  - M4300-12X12F: port 9–12 and port 21–24
- M4300 with 6.6.4.x image scales down to the S3300 feature set to become part of the stacking.
  - AVB will not be available even in Standalone mode on M4300.

- All stacking functionalities of the S3300 extend to these two M4300 platforms. However, Non-Stop Forwarding (NSF) is not supported.

- Either S3300 or M4300 can be stack master or standby.

- CLI under the console port is not supported.

- Service port is not supported for management or any other purposes.

• New features for the M4300 running the Smart 6.6.4.x image are:

- Smart Control Center (SCC) can be used to discover the Smart M4300 and do some basic settings, the same as can be done on the S3300.

- The **Reset** button on the front panel of the M4300 models can be used to reset the unit to the factory default.

  • When the **Reset** button is pressed 2–5 seconds, the switch will simply reset (reload).

  • When the **Reset** button is pressed over 5 seconds, the switch will clear all configuration followed by a reload of the factory default settings.

Basic Stack Configuration

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

Management Unit Selection

To do basic stack configuration:

1. Click **System** > **Stacking > Basic > Stack Configuration.**

2. Select the **Management Unit**. The Management Unit Selected field displays the Current Primary Management Unit. You can change it by selecting another unitID listed here.

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

4. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

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

Stack Sample Mode

To configure the stack sampling parameters:

1. Select the **Stack Sample Mode**. The global status management mode which can be:
   - **Cumulative.** This tracks the sum of received time stamp offsets cumulatively.
   - **History**. This tracks the history of received timestamps.

   The factory default is **Cumulative**.

2. Enter a value for **Max Samples** – the maximum number of samples to keep. The valid range is 100 to 500. **Max Samples** applies to **History** mode.

Figure 46. Configure Stack Sample Mode

3. Click the **Apply** button to send the updated configuration to the switch. The status management mode and sample size parameters are applied globally to all units in the stack. Configuration changes take effect immediately.

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

Stack Configuration

To configure the stack:

1. Select the **Unit ID** from the displayed list of units in the stack.

2. Use the **Change Switch ID to** field to renumber the switch ID of the selected switch.

3. Specify the **Switch Type** - the type of switch hardware when creating a new switch in the stack.

4. Specify the **Switch Priority** - the priority of a switch to become the primary management unit. The range for priority is 0 to 15. The factory default is unassigned. The switch with the highest priority value will be chosen to become primary unit. If the value is set to 0, then that switch unit never participates in Manager Election.

5. Select the **Management Status.** Indicates whether the selected switch is the management unit, or a normal stacking member, or on standby.

6. Click the **Apply** button. The system prompts the administrator to confirm the management move. Upon administrator confirmation, the entire stack, including all interfaces in the stack, is unconfigured and reconfigured with the configuration on the new Primary Management Unit. Configuration changes take place immediately.

7. Click the **Cancel** button to cancel the configuration on the screen. The data on the screen is reset to the latest value of the switch.

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

9. After the reload is complete, all stack management capability must be performed on the new Primary Management Unit.

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

Table 24. Stack Configuration

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

Basic Stack Status

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

Table 25. Basic Stack Status

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

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

Advanced Stack Configuration

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

Advanced Stack Status

Use the Stack Status page to display stack protocol information:

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

Figure 47. Advanced Stack Status

The following table describes the non-configurable Advanced Stack Status data that is displayed. Click **Refresh** to update the page with the latest information on the switch.

Table 26. Advanced Stack Status

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

Clear Sampling Information

To clear the sampling information:

The stack sampling parameters are configured on the **System** > **Stacking > Basic > Stack Configuration** page. See Stack Sample Mode on page 77.

1. Click **System** > **Stacking > Advanced > Stack Status** to display the sampling table. See Figure 47 on page 80.

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

3. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

Advanced Stack-Port Configuration

To configure a Stack-port:

1. Click **System** > **Stacking > Advanced > Stack-port Configuration.**

Figure 48. Stack-Port Configuration

2. Select either the **Unit ID** or **All**.

    • Select the **Unit ID** field to display information for the selected unit.

    • Select **All** to display information for all units.

3. In the **Configured Stack Mode** field, specify the operating mode of the port to be either **Ethernet** or **Stack**. The default value for front panel stack mode is **Stack**. The default value for back panel stack mode is **Stack**. The default value for **Configured Stack Mode** is **Ethernet.**

4. In the M4300 models, not all ports can be configured as stack ports, and only some particular ports can be configured as stack ports. The maximum is eight stack links.

5. For the predefined eight ports on the M4300-24X and M4300-12X12F models, both fiber and copper stack links are needed. So, the last eight ports are predefined as follows:

    a. For M4300-24X, predefine the last eight ports (port 17 to 24):

        - Ports 17 to 20 are 10G copper.

        - Ports 21 to 24 are combo.

    b. For M4300-12X12F, predefine four fiber ports and four copper ports:

        - Ports 9 to 12 are 10G fiber

        - Ports 12 to 24 are 10G copper.

6. Manually reboot the switch for the changes to take effect.

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

Table 27. Stack-port Configuration

Field	Description
Unit ID	The Unit ID of the specific switch.
Port	Displays the stack port on the given unit.
Running Stack Mode	Displays the runtime mode of the stack port.
Link Status	Displays the link status (Up/Down) of the port.
Link Speed (Gbps)	Displays the maximum speed of the stack port.

Table 27. Stack-port Configuration (continued)

Field	Description
Transmit Data Rate (Mbps)	Displays the approximate transmit rate on the stack port.
Transmit Error Rate (Error/s)	Displays the number of errors in transmit packets per second.
Total Transmit Errors	Displays the total number of errors in transmit packets since bootup. The counter may wrap.
Receive Data Rate (Mbps)	Displays the approximate receive rate on the stack port.
Receive Error Rate (Error/s)	Displays the number of errors in receive packets per second.
Total Receive Errors	Displays the total number of errors in receive packets since bootup. The counter may wrap.
Link Flaps	Displays a stack port counter that increments whenever a stack port link transitions to the down state.

Advanced Stack-Port Diagnostics

To display Stack-port diagnostics:

Use the Stack-port Diagnostics page to display the diagnostics for all the stack-ports in the given stack.

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

Figure 49. Stack-port Diagnostics

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

Table 28. Stack-port Diagnostics

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

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

Stack-Port Packet-Path

To display Stack-port Packet-Path:

1. Click **System** > **Stacking > Advanced > Stack-port Diagnostics** to display the Stack-port packet-path fields. See Figure 49, Stack-port Diagnostics above.
2. To navigate, select either the **Unit ID** or **All**.
    *   Select the **Unit ID** field to display the packet path starting from the selected unit.
    *   Select **All** to display the packet path starting from all the units of the stack.

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

Table 29. Stack-port Packet-path

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

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

Stack Firmware Synchronization

The Firmware Synchronization feature provides an automatic mechanism to synchronize the firmware on stack members whose firmware version is different from the version running on the stack manager. Subject to configuration, this synchronization operation may result in either an upgrade or a downgrade of firmware on the mismatched stack member. The feature also checks for boot code version compatibility before starting the upgrade.

By default, the Firmware Synchronization feature is disabled.

Activating the firmware image is not possible if the minimum boot code specified in the image file is not met by the running boot code on the switch and the auto boot code upgrade feature is not present.

The behavior of Firmware Synchronization is the same whether the system is powered on after connecting all the new members or if a new member is adding during the running operation of the stack. Stack Firmware Synchronization starts only after the stack manager selection is complete.

You can disable downgrading the image on a stack member during Firmware Synchronization operation. The Firmware Synchronization configuration parameters are global and cannot be changed for each individual stack unit.

If the stack member code is *mismatched stack*, then the backup image of the stack member is used for Firmware Synchronization.

The reboot operation is allowed, even though there is a synchronization operation in progress. In case of firmware corruption during Firmware Synchronization, manual intervention by the operator is required to bring the switch back to working condition.

To configure the Stack Firmware Synchronization:

1. Click **System** > **Stacking > Advanced > Stack Firmware Synchronization**.
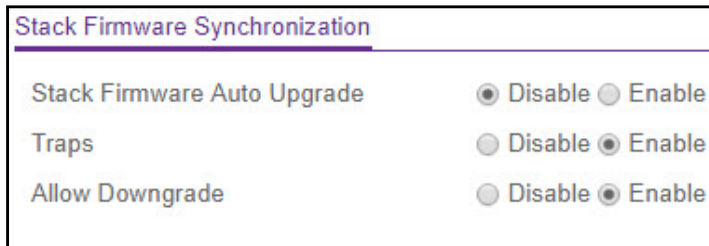
Figure 50. Stack Firmware Synchronization

2. Enable or disable the following settings:

    •   **Stack Firmware Auto Upgrade**. Use this field to enable or disable the Stack Firmware Synchronization feature. The factory default is Disabled.

    •   **Traps**. Use this field to enable or disable the sending of traps during Stack Firmware Synchronization Start, Failure, and Finish. The factory default is Enabled.

    •   **Allow Downgrade**. Use this field to enable or disable downgrading the image on a stack member if the stack member's version is newer. The factory default is Enabled.

3. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take place immediately.

4. Click the **Cancel** button to cancel the configuration on the screen. This resets the data on the screen to the latest value of the switch.

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

Multiple Stack Links

The S3300 platforms contain two dedicated (non-combo) 10GBaseT copper links (ports) and 2 dedicated SFP+ fiber links. Any of these links can be configured for normal Ethernet operation or stacking operation. When these links are configured for stacking operation, multiple links can be connected to an adjacent unit to form a higher bandwidth stacking connection. This is referred to as *Multiple Stack Links*.

The following restrictions and limitations apply when using Multiple Stack Links:

- Fiber link takes precedence over the copper link
- When fiber link is present between the stacked units, traffic is always carried through the fiber link, whether over a single link or over two links in a trunk.
  - This happens irrespective of one or two copper links present
  - Copper link, in the presence of fiber link, always acts as standby and does not participate in carrying traffic. However, when the fiber links are down/removed, the copper link becomes active and starts carrying traffic. This operation (known as switchover between the links) does not destabilize the stack.

In a multi-unit stack of S3300-52X and/or S3300-52X-PoE+, the following apply:

- One or both copper links between two adjacent S3300 units can be connected to form a Stack.
- One or both fiber links between two adjacent S3300 units can be connected to form a stack.
- Both methods above can be used to form a stack of more than two units.
  - A Stack of three units (Unit-A, Unit-B, Unit-C) can be formed by connecting Unit-A and Unit-B over two fiber links, and Unit-B and Unit-C over two copper links. This will make the effective stacking bandwidth between the units ~20G.
  - If a combination of one copper and one fiber is chosen between the units (A-B and B-C), the stack will still form, but the effective stacking bandwidth will be limited to ~10G.
- As an exception to this, if the stack is formed with only S3300-28X and/or S3300-28X-PoE+ units, the above restriction does not apply.
  - The user is free to choose any combination of copper and fiber links to form a stack without compromising on bandwidth.
  - Use of one copper and one fiber to form a stack will still give ~20G bandwidth in case all the units participating in the stack are S3300-28X and/or S3300-28X-PoE+.

In summary:

- Fiber link takes precedence over the copper link
- When fiber link is present between the stacked units, traffic is always carried through the fiber link, whether over a single link or over two links in a trunk
  - This happens irrespective of one or two copper links present

- Copper link, in the presence of fiber link, always acts as standby and does not participate in carrying traffic. However, when the fiber links are down/removed, the copper link becomes active and starts carrying traffic. This operation (known as switchover between the links) does not destabilize the stack.

PoE

Use this screen to configure a few system-level PoE parameters per unit. In other words, the parameters are specific to the whole unit, not specific to any port(s).

1. Select **System** > **PoE** > **Basic** > **PoE Configuration**.

Figure 51. PoE Basic Configuration

2. In the **Unit Selection** field, select a current PoE unit. You can change the PoE Unit by selecting another unit ID listed in this field.

3. Configure the **System Usage Threshold**. Set a threshold level at which a trap is sent if consumed power is greater than threshold power. Possible values are 1% to 99%. The factory default is **95%**.

4. Configure **Power Management Mode**. Describes or controls the power management algorithm used by the PSE to deliver power to the requesting PDs. Possible values are:

   • **Dynamic**. Power consumption of each port is measured and calculated in real-time. The default mode is **Dynamic.**

   • **Static**. Power allocated for each port depends on the type of power threshold configured on the port.

5. Configure **Traps**. **Enable** or **Disable** the activation of PoE traps by selecting the corresponding check box. The factory default is **Enable**.

6. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

7. Click the **Cancel** button to cancel the configuration on the screen. The data on the screen is reset to the latest value of the switch.

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

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

Table 30. PoE Configuration Non-configurable Data

Field	Description
Firmware Version	Version of the PoE controller's FW image.
Power Status	Indicates the power status.
Total Power (Main AC) Watt	Maximum amount of power that is available to the system from the main AC source to deliver to all ports.
Total Power (RPS) Watt	Maximum amount of power that is available to the system from an external RPS supply to deliver to all ports.
Power Source	The power source currently being used to deliver power - Main AC or RPS.
Threshold Power	The system can power up one more port if consumed power is less than Threshold Power. In other words, consumed power can be between Nominal and Threshold Power values. The Threshold Power value is effected by changing the System Usage Threshold. There could be a delay in showing the updated values. Click the **Update** button to refresh the page again if the Threshold Power is not changed accordingly. Threshold Power is displayed in milliwatts (mW).
Consumed Power	The total amount of power which is currently being delivered to all ports in milliwatts.

Advanced PoE Configuration

The **Advanced > PoE Configuration** screen displays the same table as the **Basic > PoE Configuration** screen described above. However the Advanced screen allows you to configure a host of PoE parameters specific to port(s) of a specific unit.

Advanced PoE Port Configuration

To configure advanced PoE port settings.

1. Select **System** > **PoE** > **Advanced** > **PoE Port Configuration**.

   The PoE Port Configuration screen displays.

Figure 52. PoE Port Configuration

2. In the **Unit Selection** field, select a current PoE unit. You can change the PoE Unit by selecting another unit ID listed in this field.

3. Next to **Port Power**, select the **Enable** button to enable the port to deliver PoE power. The factory default is Enable.

4. Configure the **Port Priority**. Use this field to determine which ports can deliver power when total power delivered by the system crosses a certain threshold. The switch may not be able to supply power to all connected devices. Priority is used to determine which ports can supply power. When ports have the same priority, the lower numbered port will have a higher priority. Possible priority values are:

    • **Low**. Low priority.

    • **Medium**. Medium priority.

    • **High**. High priority.

    • **Critical**. Critical priority.

    The factory default is Low.

5. Select the **Power Mode**.

    • **802.3 af**. The PoE port power is limited to IEEE 802.3af mode only. A powered device (PD) that requires IEEE 802.3at power does not receive power if the port functions in the IEEE 802.3af mode.

    • **Legacy**. A port is powered using high-inrush current, used by legacy powered devices (PDs) whose power requirement is greater than 15W at initial power up.

    • **Pre-802.3at**. This means that a port is powered in the IEEE 802.3af mode initially, then is switched to the high-power IEEE 802.3at mode before 75 msec. This mode needs to be used if PD is not performing Layer 2 Classification or if the PSE (the switch) is performing two-event Layer 1 Classification.

    • **802.3at**. The PoE port power is powered in the IEEE 802.3at mode, and is backward compatible with IEEE 802.3af. The factory default is 802.3at mode. In the 802.3at mode, if the switch detects that the attached PD requests more power than the IEEE 802.3af, but is not an IEEE 802.3at Class 4 device, then the PD does not receive power from the switch.

6. Set the **Power Limit Type** to control the maximum power that a port can deliver. Use of these options may lead to a situation where the port reserves a higher amount of PoE power than the port can actually deliver to a connected PD. This happens when the PD reports

class information incorrectly. Note that incorrect setting of this field may prevent a PDF from receiving PoE power from a given port(s).

Possible values are:

- **None**. This value allows the port to draw up to class 0 max power in case of low power mode, and up to class 4 max power in case of high power mode.
- **Class**. This value means that the port power limit is equal to the class of the PD attached.
- **User**. This value means that the port power limit is equal to the value specified by Power Limit.

The factory default is User.

7. In the **Power Limit (mw)** field, specify the maximum power that can be delivered by a port. The range is 3000–30000 watts with step of 1 milliwatt (mw). The factory default is 30000 mW.

8. In the **Detection Type** field, select the PD detection mechanism performed by the PSE port. Possible values are:

- **IEEE 802**. 4-Point Resistive Detection is done.
- **4pt 802.3af + legacy**. 4-Point Resistive Detection in 802.3af mode, followed by Legacy Detection, is done.
- **Legacy**. Only Legacy Detection is done.

The factory default is IEEE 802.

9. Assign a **Timer Schedule** to the port. Select **None** to remove the timer schedule assignment. The factory default is None. See <u>Timer Schedule on page 127</u>.

10. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

11. Click the **Cancel** button to cancel the configuration on the screen. The data on the screen is reset to the latest value of the switch.

12. Click the **Power Cycle Port(s)** button to forcibly reset the PSE port.

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

Table 31. PoE Port Configuration Non-Configurable Data

Field	Description
Port	The interface for which data is to be displayed or configured.
High Power	Enabled when a particular port supports High Power Mode.
Max Power (mW)	The maximum power in milliwatts that can be provided by the port.

Table 31. PoE Port Configuration Non-Configurable Data (continued)

Field	Description
Class	The class of the Powered Device (PD) defines the range of power a PD is drawing from the system. Class definitions are: 0. 0.44–16.2 watts 1. 0.44–4.2 watts 2. 0.44–7.4 watts 3. 0.44–16.2 watts 4. 0.44–31.2 watts
Output Voltage	Current voltage being delivered to the device in Volts.
Output Current	Current being delivered to the device in mA.
Output Power	Current power being delivered to the device in milliwatts.
Temperature	The temperature measured at this port of the PoE Controller. The temperature is measured in degrees Celsius.
Status	Operational status of the port PD detection. Possible values are: • Disabled. Indicates that no power is being delivered. • Delivering Power. Indicates that power is being drawn by the device. • Fault. Indicates a problem with the power. • Other Fault. Indicates that the port is idle due to an error condition. • Requesting Power. Indicates that the port is requesting power. • Searching. Indicates that the port is not in one of the other states in this list. • Test. Indicates that the port is in Test mode.
Fault Status	Describes the error description when the PSE port is in fault status. Possible values are: • No Error. Specifies that the PSE port is not in any error state • MPS Absent. Specifies that the PSE port has detected an absence of main power supply. • Short. Specifies that the PSE port has detected a short circuit condition. • Overload. Specifies that the PD connected to the PSE port has tried to provide more power than is permissible by the hardware. • Power Denied. Specifies that the PSE port has been denied power because of a shortage of power, or due to administrative action.

SNMP

This section describes how to configure the Simple Network Management Protocol (SNMP) version 1 and SNMP version 2 information on the switch. For information about configuring the SNMPv3 administrative profile, see Use SNMPv3 on page 26.

The screens you access from the SNMPV1/V2 link allow you to configure SNMPv1/v2 community information, traps, and trap flags.

Configure the SNMPv1/v2 Community

Only the communities that you define using this screen will have access to the switch using the SNMPv1 and SNMPv2c protocols. Only those communities with read/write level access can be used to change the configuration using SNMP.

Use this screen when you are using the SNMPv1 and SNMPv2 protocol.

To add an SNMP community:

1. Select **System** > **SNMP** > **SNMP V1/V2** > **Community Configuration**.

Figure 53. SNMP V1/V2 Community Configuration

2. In the Management Station IP field, specify the IP address of the management station.

3. In the Management Station IP Mask field, specify the subnet mask to associate with the management station IP address.

    Together, the management station IP and the management station IP mask denote a range of IP addresses from which SNMP clients can use that community to access this device. If either (management station IP or management station IP mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's address is ANDed with the mask, as is the management station IP address; and, if the values are equal, access is allowed. For example, if the management station IP and management station IP mask parameters are 192.168.1.0/255.255.255.0, then any client whose address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a management station IP mask value of 255.255.255.255, and use that machine's IP address for client address.

4. In the Community String field, specify a community name.

5. From the Access Mode list, select the access level for this community, which is either Read/Write or Read Only.

6. From the Status list, enable or disable the community.

If you select Enable, the community name must be unique among all valid community names or the set request will be rejected. If you select Disable, the community name will become invalid.

7. Click the **Add** button.

To modify an existing community:

1. Select the check box next to the community.
2. Update the desired fields.
3. Click the **Apply** button.

To delete a community:

1. Select the check box next to the community to remove.
2. Click the **Delete** button.

Trap Configuration

Use this screen to configure settings for each SNMPv1 or SNMPv2 management host that will receive notifications about traps generated by the device. The SNMP management host is also known as the SNMP trap receiver.

To add an SNMP trap receiver:

1. Select **System** > **SNMP** > **SNMP V1/V2** > **Trap Configuration**

Figure 54. Trap Configuration

2. In the Recipients IP field, specify the IP address in x.x.x.x format to receive SNMP traps from this device.
3. From the Version list, select the trap version to be used by the receiver.
    • **SNMP v1**. The switch uses SNMP v1 to send traps to the receiver.
    • **SNMP v2**. The switch uses SNMP v2 to send traps to the receiver.
4. In the Community String field, specify the name of the SNMP community that includes the SNMP management host and the SNMP agent on the device.
5. From the Status list, select Enable to send traps to the receiver.
6. Click the **Add** button.

To modify information about an existing SNMP recipient:

1. Select the check box next to the recipient.
2. Update the desired fields.

3. Click the **Apply** button.

To delete an SNMP trap recipient:

1. Select the check box next to the recipient to remove.

2. Click the **Delete** button.

Trap Flags

Use the Trap Flags screen to enable or disable traps the switch can send to an SNMP manager. When the condition identified by an active trap is encountered by the switch, a trap message is sent to any enabled SNMP trap receivers, and a message is written to the trap log.

To configure the trap flags:

1. Select **System** > **SNMP** > **SNMP V1/V2** > **Trap Flags**.
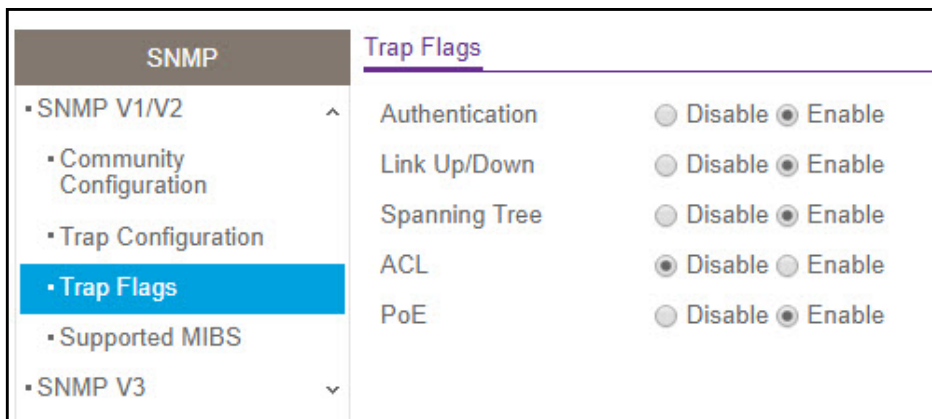
Figure 55. SNMP V1/V2 Trap Flags

2. Enable or disable the following system traps:

- **Authentication**. When enabled, SNMP traps are sent when events involving authentication occur, such as when a user attempts to access the device management interface and fails to provide a valid user name and password.

- **Link Up/Down**. When enabled, SNMP traps are sent when the administrative or operational state of a physical or logical link changes.

- **Spanning Tree**. When enabled, SNMP traps are sent when various spanning tree events occur.

- **ACL**. When enabled, SNMP traps are sent when a packet matches a configured ACL rule that includes ACL logging.

- **PoE**. When enabled, SNMP traps are sent when the PoE status changes.

3. Click the **Apply** button.

SNMP Supported MIBS

This screen displays a list of all MIBs supported by the switch.

To view the supported MIBs, select **System** > **SNMP** > **SNMP V1/V2** > **Supported MIBs.**

The following table describes the fields on the screen.

Table 32. SNMP MIB

Field	Description
Name	The name of the public or private MIB.
Description	A description of the MIB's purpose.

LLDP

The IEEE 802.1AB-defined standard, Link Layer Discovery Protocol (LLDP), allows stations on an 802 LAN to advertise major capabilities and physical descriptions. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

From the LLDP configuration menu, you can access the following links:

-
-
-
-
-
-
-

LLDP is a one-way protocol; there are no request and 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 or disabled separately per port. By default, both transmit and receive are enabled on all ports. The application is responsible for starting each transmit and receive state machine appropriately, based on the configured status and operational state of the port.

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

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority, and DiffServ settings), enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet endpoints.

- Inventory management, enabling network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

LLDP Configuration

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

To configure global LLDP settings:

1. Select **System > LLDP > Basic > LLDP Configuration**.

Figure 56. LLDP Configuration

2. (Optionally). Configure non-default values for the following LLDP properties.
   - **TLV Advertised Interval**. The number of seconds between transmissions of LLDP advertisements.
   - **Hold Multiplier**. The transmit interval multiplier value, where transmit hold multiplier × transmit interval = the time to live (TTL) value the device advertises to neighbors.
   - **Reinitializing Delay**. The number of seconds to wait before attempting to reinitialize LLDP on a port after the LLDP operating mode on the port changes.
   - **Transmit Delay**. The minimum number of seconds to wait between transmissions of remote data change notifications to one or more SNMP trap receivers configured on the switch.

3. (Optionally) In the Fast Start Duration field, configure a non-default value.

   This value sets the number of LLDP packets sent when the LLDP-MED fast start mechanism is initialized, which occurs when a new endpoint device links with the LLDP-MED network connectivity device.

4. Click the **Apply** button.

LLDP Port Settings

Use the LLDP Port Settings screen to specify per-interface LLDP settings.

To configure LLDP port settings:

1. Select **System** > **LLDP** > **Advanced** > **LLDP Port Settings**.

Figure 57. LLDP Port Settings

2. Select one or more ports to configure.
   - To configure a single port, select the check box associated with it, or type the port number in the Go To Interface field and click the **Go** button.
   - To configure multiple ports with the same settings, select the check box associated with each port to configure.
   - To configure all ports with the same settings, select the check box in the heading row.

3. Use the lists to configure the LLDP settings for the selected ports:
   - **Admin Status**. Select the status for transmitting and receiving LLDP packets:
     - **Tx Only**. Enable only transmitting LLDP PDUs on the selected ports.
     - **Rx Only**. Enable only receiving LLDP PDUs on the selected ports.
     - **Tx and Rx**. Enable both transmitting and receiving LLDP PDUs on the selected ports.
     - **Disabled**. Do not transmit or receive LLDP PDUs on the selected ports.

     The factory default is **Tx and Rx**.

   - **Management IP Address**. Choose whether to advertise the management IP address from the interface. The possible field values are:
     - **Stop Advertise**. Do not advertise the management IP address from the interface.
     - **Auto Advertise**. Advertise the current IP address of the device as the management IP address.

     The factory default is **Auto Advertise**.

   - **Notification**. When notifications are enabled, LLDP interacts with the trap manager to notify subscribers of remote data change statistics. The default is **Disable**.
   - **Optional TLV(s)**. Enable or disable the transmission of optional type-length value (TLV) information from the interface. The factory default is **Enable.** The TLV

information includes the system name, system description, system capabilities, and port description. For information about how to configure the system name, see Management on page 35. For information about how to configure the port description, see Ports on page 132.

4. Click the **Apply** button.

LLDP-MED Network Policy

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

To view LLDP-MED network policy information for an interface:

1. Select **System** > **LLDP** > **Advanced** > **LLDP-MED Network Policy**.
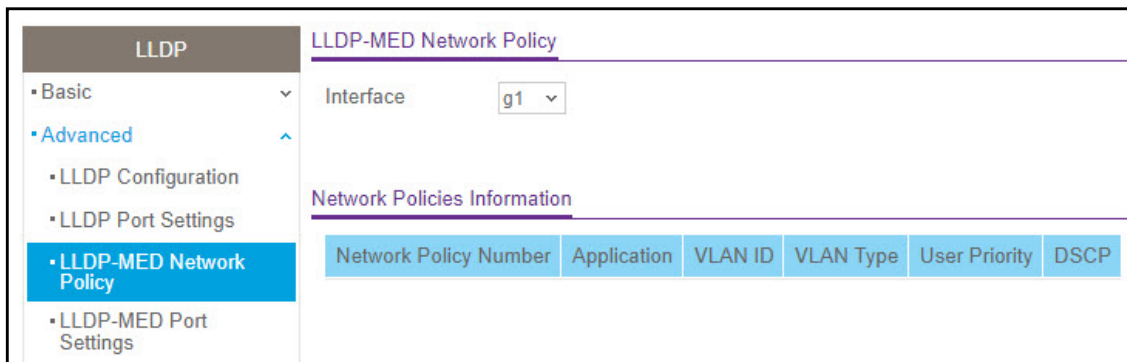
Figure 58. LLDP-MED Network Policy

2. From the Interface list, select the interface with the information to view.

Note: The list includes only the interfaces on which LLDP is enabled. If no interfaces are enabled for LLDP, the Interface list does not display.

The screen refreshes and displays the data transmitted in the network policy TLVs. for the interface. The following table describes the LLDP-MED network policy information that displays on the screen.

Table 33. LLDP-MED network policy information

Field	Description
Network Policy Number	The policy number.
Application	The media application type associated with the policy, which can be one of the following: • Unknown • Voice • Guest Voice • Guest Voice Signaling • Softphone Voice • Video Conferencing • Streaming Video • Video Signaling A port can receive multiple application types. The application information is displayed only if a network policy TLV has been transmitted from the port.
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Indicates whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.

LLDP-MED Port Settings

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

To configure LLDP-MED settings for a port:

1. Select **System** > **LLDP** > **Advanced** > **LLDP-MED Port Settings**.

Figure 59. LLDP-MED Port Settings

2. From the Port list, select the port to configure.

3. Use the lists to enable or disable the following LLDP-MED settings for the selected port:

- **LLDP-MED Status**. The administrative status of LLDP-MED on the interface. When LLDP-MED is enabled, the transmit and receive function of LLDP is effectively enabled on the interface.

- **Notification**. When enabled, the port sends a topology change notification if a device is connected or removed.

- **Transmit Optional TLVs**. When enabled, the port transmits the following optional type length values (TLVs) in the LLDP PDU frames:

  - MED Capabilities
  - Network Policy
  - Location Identification
  - Extended Power via MDI: PSE
  - Extended Power via MDI: PD
  - Inventory

4. Click the **Apply** button.

LLDP-MED Neighbors Information

Use this screen to display the LLDP-MED Neighbors/Remote Device information.

To display the LLDP-MED Neighbors Information:

1. Select **System** > **LLDP** > **Advanced** > **LLDP-MED Neighbors Information**.

Figure 60. LLDP-MED Neighbors Information

2. In the **LLDP-MED Interface Selection** section of the window, the **Interface** field lists all the ports on which LLDP-MED is enabled. Select the interface from the **Interface** list to display information about that interface.

3. Table 34, LLDP-MED Neighbors Information below describes the non-configurable LLDP-MED Neighbors information for the selected interface.

4. Click the **Refresh** button to refresh the information on the page with the latest information on the switch.

Table 34. LLDP-MED Neighbors Information

Field	Description
LLDP-MED Interface Selection	
Remote ID	Specifies the remote client identifier assigned to the remote system.

Table 34. LLDP-MED Neighbors Information (continued)

Field	Description
Capability Information	This table specifies the supported and enabled capabilities received in MED TLV on this port.
Supported Capabilities	Specifies supported capabilities received in MED TLV on this port.
Enabled Capabilities	Specifies enabled capabilities received in MED TLV on this port.
Device Class	Specifies the device class as advertised by the device remotely connected to the port.
Network Policies Information	This table specifies if network policy TLV is received in the LLDP frames on this port.
Media Application Type	Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, videosignalling. Each application type that is received has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been received on this port, only then would this information be displayed.
VLAN ID	Specifies the VLAN ID associated with a particular policy type.
Priority	Specifies the priority associated with a particular policy type.
DSCP	Specifies the DSCP associated with a particular policy type.
Unknown Bit Status	Specifies the unknown bit associated with a particular policy type.
Tagged Bit Status	Specifies the tagged bit associated with a particular policy type.
Inventory Information	This table specifies if inventory TLV is received in LLDP frames on this port.
Hardware Revision	Specifies the hardware version of the remote device.
Firmware Revision	Specifies the firmware version of the remote device.
Software Revision	Specifies the software version of the remote device.
Serial Number	Specifies the serial number of the remote device.
Manufacturer Name	Specifies the manufacturer name of the remote device.
Model Name	Specifies the model name of the remote device.
Asset ID	Specifies the asset ID of the remote device.
Location Information	This table specifies if location TLV is received in LLDP frames on this port.
Sub Type	Specifies the type of location information.
Location Information	Specifies the location information in a string for a given type of location ID.
Extended PoE	This table specifies if the remote device is a PoE device.
Device Type	Specifies the remote device's PoE device type connected to this port.

Table 34. LLDP-MED Neighbors Information (continued)

Field	Description
Extended PoE PSE	This table specifies if the extended PSE TLV is received in an LLDP frame on this port.
Device Type	Specifies the remote device's PoE device type connected to this port.
Power Source	Specifies the remote port's PSE power source.
Power Priority	Specifies the remote port's PSE power priority.
Power Value	Specifies the remote port's PSE power value in tenths of watts.
Extended PoE PD	This table specifies if extended PD TLV is received in an LLDP frame on this port.
Device Type	Specifies the remote device's PoE device type connected to this port.
Power Source	Specifies the remote port's PD power source.
Power Priority	Specifies the remote port's PD power priority.
Power Value	Specifies the remote port's PD power value.

Local Information

Use the LLDP Local Information screen to view the data that each port advertises through LLDP. To view local LLDP information, select **System** > **Advanced** > **LLDP** > **Local Information**.

Note: The screen includes only the interfaces on which LLDP is enabled.

Figure 61. LLDP Local Device Information

The following table describes the LLDP device information and port summary information.

Table 35. LLDP local device information

Field	Description
Chassis ID Subtype	The type of information used to identify the switch in the Chassis ID field.
Chassis ID	The hardware platform identifier for the switch.
System Name	The user-configured system name for the switch.
System Description	The switch description, which includes information about the product model and platform.
System Capabilities	The primary functions the switch supports.
Interface	The interface associated with the rest of the data in the row.
Port ID Subtype	The type of information used to identify the interface in the Port ID field.
Port ID	The port number.
Port Description	The user-defined description of the port. For information about how to configure the port description, see Ports on page 132.
Advertisement	The TLV advertisement status of the port.

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

Figure 62. LLDP-MED Local Port Information

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

Table 36. Detailed LLDP local port information

Field	Description
Managed Address	
Address SubType	The type of address the management interface uses, such as an IPv4 address.
Address	The address used to manage the device.
Interface SubType	The port subtype.
Interface Number	The number that identifies the port.
MAC/PHY Details	
Auto Negotiation Supported	Indicates whether the interface supports port speed autonegotiation. The possible values are True or False.
Auto Negotiation Enabled	The port speed autonegotiation support status. The possible values are True (enabled) or False (disabled).
Auto Negotiation Advertised Capabilities	The port speed auto-negotiation capabilities such as 1000BASE-T half-duplex mode or 100BASE-TX full-duplex mode.
Operational MAU Type	The Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network.
MED Details	
Capabilities Supported	The MED capabilities enabled on the port.
Current Capabilities	The TLVs advertised by the port.
Device Class	Network Connectivity indicates the device is a network connectivity device.
Network Policies	
Application Type	The media application type associated with the policy.
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.

Neighbors Information

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

To view LLDP information received from a neighbor device, select **System** > **Advanced** > **LLDP** > **Neighbors Information**.

Note: If no information has been received from a neighbor device, or if the link partner is not LLDP-enabled, no information displays.

\

Neighbors Information						
MSAP Entry	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name
2	g1	MAC Address	00:1E:C9:AA:AB:F7	Interface Name	Gi1/0/9	

Figure 63. LLDP Neighbors Information

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

Table 37. LLDP neighbor summary information

Field	Description
MSAP Entry	The Media Service Access Point (MSAP) entry number for the remote device.
Local Port	The interface on the local system that received LLDP information from a remote system.
Chassis ID Subtype	The type of data displayed in the Chassis ID field on the remote system.
Chassis ID	The remote 802 LAN device's chassis.
Port ID Subtype	The type of data displayed in the remote system's Port ID field.
Port ID	The physical address of the port on the remote system from which the data was sent.
System Name	The system name associated with the remote device. If the field is blank, the name might not be configured on the remote system.

To view additional information about the remote device, click the link in the MSAP Entry field. A pop-up window displays information for the selected port.

The following table describes the information transmitted by the neighbor.

Table 38. LLDP neighbor details

Field	Description
Port Details	
Local Port	The interface on the local system that received LLDP information from a remote system.
MSAP Entry	The Media Service Access Point (MSAP) entry number for the remote device.
Basic Details	
Chassis ID Subtype	The type of data displayed in the Chassis ID field on the remote system.
Chassis ID	The remote 802 LAN device's chassis.
Port ID Subtype	The type of data displayed in the remote system's Port ID field.
Port ID	The physical address of the port on the remote system from which the data was sent.
Port Description	The user-defined description of the port.
System Name	The system name associated with the remote device.
System Description	The description of the selected port associated with the remote system.
System Capabilities	The system capabilities of the remote system.
Managed Addresses	
Address SubType	The type of the management address.
Address	The advertised management address of the remote system.
Interface SubType	The port subtype.
Interface Number	The port on the remote device that sent the information.
MAC/PHY Details	
Auto-Negotiation Supported	Specifies whether the remote device supports port-speed auto-negotiation. The possible values are True or False.
Auto-Negotiation Enabled	The port speed autonegotiation support status. The possible values are True or False
Auto Negotiation Advertised Capabilities	The port speed autonegotiation capabilities.
Operational MAU Type	The Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network.

Table 38. LLDP neighbor details (continued)

Field	Description
MED Details	
Capabilities Supported	The supported capabilities that were received in MED TLV from the device.
Current Capabilities	The advertised capabilities that were received in MED TLV from the device.
Device Class	The LLDP-MED endpoint device class. The possible device classes are: • Endpoint Class 1 Indicates a generic endpoint class, offering basic LLDP services. • Endpoint Class 2 Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features. • Endpoint Class 3 Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support and device information management capabilities.
Hardware Revision	The hardware version advertised by the remote device.
Firmware Revision	The firmware version advertised by the remote device.
Software Revision	The software version advertised by the remote device.
Serial Number	The serial number advertised by the remote device.
Model Name	The model name advertised by the remote device.
Asset ID	The asset ID advertised by the remote device.
Location Information	
Civic	The physical location, such as the street address, the remote device has advertised in the location TLV. For example, 123 45th St. E. The field value length range is 6–160 characters.
Coordinates	The location map coordinates the remote device has advertised in the location TLV, including latitude, longitude, and altitude.
ECS ELIN	The Emergency Call Service (ECS) Emergency Location Identification Number (ELIN) the remote device has advertised in the location TLV. The field range is 10–25.
Unknown	Displays unknown location information for the remote device.
Network Policies	
Application Type	The media application type associated with the policy advertised by the remote device.
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.

Table 38. LLDP neighbor details (continued)

Field	Description
LLDP Unknown TLVs	
Type	The unknown TLV type field.
Value	The unknown TLV value field.

Services

This section describes how to configure the DHCP L2 Relay, DHCP snooping, DHCPv6 snooping, and Dynamic ARP Inspection (DAI) features on the switch. DHCP snooping and DAI are layer 2 security features that examine traffic to help prevent accidental and malicious attacks on the switch or network. From the Services configuration menu, you can access screens described in the following sections:

-
-
-
-

DHCP L2 Relay

DHCP relay agents eliminate the need to have a DHCP server on each physical network. Relay agents populate the giaddr field and also append the Relay Agent Information option to the DHCP messages. DHCP servers use this option for IP addresses and other parameter assignment policies. These DHCP relay agents are typically IP routing-aware devices and are referred to as Layer 3 relay agents. In some network configurations, there is a need for Layer 2 devices to append the Relay Agent Information option as they are closer to the end hosts.

These Layer 2 devices typically operate only as bridges for the network and might not have an IPv4 address on the network. Lacking a valid IPv4 source address, they cannot relay packets directly to a DHCP server located on another network. These Layer 2 devices append the Relay Agent Information option and broadcast the DHCP message.

DHCP L2 Relay Global Configuration

Use this screen to view and configure the global settings for DHCP snooping.

To enable DHCP L2 Relay global settings:

1. Select **System** > **Services** > **DHCP L2 Relay** > **DHCP L2 Relay Global Configuration**.
2. Next to **DHCP L2 Relay Global Configuration**, select **Enable** in the **Admin Mode** field. The factory default Admin Mode is Disabled.

3. Click the **Apply** button. The updated configuration is sent to the switch. Configuration changes take effect immediately.

4. Click the **Cancel** button to cancel the configuration on the screen, and reset the data displayed on the screen to the latest value of the switch.

DHCP L2 Relay VLAN Configuration

Use this screen to configure the DHCP L2 Relay VLAN.

Figure 64. DHCP L2 Relay VLAN Configuration

To configure DHCP L2 Relay VLAN:

1. Select **System** > **Services** > **DHCP L2 Relay** > **DHCP L2 Relay Global Configuration**.

2. **VLAN ID** shows the VLAN ID configured on the switch. Select the ID number of the VLAN to configure.

> **Note:** For VLAN IDs to appear in the table, they must first be configured using the **Switching > VLAN** menu. For more information see Basic VLAN Configuration on page 140.

3. Use the **Admin Mode** field to **Enable** or **Disable** DHCP L2 Relay on the selected VLAN. The factory default is Disabled.

4. Use the **Circuit ID Mode** field to **Enable** or **Disable** the Circuit ID sub option of DHCP Option-82. The factory default is Disabled.

5. Use the **Remote ID String** field to specify the Remote ID String. The string can contain up to 32 characters.

6. Click the **Apply** button. The updated configuration is sent to the switch. Configuration changes take effect immediately.

7. Click the **Cancel** button to cancel the configuration on the screen, and reset the data displayed on the screen to the latest value of the switch.

DHCP L2 Relay Interface Configuration

Use this screen to view and configure the DHCP L2 Relay Interface.

Figure 65. DHCP L2 Relay Interface Configuration

To configure DHCP L2 Relay Interface settings:

1. Select **System** > **Services** > **DHCP L2 Relay** > **DHCP L2 Relay Interface Configuration**.

2. In the **Go To Interface** field, enter the interface in unit/slot/port format and click on the **Go** button. The entry corresponding to the specified interface is selected.

3. The **Interface** field shows the interface from which the DHCP message is received.

4. In the **Admin Mode** field, enable or disable the DHCP L2 Relay on the selected interface. The default is **Disable**.

5. In the **82 Option Trust Mode**, enable or disable an interface to be trusted for DHCP L2 Relay (Option-82) received. The default is **Disable**.

6. Click the **Apply** button. The updated configuration is sent to the switch. Configuration changes take effect immediately.

7. Click the **Cancel** button to cancel the configuration on the screen, and reset the data displayed on the screen to the latest value of the switch.

DHCP L2 Relay Interface Statistics

The DHCP L2 Relay Interface Statistics table shows information about the DHCP L2 Relay interface.

Figure 66. DHCP L2 Relay Interface Statistics

Table 39 describes the non-configurable data that is displayed.

Table 39. DHCP L2 Relay Interface Statistics

Field	Description
Interface	The interface from which the DHCP message is received.
Untrusted Server Messages With Opt82	The number of DHCP message with option82 received from an untrusted server.
Untrusted Client Messages With Opt82	The number of DHCP message with option82 received from an untrusted client.
Trusted Server Messages Without Opt82	The number of DHCP message without option82 received from a trusted server.
Trusted Client Messages Without Opt82	The number of DHCP message without option82 received from a trusted client.

Click the **Clear** button to reset the DHCP L2 Relay Interface statistics.

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

The latest DHCP L2 Relay Interface statistics is displayed.

DHCP Snooping

DHCP snooping is a useful feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

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

Global Configuration

Use this screen to view and configure the global settings for DHCP snooping.

To configure DHCP snooping global settings:

1. Select **System** > **Services** > **DHCP Snooping** > **Global Configuration**.

Figure 67. DHCP Snooping Global Configuration

2. Next to **DHCP Snooping Mode**, enable the DHCP Snooping feature. The factory default is **Disabled**.

3. (Optionally) Next to **MAC Address Validation**, enable the verification of the sender MAC address for DHCP snooping. The factory default is **Enabled**.

   When MAC address validation is enabled, the device checks packets that are received on an untrusted interface to verify that the MAC address and the DHCP client hardware address match. If the addresses do not match, the device drops the packet.

4. Click the **Apply** button.

To enable DHCP snooping for all interfaces that are members of a VLAN:

1. In the **VLAN ID** field, specify the VLAN on which DHCP snooping is enabled.

2. From the **DHCP Snooping Mode** list, select **Enable**.

3. Click the **Apply** button.

Interface Configuration

Use the DHCP Snooping Interface Configuration screen to view and configure each port as a trusted or untrusted port. Any DHCP responses received on a trusted port are forwarded. If a port is configured as untrusted, any DHCP (or BootP) responses received on that port are discarded.

To configure DHCP snooping interface settings:

1. Select **System** > **Services** > **DHCP Snooping** > **Interface Configuration**.

Figure 68. DHCP Snooping Interface Configuration

2. Select one or more ports or LAGs to configure.

   For information about how to select and configure one or more ports and LAGs, see Configuring Interface Settings on page 28.

3. From the **Trust Mode** list, select the desired trust mode.

   - **Disabled**. The interface is considered to be untrusted and could potentially be used to launch a network attack. DHCP server messages are checked against the bindings database. On untrusted ports, DHCP snooping enforces the following security rules:

     - DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped.

     - DHCPRELEASE and DHCPDECLINE messages are dropped if the MAC address is in the snooping database but the binding's interface is other than the interface where the message was received.

     - DHCP packets are dropped when the source MAC address does not match the client hardware address if MAC address validation is globally enabled.

   - **Enabled**. The interface is considered to be trusted and forwards DHCP server messages without validation.

4. From the **Logging Invalid Packets** list, select the packet logging mode.

When enabled, the DHCP snooping feature generates a log message when an invalid packet is received and dropped by the interface.

5. In the **Rate Limit (pps) field**, specify the rate limit value for DHCP snooping purposes.

   If the incoming rate of DHCP packets exceeds the value of this object for consecutively burst interval seconds, the port will be shut down. If this value is N/A, then the burst interval has no meaning, and rate limiting is disabled.

6. In the **Burst Interval (secs) field**, specify the burst interval value for rate limiting purposes on this interface.

   If the rate limit is N/A, then the burst interval has no meaning and the field displays N/A.

7. Click the **Apply** button.

Binding Configuration

Use this screen to view, add, and remove static bindings in the DHCP snooping bindings database and to view or clear the dynamic bindings in the bindings table.

To configure static DHCP bindings:

1. Select **System** > **Services** > **DHCP Snooping** > **Binding Configuration**.

Figure 69. DHCP Snooping Binding Configuration

2. From the Interface list, select the interface on which the DHCP client is authorized.
3. In the **MAC Address** field, specify the MAC address for the binding to be added.

   This is the key to the binding database.

4. From the **VLAN ID** list, select the ID of the VLAN the client is authorized to use.
5. In the **IP Address field**, specify the IP address of the client.
6. Click the **Add** button**.**

   The DHCP snooping binding entry is added to the database.

The DHCP Snooping Dynamic Binding Configuration table shows information about the DHCP bindings that have been learned on each interface on which DHCP snooping is enabled. Table 40 describes the dynamic bindings information.

Table 40. DHCP Snooping Dynamic Binding Information

Field	Description
Interface	The interface on which the DHCP client message was received.
MAC Address	The MAC address associated with the DHCP client that sent the message. This is the key to the binding database.
VLAN ID	The VLAN ID of the client interface.
IP Address	The IP address assigned to the client by the DHCP server.
Lease Time	The remaining IP address lease time for the client.

Persistent Configuration

Use this screen to configure the persistent location of the DHCP snooping bindings database. The bindings database can be stored locally on the device or on a remote system somewhere else in the network. The device must be able to reach the IP address of the remote system to send bindings to a remote database.

To configure DHCP snooping persistent settings:

1. Select **System** > **Services** > **DHCP Snooping** > **Persistent Configuration**.

Figure 70. DHCP Snooping Persistent Configuration

2. Specify where the DHCP snooping bindings database is located.
   - **Local**. The binding table will be stored locally on the switch.
   - **Remote**. The binding table will be stored on a remote TFTP server.

   If the database is stored on a remote server:

   a. Specify the IP address of the TFTP server.

   b. Specify the file name of the DHCP snooping bindings database in which the bindings are stored.

3. In the **Write Delay** field, specify the amount of time to wait between writing bindings information to persistent storage.

The delay allows the device to collect as many entries as possible (new and removed) before writing them to the persistent file.

4. Click the **Apply** button.

DHCP Snooping Statistics

Use this screen to view and clear per-interface statistics about the DHCP messages filtered by the DHCP snooping feature on untrusted interfaces.

To view and clear the DHCP snooping statistics:

1. Select **System** > **Services** > **DHCP Snooping** > **Statistics**.

Figure 71. DHCP Snooping Statistics

2. Click **Clear** to clear all interfaces statistics.

The following table describes the DHCP snooping statistics.

Table 41. DHCP snooping statistics

Field	Description
Interface	The interface associated with the rest of the data in the row.
MAC Verify Failures	The number of DHCP messages that were dropped because the source MAC address and client hardware address did not match. MAC address verification is performed only if it is globally enabled.
Client Ifc Mismatch	The number of packets that were dropped by DHCP snooping because the interface and VLAN on which the packet was received does not match the client's interface and VLAN information stored in the binding database.
DHCP Server Msgs Received	The number of DHCP server messages ((DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) that have been dropped on an untrusted port.

DHCPv6 Snooping

DHCPv6 snooping is a useful feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCPv6 snooping acts like a firewall between untrusted hosts and DHCP servers. It also provides way to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Global Configuration

Use this screen to view and configure the global settings for DHCPv6 snooping.

To configure DHCPv6 snooping global settings:

1. Select **System** > **Services** > **DHCPv6 Snooping** > **Global Configuration**.
2. Next to **DHCPv6 Snooping Mode**, enable the DHCPv6 Snooping feature. The factory default is **Disabled**.
3. (Optionally) Next to **MAC Address Validation**, enable the verification of the sender MAC address for DHCPv6 snooping. The factory default is **Enabled**.

   When MAC address validation is enabled, the device checks packets that are received on an untrusted interface to verify that the MAC address and the DHCPv6 client hardware address match. If the addresses do not match, the device drops the packet.
4. Click the **Apply** button.

To enable DHCPv6 snooping for all interfaces that are members of a VLAN:

1. In the **VLAN ID** field, specify the VLAN on which DHCPv6 snooping is enabled.
2. From the **DHCPv6 Snooping Mode** list, select **Enable**.
3. Click the **Apply** button.

Interface Configuration

Use the DHCPv6 Snooping Interface Configuration screen to view and configure each port as a trusted or untrusted port. Any DHCPv6 responses received on a trusted port are forwarded. If a port is configured as untrusted, any DHCPv6 (or BootP) responses received on that port are discarded.

To configure DHCPv6 snooping interface settings:

1. Select **System** > **Services** > **DHCPv6 Snooping** > **Interface Configuration**.

2. Select one or more ports or LAGs to configure.

   For information about how to select and configure one or more ports and LAGs, see Configuring Interface Settings on page 28.

3. **From the Trust Mode** list, select the desired trust mode. The factory default is Disabled.

   • **Disabled**. The interface is considered to be untrusted and could potentially be used to launch a network attack. DHCP server messages are checked against the bindings database. On untrusted ports, DHCP snooping enforces the following security rules:

   - DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped.

   - DHCPRELEASE and DHCPDECLINE messages are dropped if the MAC address is in the snooping database but the binding's interface is other than the interface where the message was received.

   - DHCP packets are dropped when the source MAC address does not match the client hardware address if MAC address validation is globally enabled.

   • **Enabled**. If Trust Mode is enable, the DHCPv6 snooping application considers the port as trusted and forwards DHCP server messages without validation.

4. From the **Invalid Packets** list, select the packet logging mode. The default is Disabled.

   When enabled, the DHCPv6 snooping application generates a log message when an invalid packet is received and dropped by the interface.

5. In the **Rate Limit (pps)** field, specify the rate limit value for DHCPv6 snooping purposes.

   If the incoming rate of DHCPv6 packets exceeds the value of this object for consecutively burst interval seconds, the port will be shut down. If this value is None, then the burst interval has no meaning, and rate limiting is disabled. The default value is None. It can be set to a value –1, which means None. The Rate Limit range is 0 to 300.

6. In the **Burst Interval (secs)** field, specify the burst interval value for rate limiting purposes on this interface.

   If the rate limit is None, then the burst interval has no meaning and the field displays N/A. The default value is N/A. The range of Burst Interval is 1 to 15.

7. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

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

Binding Configuration

Use this screen to view, add, and remove static bindings in the DHCPv6 snooping bindings database and to view or clear the dynamic bindings in the bindings table.

To configure static DHCPv6 bindings:

1. Select **System** > **Services** > **DHCPv6 Snooping** > **Binding Configuration**.
2. From the Interface list, select the interface to add a binding into the DHCPv6 snooping database.
3. In the **MAC Address** field, specify the MAC address for the binding to be added.

    This is the key to the binding database.

4. From the **VLAN ID** list, select the VLAN for the binding rule. The VLAN ID range is 1 to 4093.
5. In the **IPv6 Address** field, specify a valid IPv6 address for the binding rule.
6. Click the **Add** button to the DHCPv6 snooping binding entry to the database.
7. Click the **Delete** button to delete selected static entries from the database.
8. Click the **Cancel** button to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The DHCPv6 Snooping Dynamic Binding Configuration table shows information about the DHCPv6 bindings that have been learned on each interface on which DHCPv6 snooping is enabled. Table 40 describes the dynamic bindings information.

Table 42. DHCPv6 Snooping Dynamic Binding Information

Field	Description
Interface	The interface on which the DHCPv6 client message was received.
MAC Address	The MAC address associated with the DHCP client that sent the message. This is the key to the binding database.
VLAN ID	The VLAN ID for the binding entry in the binding database. The VLAN ID range is 1 to 4093.
IPv6 Address	The IPv6 address for the binding entry in the binding database.
Lease Time	The remaining lease time for the dynamic entries.

9. Click **Clear** to clear the configuration and reset all statistics for the selected interface to the default values.
10. Click **Refresh** to refresh the data on the screen with the latest DHCPv6 snooping dynamic binding information on the switch.

Persistent Configuration

Use this screen to configure the persistent location of the DHCPv6 snooping bindings database. The bindings database can be stored locally on the device or on a remote system somewhere else in the network. The device must be able to reach the IP address of the remote system to send bindings to a remote database.

To configure DHCP snooping persistent settings:

1. Select **System** > **Services** > **DHCPv6 Snooping** > **Persistent Configuration**.
2. Specify where the DHCPv6 snooping bindings database is located.
   - **Local**. The binding table will be stored locally on the switch.
   - **Remote**. The binding table will be stored on a remote TFTP server.

   If the database is stored on a remote server:

   a. Specify the **Remote IP Address** of the TFTP server on which the snooping database is stored when **Remote** is selected.
   b. Specify the **Remote File Name** of the DHCPv6 snooping bindings database in which the bindings are stored when **Remote** is selected. The Remote File Name can be 1 to 32 alphanumeric characters.

3. In the **Write Delay** field, specify the maximum amount of time to wait between writing bindings information to persistent storage. The Write Delay range is 15 to 86400 seconds. The default is 300 seconds.

   The delay allows the device to collect as many entries as possible (new and removed) before writing them to the persistent file.

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

DHCPv6 Snooping Statistics

Use this screen to view and clear per-interface statistics about the DHCPv6 messages filtered by the DHCPv6 snooping feature on untrusted interfaces.

To view and clear the DHCPv6 snooping statistics:

1. Select **System** > **Services** > **DHCPv6 Snooping** > **Statistics**.
2. Click **Clear** to clear all interfaces statistics.
3. Click **Refresh** to refresh the data on the page with the latest information on the switch.

The following table describes the DHCP snooping statistics.

Table 43. DHCPv6 snooping statistics

Field	Description
Interface	The untrusted and snooping-enabled interface on which statistics are displayed.
MAC Verify Failures	The number of packets that were dropped by DHCPv6 snooping because the source MAC address and client hardware address did not match. MAC address verification is performed only if it is globally enabled.

Table 43. DHCPv6 snooping statistics (continued)

Field	Description
Client Ifc Mismatch	The number of DHCPv6 messages that were dropped by DHCPv6 snooping based on the source MAC address and client hardware address verification.
DHCPv6 Server Msgs Received	The number of DHCPv6 server messages ((DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) that have been dropped on an untrusted port.

Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The malicious attacker sends ARP requests or responses mapping another station's IP address to its own MAC address.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

When DAI is enabled on a VLAN, DAI is enabled on the interfaces (physical ports or LAGs) that are members of that VLAN. Individual interfaces are configured as trusted or untrusted. The trust configuration for DAI is independent of the trust configuration for DHCP snooping.

Configure DAI on a VLAN and an Interface

In this example, DAI is enabled on VLAN 100. Ports 1-10 connect end users to the network and are members of VLAN 100. These ports are configured to limit the maximum number of ARP packets with a rate limit of 10 packets per second. LAG 1, which is also a member of VLAN 100 and contains ports 11-14, is the trunk port that connects the switch to the data center, so it is configured as a trusted port.

This example assumes VLAN 100 and LAG 1 have already been configured.

To configure DAI on a VLAN and an Interface:

1. Enable DAI on VLAN 1.

    a. Select **System** > **Services** > **Dynamic ARP Inspection** > **DAI VLAN Configuration.**

    b. Next to VLAN 1, select the check box

    c. From the Admin Mode list, select **Enable**.

Figure 72. DAI VLAN Configuration

    d. Click the **Apply** button.

2. Configure LAG 1, which includes ports 11-14, as a trusted port. All other interfaces are untrusted by default.

    a. Select **System** > **Services** > **Dynamic ARP Inspection** > **DAI Interface Configuration.**

    b. Click the **LAGS** link to view all LAG interfaces.

    c. Next to l1, select the check box.

    d. From the Trust Mode list, select **Enable**.

Figure 73. DAI Interface Configuration - LAGS

    e. Click the **Apply** button.

3. Configure rate limiting for ports 1–8, which are untrusted ports.

    a. Click **1** in the interface-selection field to view all ports.

    b. Select each check box associated with ports 1–8.

    c. In the Rate Limit field, type **10**.

Figure 74. DAI Interface Configuration - Rate Limiting

    d. Click the **Apply** button.

Configure a DAI ACL

DAI relies on the information in the DHCP snooping bindings database to validate ARP packets. For networks that use static IP addresses and do not use DHCP, DAI access control lists (ACLs) can be used to statically map an IP address to a MAC address on a VLAN. When hosts use static IP addresses, the DHCP snooping feature cannot build a bindings database. DAI ACLs are also useful when other switches in the network do not run DAI.

DAI consults the static mappings configured in the DAI ACLs before it consults the DHCP snooping bindings database; thus static mappings have precedence over DHCP snooping bindings. If the static flag is enabled on a VLAN, DAI consults the DAI ACL only and does not validate ARP information against the DHCP snooping bindings database.

To configure a DAI ACL with three rules and associate it with VLAN 100:

1. Select **System** > **Services** > **Dynamic ARP Inspection** > **DAI ACL Configuration.**

2. In the Name field, specify a name for the ACL, for example arpACL.

3. Click the **Add** button.

    The screen displays the new ACL.
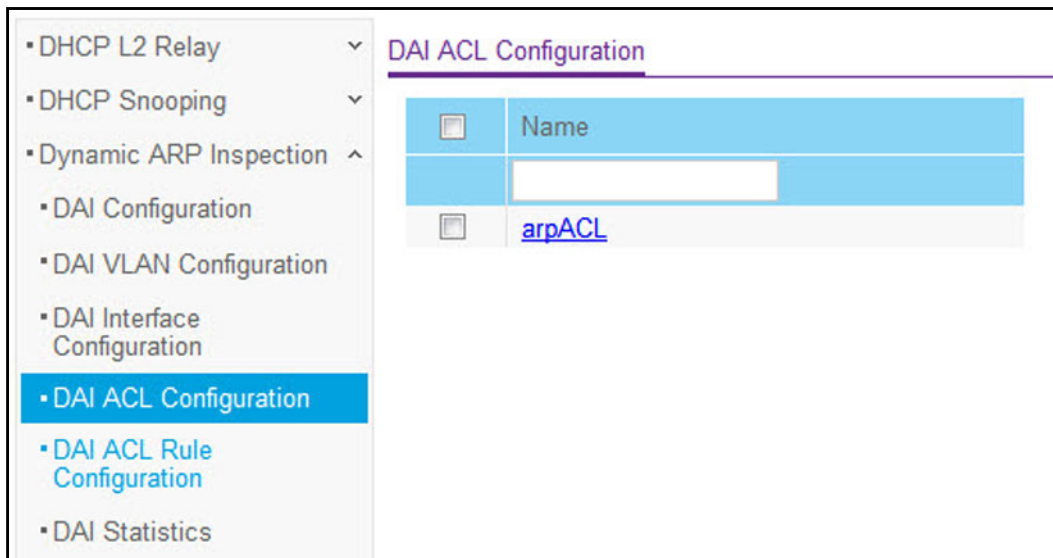
Figure 75. DAI ACL Configuration

4. Click the ACL name, which is a hyperlink to the Dynamic ARP Inspection ACL Rules Configuration page.

5. From the ACL Name list, select the DAI ACL to configure.

6. In the Source IP Address field, specify the IP address of a host.

7. In the Source MAC Address field, specify the MAC address of the host that is statically mapped to the IP address specified in the Source IP Address field.

8. Click the **Add** button.

9. Repeat Step 6 through Step 8 to add the second rule.

   You can add up to 20 static IP address-MAC address mappings to a DAI ACL.
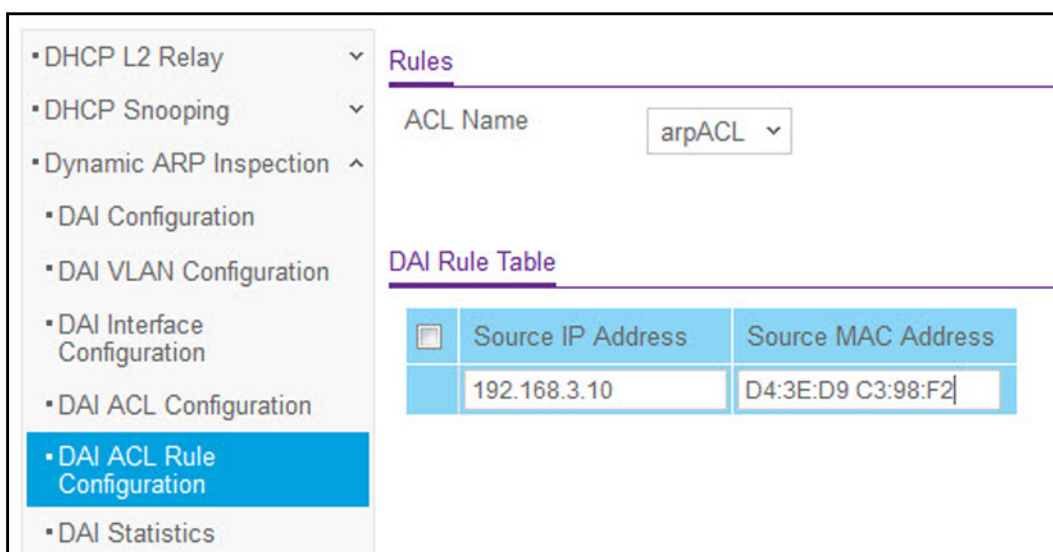
Figure 76. DAI Rule Table

10. Select **System** > **Services** > **Dynamic ARP Inspection** > **DAI VLAN Configuration.**

11. Next to VLAN 100, select the check box.

12. In the ARP ACL Name field, specify the name of the DAI ACL to associate with the VLAN.

13. Click the **Apply** button.

Figure 77. ARP ACL Name

Configure Optional DAI Features

If you configure the source MAC address validation option, DAI verifies that the sender MAC address in an ARP packet equals the source MAC address in the Ethernet header. There is a configurable option to verify that the target MAC address in the ARP packet equals the destination MAC address in the Ethernet header. This check applies only to ARP responses, since the target MAC address is unspecified in ARP requests. You can also enable IP address checking. When this option is enabled, DAI drops ARP packets with an invalid IP address. The following IP addresses are considered invalid:

*   0.0.0.0
*   255.255.255.255
*   All IP multicast addresses
*   All class E addresses (240.0.0.0/4)
*   Loopback addresses (in the range 127.0.0.0/8)

The valid IP check is applied only on the sender IP address in ARP packets. In ARP response packets, the check is applied only on the target IP address.

To configure the optional DAI features:

1. Select **System** > **Services** > **Dynamic ARP Inspection** > **DAI Configuration.**

2. Next to Validate Source MAC, select the **Enable** radio button.

3. Next to Validate Destination MAC, select the **Enable** radio button.

4. Next to Validate IP, select the **Enable** radio button.
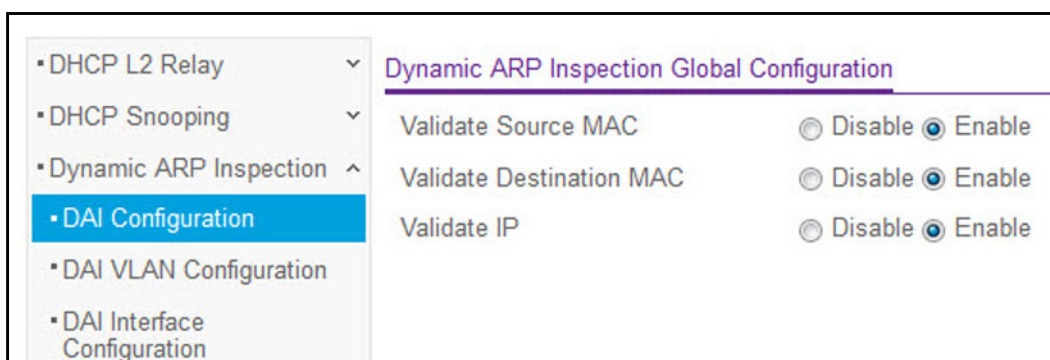
Figure 78. DAI Global Configuration

5. Click the **Apply** button.

The additional ARP validations are performed on packets received on VLANs that are enabled for DAI and interfaces configured as untrusted.

Display DAI Statistics

To display and clear the DAI statistics per VLAN:

1. Select **System** > **Services** > **Dynamic ARP Inspection** > **Statistics**.

Figure 79. Dynamic ARP Inspection Statistics

2. Click **Clear** to clear all DAI statistics.

3. Click **Refresh** to refresh the data on the page with the latest information on the switch.

Table 44, Dynamic ARP Inspection (DAI) statistics describes the Dynamic ARP Inspection (DAI) statistics.

Table 44. Dynamic ARP Inspection (DAI) statistics

Field	Description
VLAN	The enabled VLAN ID for which statistics are displayed.
DHCP Drops	The number of ARP packets that were dropped by DAI as there is no matching DHCP Snooping binding entry found.
DHCP Permits	The number of ARP packets that were forwarded by DAI as there is a matching DHCP Snooping binding entry found
ACL Drops	The number of ARP packets that were dropped by DAI as there is no matching ARP ACL rule found for this VLAN, and the static flag is set on this VLAN.

Table 44. Dynamic ARP Inspection (DAI) statistics (continued)

Field	Description
ACL Permits	The number of ARP packets that were permitted by DAI, as there is a matching ARP ACL rule found for this VLAN
Bad Source MAC	The number of ARP packets that were dropped by DAI because the sender MAC address in the ARP packet did not match the source MAC in the Ethernet header.
Bad Dest MAC	The number of ARP packets that were dropped by DAI because the target MAC address in the ARP reply packet did not match the destination MAC in the Ethernet header.
Invalid IP	The number of ARP packets that were dropped by DAI because the sender IP address in the ARP packet, or the target IP address in the ARP reply packet, is invalid. Invalid addresses include 0.0.0.0, 255.255.255.255, IP multicast addresses, class E addresses (240.0.0.0/4), and loopback addresses (127.0.0.0/8).
Forwarded	The number of valid ARP packets forwarded by DAI.
Dropped	The number of invalid ARP packets dropped by DAI.

Timer Schedule

The NETGEAR Smart Switch provides timer schedules for use with PoE/PoE+.

To use Timer Schedules with PoE/PoE+, you first define a timer schedule on the **System > Timer Schedule** screen. Then you associate the timer schedule to a PoE/PoE+ port (or ports) on the **System > PoE > PoE Port Configuration** screen. See <u>PoE on page 86</u>**.**

- <u>Define a Timer Schedule Name on page 127</u>
- <u>Configure Timer Schedule on page 128</u>

Define a Timer Schedule Name

Use this screen to add or delete the name of a timer schedule.

To add a timer schedule name:

1. **Select System > Timer Schedule > Basic > Global Configuration**.

   You can also select **System** > **Timer Schedule** > **Advanced > Global Configuration**.

2. The **Timer Schedule** screen displays.

3. Specify the name of a timer schedule in the **Timer Schedule Name** field.

4. Click the **Add** button. The new timer schedule, with the name you specified, is added. Configuration changes take effect immediately.
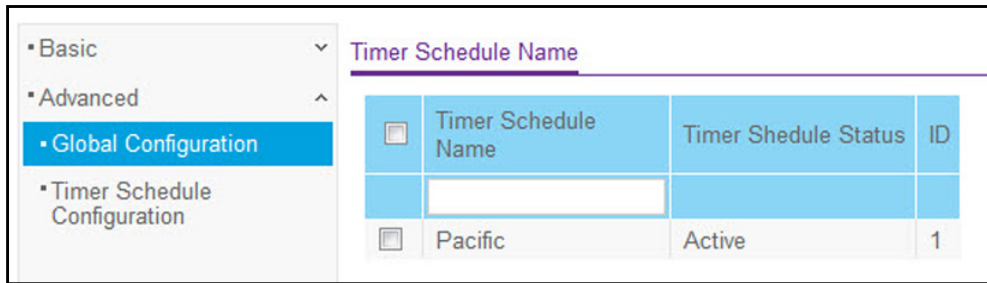
Figure 80. Timer Schedule Name

To delete a timer schedule name:

1. **Select System > Timer Schedule > Basic > Global Configuration.**

    You can also select **System** > **Timer Schedule** > **Advanced > Global Configuration.**

2. The **Timer Schedule** screen displays.

3. In the **Timer Schedule Name** field, type the name of the timer schedule to be deleted.

4. Click the **Delete** button. The timer schedule with the name you specified is deleted. Configuration changes take effect immediately.

The following table describes the non-configurable fields on the Timer Schedule Global Configuration page.

Table 45. Timer Schedule Information

Field	Description
Time Schedule Status	Specifies if the current status of the timer schedule is active or inactive.
ID	Identifies the timer schedule. The maximum number of timer schedules that can be created is 100.

Configure Timer Schedule

Use this screen to configure timer schedule.

To select the timer schedule criteria:

1. **Select System > Timer Schedule > Advanced > Time Schedule Configuration**.

2. Select the **Timer Schedule Name** to be configured.

3. Select the **Timer Schedule Type** of entry to be configured. The choices are **Absolute** or **Periodic**. The factory default is **Absolute.**

4. Select the number of the **Timer Schedule Entry** to be configured or added. Select the option **New** to add a new entry.

Figure 81. Timer Schedule Criteria

To configure the timer schedule:

1. Enter the **Time Start**. This is the time of day in hh:mm format when the schedule operation is started. This field is required.

2. Enter the **Time End**. This is the time of day in hh:mm format when the schedule operation is stopped. This field is required.

3. Enter the **Date Start**. This is the schedule start date. This field is required.

4. Enter the **Date End**. This is the schedule end date. If **No End Date** is selected, the schedule operates indefinitely.

5. Select the **Recurrence Pattern**. This field is displayed only when you select **Periodic** as the **Timer Schedule Type**. Select the recurrence period that the event will repeat. If recurrence is not needed (a timer schedule should be triggered just once), then set the **Date End** as equal to **Date Start** or leave the **Daily Mode-Every** field empty. The possible values of recurrence are:

   • **Daily**. The timer schedule works with daily recurrence.

   • **Daily Mode**. **Every WeekDay** means that the schedule will be triggered every day from Monday to Friday. The field **Every Day(s)** means that the schedule will be triggered every defined number of days. If number of days is not specified, then the schedule will be triggered only once. The possible value of every day(s) is from 0 to 255.

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

   • **Every Week**. Define the number of weeks when the schedule will be triggered. The field **Every Week(s)** means that the schedule will be triggered every defined number of weeks. If **Every Week(s)** is not specified, then the schedule will be triggered only once. The possible value of every week(s) is from 0 to 255.

   • **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 will be triggered. The field **Every Month(s)** means that the schedule will be triggered every defined number of months. If **Every Month(s)** is not specified, then the schedule will be triggered only once. The possible value of every month(s) is from 0 to 255.

6. Click the **Add** button to add a new absolute or periodic timer schedule entry to the selected timer schedule. Configuration changes take effect immediately.

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

8. Click the **Cancel** button to cancel the configuration on the screen. The system resets the data on the screen to the latest value.

9. Click the **Delete** button to delete the selected entry from the timer schedule. Configuration changes take effect immediately.

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

3

Configuring Switching

Use the features you access from the Switching tab to define Layer 2 features. The Switching tab contains links to the features described in the following sections.

Ports

The screens you access from the Ports menu allow you to view and monitor the physical port information for the ports available on the switch. The Ports menu contains links described in the following sections.

- Port Configuration

Port Configuration

Use the Port Configuration screen to configure various characteristics about the physical ports or LAGs on the switch.

To configure port settings:

1. Select **Switching** > **Ports** > **Port Configuration**.

Figure 82. Port Configuration

2. Select one or more ports or LAGs to configure.

   For information about how to select and configure one or more ports and LAGs, see Configuring Interface Settings on page 28.

3. Configure or view the settings:

   - **Description**. Enter the description string to be attached to a port. The string can be up to 64 characters in length.

   - **Admin Mode**. Select the port control administration state, which can be one of the following:

     - **Enable**. You must select enable if you want the port to participate in the network. The default is enable.

     - **Disable**. The port is administratively down and does not participate in the network.

   - Auto-negotiation. Select to enable or disable auto-negotiation mode for this port.

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

   - **Speed**. Select the port's speed. Possible values are:

     - **Auto**. All supported speeds. If you select Auto, the duplex mode and speed will be set by the auto-negotiation process. The port's maximum capability (full duplex

and 1000 Mbps) will be advertised. Otherwise, your selection will determine the port's duplex mode and transmission rate. The factory default is Auto.

- **10**. 10 Mbits/sec.
- **100**. 100 Mbits/sec.
- **10G**. 10 Gbits/sec.

The delimiter characters for setting different speed values is ',', '.' and space. You must set Auto-negotiation mode to Enable in order for you to be able to set the auto-negotiation speeds.

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

- **Duplex Mode**. Specify the duplex mode for this port. Possible values are:
  - **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.
  - **Auto**. Set by auto-negotiation process.

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

- **Link Trap**. Select whether or not to send a trap when link status changes. The factory default is enabled for normal interfaces and disabled for LAG interfaces. Possible values are:
  - **Enable**. Specifies that the system sends a trap when the link status changes.
  - **Disable**. Specifies that the system does not send a trap when the link status changes.
- **Maximum Frame Size**. Specify the maximum Ethernet frame size the interface supports. Valid values are 1500 to 9198. The default value is 1500. The size includes the Ethernet header, CRC, and payload. Any change to the maximum frame size is immediately applied to all interfaces.
- **Flow Control**. Specify the IEEE 802.3x flow control mode for this port from the following options:
  - **Disable** flow control. Flow control helps to prevent data loss when the port cannot keep up with the amount of frames being switched. When enabled, the switch can send a PAUSE frame to stop traffic on a port if the amount of memory used by packets on the port exceeds a preconfigured threshold, and will respond to pause requests from partner devices. The paused port does not forward packets for the period of time specified in the PAUSE frame. When the PAUSE frame time elapses, or the utilization returns to a specified low threshold, the switch enables the port to again transmit frames. The factory default is **Disabled**. When flow control is disabled, the switch does not generate PAUSE frames. The switch also does not throttle packet transmission on receiving PAUSE frames from a partner.

For LAG interfaces Flow Control Mode is displayed as *blank* because flow control is not applicable.

- **Symmetric**.The port or device can send as well as honor the PAUSE frames. The port or device generates PAUSE frames towards the peer in response to congestion at ingress. The port or device is also capable of throttling the transmit rate in response to the PAUSE frames received from the peer.

- **Asymmetric**.The port or device can honor the received PAUSE frames, but the port or device cannot generate PAUSE frames towards peer in response to congestion at ingress. The port or device is capable of throttling the transmit rate in response to the pause frames received from peer.

4. Click the **Apply** button.

The following table shows the non-configurable information on the Port Configuration screen.

Table 46. Switching Ports Port Configuration

Field	Description
Port Type	For most ports this field is blank. Otherwise, the possible values are: • **Trunk Member**. The port is a member of a Link Aggregation trunk. • **Mirrored**. The port is a mirrored port. • **Probe**. The port is a monitoring port.
Physical Status	Indicates the physical port's speed and duplex mode
Link Status	Indicates whether the link is up or down.
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 ifIndex of the interface table entry associated with this port. If the interface field is set to All, this field is blank.

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 default management VLAN (that is, VLAN 1).

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 LAGPDUs. The switch supports 26 LAGs.

The LAGs menu contains the links described in the following sections.

-
-
-
-

LAG Configuration

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

To configure LAG settings:

1. Select **Switching** > **LAG** > **Basic** > **LAG Configuration**.

LAG Name	Description	LAG ID	Admin Mode	Hash Mode	STP Mode	Link Trap	LAG Type	Active Ports	LAG State	Local Preference Mode
			v		v	v	v			v
ch1		l1	Enabled	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Static		Link Down	Disable
ch2		l2	Enabled	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Static		Link Down	Disable
ch3		l3	Enabled	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Enable	Static		Link Down	Disable

Figure 83. Basic LAG Configuration

2. Select the check box next to the LAG to configure.

    You can select multiple LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

3. Configure or view the following settings:

Note: Click current members in the list to see existing member ports in that LAG.

- **LAG Name**. Specify the name you want assigned to the LAG. You can enter any string of up to 15 alphanumeric characters. A valid name has to be specified in order to create the LAG

- **Description**. Specify the description string to be attached to a LAG. It can be up to 64 characters in length.

- **Admin Mode**. Select Enable or Disable from the list. When the LAG (port channel) is disabled, no traffic will flow and LAGPDUs will be dropped, but the links that form the LAG (port channel) will not be released. Disabled indicates that interface was set in diagnostic disabled state by the Auto Recovery feature. The factory default is Enable.

- **Hash Mode**. This Mode selects the load-balancing mode used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a

binary pattern from selected fields in a packet, and associating that pattern with a particular link.

- **Src MAC,VLAN,EType,incoming port**. Source MAC, VLAN, EtherType, and incoming port associated with the packet.

- **Dest MAC,VLAN,EType,incoming port**. Destination MAC, VLAN, EtherType, and incoming port associated with the packet.

- **Src/Dest MAC,VLAN,EType,incoming port**. Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.

- **Src IP and Src TCP/UDP Port Fields**. Source IP and Source TCP/UDP fields of the packet.

- **Dest IP and Dest TCP/UDP Port Fields**. Destination IP and Destination TCP/UDP Port fields of the packet.

- **Src/Dest IP and TCP/UDP Port Fields**. Source/Destination IP and source/destination TCP/UDP Port fields of the packet.

- **Enhanced hashing mode**. Dynamic selections of fields based on packet flow. For L2 packets Source and Destination MAC address, for IP packets, Source IP, Destination IP address, TCP/UDP ports are used.

• **STP Mode**. Select the Spanning Tree Protocol administrative mode associated with the LAG.

• **Link Trap**. Specify whether you want to have a trap sent when link status changes. The factory default is Disable, which will cause the trap to be sent.

• **LAG Type**. Specify whether the LAG is configured as a static or LACP port.

- **Static**. Disables Link Aggregation Control Protocol (LACP). The port does not transmit or process received LAGPDUs, for example the member ports do not transmit LAGPDUs and all the LAGPDUs it can receive are dropped. The LAG is configured manually. The default is Static.

- **LACP**. Enables Link Aggregation Control Protocol (LACP) on the selected LAG. The LAG is configured automatically.

• **Local Preference Mode**. Enable or disable the LAG interface's Local Preference mode. Local preference is one of the properties of a LAG interface which is intended for a Stacking environment. This is useful when the LAG is formed with ports from across the units. In such a scenario, when this feature is enabled, any known unicast traffic sent to the LAG uses only the LAG interface on the local unit. This ensures that the known unicast traffic, destined to the LAG, does not cross the external stack link when the LAG has a member or members on the local unit. Local preference does not impact behavior with respect to unknown unicast, broadcast and multicast traffic.

4. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

The following table shows the non-configurable information on the screen.

Table 47. Basic LAG Configuration

Field	Description
LAG ID	The number assigned to the LAG. This field is read-only.
Active Ports	A listing of the ports that are actively participating members of this port channel. A maximum of 8 ports can be assigned to a port channel.
LAG State	Indicates whether the link is Up or Down.

LAG Membership

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

To add members to a LAG:

1. Select **Switching** > **LAG** > **Basic** > **LAG Membership**.
2. From the LAG ID list, select the LAG to configure.
3. (Optionally) In the LAG Name field, enter the name you want assigned to the LAG.

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

4. In the Port Selection Table, click the box below each port to include in the LAG.

   A check mark in the box below the port indicates that the port is a member of the LAG. In the following figure, ports 11–14 are members of LAG 1.
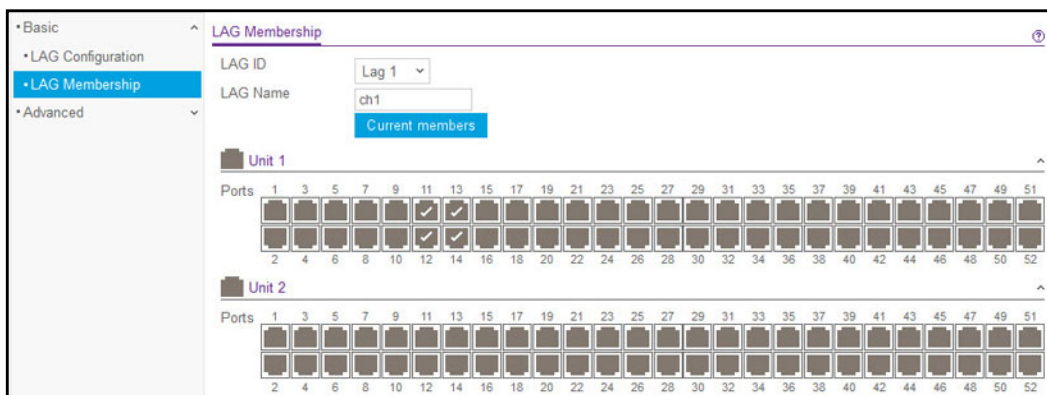
Figure 84. LAG Membership

5. Click the **Apply** button.
6. To verify the configuration and view the ports that are members of the selected LAG, click **Current Members**. This action opens a new window with a list of current members.

LACP Configuration

The LACP configuration screen is used to set the LACP system priority.

To configure LACP:

1. Select **Switching** > **LAG** > **Advanced** > **LACP Configuration**.
2. In the LACP System Priority field, specify the device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled.

   A higher value indicates a lower priority. You can change the value of the parameter globally by specifying a priority from 1–65535. The default value is 32768.
3. Click the **Apply** button.

LACP Port Configuration

The LACP port configuration screen is used to configure the LACP priority value for the selected port and the administrative LACP time-out value.

To configure LACP port priority settings:

1. Select **Switching** > **LAG** > **Advanced** > **LACP Port Configuration**.
2. Select the ports to configure:

   For information about how to select and configure one or more ports and LAGs, see Configuring Interface Settings on page 28.
3. Configure the LACP Priority value for the selected port(s).

   This value specifies the device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. A higher value indicates a lower priority.
4. Configure the administrative LACP time-out value.
   - **Long**. Specifies a long time-out value.
   - **Short**. Specifies a short time-out value.
5. Click the **Apply** button.

VLANs

Adding virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security, and management of multicast traffic.

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

Each VLAN in a network has an associated VLAN ID, which displays 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.

For more information about configuring VLANs, see Virtual Local Area Network Configuration Example on page 319.

The VLAN menu contains links described in the following sections.

- Basic VLAN Configuration on page 140
- VLAN Membership Configuration on page 140
- VLAN Status on page 142
- Port VLAN ID Configuration on page 142
- MAC-Based VLAN on page 143
- Protocol-Based VLAN Group Configuration on page 144
- Protocol-Based VLAN Group Membership on page 145
- Voice VLAN on page 145
- GARP Switch Configuration on page 146
- GARP Port Configuration on page 147

Basic VLAN Configuration

Use the VLAN Configuration screen to define VLAN groups stored in the VLAN membership table. The switch supports up to 256 VLANs. The default VLAN (1), voice VLAN (2) and auto-video VLAN (3) are created by default, and all ports are untagged members. When you create a VLAN on this screen, its type is always static.

To add a VLAN:

1. Select **Switching** > **VLAN** > **Basic** > **VLAN Configuration**.
2. In the VLAN ID field, specify the VLAN identifier for the new VLAN.
3. (Optionally) In the VLAN Name field, specify a name to help identify the VLAN.
4. Click the **Add** button.

To delete one or more VLANs:

1. Select the check box next to each VLAN to delete.

    Note: You cannot delete VLANs 1 or 4089 which are created by default.

2. Click the **Delete** button.

To modify the VLAN name:

1. Select the check box next to the VLAN to modify.
2. In the VLAN Name field, specify the new name.
3. Click the **Apply** button.

To reset the VLAN settings on the switch to the factory defaults:

1. Select the **Reset Configuration** check box.
2. Click the **OK** button in the pop-up message to confirm the action.

    If the Management VLAN is set to a non-default VLAN (VLAN 1), it is automatically set to 1 after the VLAN configuration is reset.

VLAN Membership Configuration

Use this screen to configure VLAN port membership for a particular VLAN. You can select the Group operation through this screen.

To configure VLAN membership for individual ports and LAGs:

1. Select **Switching** > **VLAN** > **Advanced** > **VLAN Membership**.
2. From the VLAN ID list, select the VLAN to which you want to add ports.

3. Click the Unit number icon below the VLAN Type field to display the physical ports on the switch.

4. Click the Unit number icon to display the LAGs on the switch.

5. To select the ports or LAGs to add to the VLAN, click the square below each port or LAG.

   You can add each interface as a tagged (T) or untagged (U) VLAN member. A blank square means that the port is not a member of the VLAN.

   - **Tagged**. Frames transmitted from this port are tagged with the port VLAN ID.
   - **Untagged**. Frames transmitted from this port are untagged. Each port can be an untagged member of only one VLAN. By default, all ports are an untagged member of VLAN 1.

   In the following figure, ports 8, 10, and 12 and LAG 1 are being added as tagged members to VLAN 1.

Figure 85. VLAN Membership

6. Click the **Apply** button.

To configure the same VLAN membership settings for all ports and LAGs:

1. Select **Switching** > **VLAN** > **Advanced** > **VLAN Membership**.

2. In the VLAN ID list, select the VLAN to which you want to add ports.

3. In the Group Operations list, select one of the following options:

   - **Untag All**. All frames transmitted from this VLAN will be untagged. All the ports will be included in the VLAN.

- **Tag All**. All frames transmitted for this VLAN will be tagged. All the ports will be included in the VLAN.
- **Remove All**. Excluding all ports from the selected VLAN.

4. Click the **Apply** button.

VLAN Status

This VLAN Status screen displays the status of all currently configured VLANs.

To view the current VLAN status:

1. Select **Switching** > **VLAN** > **Advanced** > **VLAN Status**.
2. View the following VLAN status information:
   - **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 an administrator has configured.
     - **Dynamic**. The VLAN that is created by GVRP registration initially has a type of Dynamic (GVRP).

       The type of AUTO VoIP VLAN is Dynamic (AUTO VoIP). The VLAN that is created by MVRP registration initially has type of Dynamic (MVRP). The VLAN that is created by DOT1x registration has a type of Dynamic (DOT1X). The type of Auto Video VLAN is Auto-Video.
   - **Routing Interface**. The routing interface.
   - **Member Ports**. The ports that are included in the VLAN.

Port VLAN ID Configuration

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

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

To configure PVID information:

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

2. Select the interfaces for which you want to configure the PVID settings:

   For information about how to select and configure one or more ports and LAGs, see
   Configuring Interface Settings on page 28.

3. In the Configured PVID field, specify the PVID to assign to untagged or priority tagged
   frames received on the selected interfaces.

4. (Optionally) Use the VLAN Member and VLAN Tag fields to change the VLAN membership
   and tagging for the selected interfaces.

   The VLAN membership and tagging information can also be configured by using the
   VLAN Membership screen.

5. From the Acceptable Frame Types list, specify how you want the selected interfaces to
   handle untagged and priority tagged frames.

   Whichever you select, VLAN tagged frames will be forwarded in accordance with the
   IEEE 802.1Q VLAN standard. The factory default is Admit All.

   • **VLAN Only**. The port will discard any untagged or priority tagged frames it receives.

   • **Admit All**. Untagged and priority tagged frames received on the port will be accepted
     and assigned the value of the port VLAN ID for this port.

6. From the Configured Ingress Filtering list, specify how you want the port to handle tagged
   frames.

   • **Enable**. A tagged frame is discarded if this interface is not a member of the VLAN
     identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the port VLAN
     ID specified for the port that received this frame.

   • **Disable**. all frames are forwarded in accordance with the 802.1Q VLAN bridge
     specification. The factory default is disabled.

7. Specify the default 802.1p priority assigned to untagged packets arriving at the port.

   Possible values are 0–7.

8. Click the **Apply** button.

MAC-Based VLAN

The MAC Based VLAN feature uses the source MAC address of incoming untagged packets
to classify the traffic and to assign the packets to the appropriate VLAN.

A MAC to VLAN mapping is defined by configuring an entry in the MAC to VLAN table. An
entry is specified by 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
that has MAC address to VLAN ID mappings).

When untagged or priority tagged packets arrive at the switch and entries exist in the MAC to
VLAN table, the source MAC address of the packet is looked up. If an entry is found, the
corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged it
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 you are allowed to configure a MAC address mapping to a VLAN that has not been created on the system.

To configure a MAC based VLAN:

1. Select **Switching** > **VLAN** > **Advanced** > **MAC Based VLAN**.

2. In the MAC Address field, specify the source MAC address of the host to be bound to a VLAN ID.

   All untagged traffic that includes this address in the source MAC address field of the Ethernet frame is placed in the associated VLAN.

3. Enter the VLAN ID of the MAC-based VLAN.

   If an untagged frame received on any port or LAG matches the associated MAC address, it is tagged with this VLAN ID.

4. Click the **Add** button.

Protocol-Based VLAN Group Configuration

Protocol-based VLAN can be used to define filtering criteria for untagged packets. By default, if you do not configure any port (IEEE 802.1Q) or protocol-based VLANs, untagged packets 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 have specifically assigned to the port using the Port VLAN Configuration screen.

You define a protocol-based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple ports. When you create a group, you choose a name, and a group ID is assigned automatically.

To configure a protocol-based VLAN group:

1. Select **Switching** > **VLAN** > **Advanced** > **Protocol-Based VLAN Group Configuration**.

2. In the Group ID field, specify a unique number used to identify the group.

3. In the Group Name field, specify a name to identify the group.

   You can enter up to 16 characters.

4. In the Protocol field, specify the protocol or protocols to use as the match criteria to determine whether a particular packet belongs to the protocol-based VLAN.

   The protocols you specify are checked against the 2-byte EtherType field of ingress Ethernet frames on the PVBLAN group interfaces. When adding a protocol, you can specify the EtherType hex value or (for IP, ARP, and IPX) the protocol keyword.

5. In the VLAN ID field, specify the VLAN ID to associate with the protocol-based VLAN.

   All the ports in the group will assign this VLAN ID to untagged packets received for the protocols you included in this group.

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

6. Click the **Add** button.

To modify protocol-based VLAN information:

1. Select the check box next to the protocol-based VLAN to update.
2. Specify the desired value in the available fields.
3. Click the **Apply** button.

To delete a protocol-based VLAN group:

1. Select the check box next to each protocol-based VLAN to remove.
2. Click the **Delete** button.

Protocol-Based VLAN Group Membership

The Protocol-Based VLAN Group Membership screen is used to define a protocol-based VLAN group.

To set up protocol-based VLAN group membership:

1. Select **Switching** > **VLAN** > **Advanced** > **Protocol-Based VLAN Group Membership**.
2. From the Group ID list, select the protocol-based VLAN group ID for which you want to display or configure data.
3. Click display the port list.

   Use this port list to add ports to this protocol-based VLAN group.

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

4. In the Group Name field, enter the name for the protocol-based VLAN you selected.
5. Click the **Apply** button.
6. Click **Current Members** button to view the current members of the selected protocol-based VLAN group.

Voice VLAN

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

To configure the voice VLAN:

1. Select **Switching** > **VLAN** > **Advanced** > **Voice VLAN Configuration.**

2. Next to **Admin Mode, globally enable** the administrative mode for Voice VLAN on the switch.

3. Select the ports to configure:

   For information about how to select and configure one or more ports, see <u>Configuring Interface Settings on page 28</u>.

4. From the Interface Mode list, select one of the following options to determine how an IP phone connected to the selected port should send voice traffic:

   - **VLAN ID**. Forward voice traffic in the specified voice VLAN.

   - **Dot1p**. Tag voice traffic with the specified 802.1p priority value.

   - **None**. Use the settings configured on the IP phone to send untagged voice traffic.

   - **Untagged**. Send untagged voice traffic.

   - **Disable**. Operationally disables the voice VLAN feature on the interface.

5. If the interface mode is VLAN ID or Dot1p, specify the VLAN ID or 802.1p priority value in the Value field.

   This field is valid only when VLAN ID or dot1p is selected as the interface mode.

6. From the CoS Override Mode list, specify the CoS override mode for the selected ports:

   - **Enabled**. The port ignores the 802.1p priority value in the Ethernet frames it receives from connected devices.

   - **Disabled**. The port trusts the priority value in the received frame.

7. Click the **Apply** button**.**

GARP Switch Configuration

The Generic Attribute Registration Protocol (GARP) is used to exchange information between GARP participants to register and deregister attribute values within a bridged LAN. When a GARP participant declares or withdraws a given attribute, the attribute value is recorded with the applicant state machine for that attribute, for the port from which the declaration or withdrawal was made.

- Registration occurs only on ports that receive the GARP PDU containing a declaration or withdrawal.

- Deregistration occurs only if all GARP participants connected to the same LAN segment as the port withdraw the declaration.

GARP is part of the IEEE 802.1p extension to its 802.1D (spanning tree) specification. It includes:

- GARP Information Declaration (GID)—The part of GARP that generates data.

- GARP Information Propagation (GIP)—The part of GARP that distributes data.

To configure the GARP switch:

1. Select **Switching** > **VLAN** > **Advanced > GARP Switch Configuration**.

2. Choose the GARP VLAN Registration Protocol administrative mode for the switch by selecting **Enable** or **Disable** from the **GVRP Mode** radio button. The factory default is **Disable**.

3. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

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

---

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

GARP Port Configuration

To configure a GARP port:

1. Select **Switching** > **VLAN** > **Advanced > GARP Port Configuration**. The GARP Port Configuration table is displayed.

2. To navigate the page, select one of the following links. For more navigation information, see Configuring Interface Settings on page 28.

    *   To display all of the physical ports, click the **1** link.

    *   To display all LAGs, click the **LAGS** link.

    *   To display all ports and LAGs, click the **All** link.

    *   To select a single interface, type the port number, for example g4, in the **Go To Interface** field. Click the **Go** button.

3. Click a check box to select a physical interface for which data is to be displayed or configured.

4. Configure the **Port GVRP Mode**. Choose the GARP VLAN Registration Protocol administrative mode for the port by selecting **Enable** or **Disable** from the list. If you select **Disable**, the protocol will not be active and the **Join Time**, **Leave Time** and **Leave All Time** will have no effect. The factory default is **Disable**.

5. Configure the **Join Timer** (centiseconds). 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.

6. Configure the **Leave Timer** (centiseconds). Specify the time to wait in centiseconds, after receiving an unregister request for a VLAN or multicast group, before deleting the associated entry. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 20 and 600 (0.2

to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.

7. Configure the **Leave All Timer** (centiseconds). The Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5 x 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.

8. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

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

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

Auto-VoIP Configuration

Voice over Internet Protocol (VoIP) enables telephone calls over a data network. Because voice traffic is typically more time-sensitive than data traffic, the Auto VoIP feature helps provide a classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better Quality of Service (QoS). With the Auto VoIP feature, voice prioritization is provided based on call-control protocols (SIP, SCCP, H.323) or OUI bits.

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

- Configure Protocol-Based Auto VoIP Settings
- Configure OUI-Based Auto-VoIP
- Display Auto-VoIP Status

Configure Protocol-Based Auto VoIP Settings

To prioritize time-sensitive voice traffic over data traffic, protocol-based Auto VoIP checks for packets carrying the following VoIP protocols:

- Session Initiation Protocol (SIP)
- H.323
- Signalling Connection Control Part (SCCP)

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

To configure the protocol-based port settings:

1. Select **Switching** > **Auto-VoIP** > **Protocol-Based Port Settings**.

2. In the Prioritization Type list, select method used to prioritize VoIP traffic when a call-control protocol is detected, which is one of the following:

    •   **Remark**. Remark the voice traffic with the specified 802.1p priority value at the ingress interface.

    •   **Traffic Class.** Assign VoIP traffic to the specified traffic class when egressing the interface.

3. In the Class Value list, select the CoS tag value to be reassigned for packets received on the voice VLAN when Remark CoS is enabled.

4. Select the interface to configure.

    For information about how to select and configure one or more ports, see Configuring Interface Settings on page 28.

5. In the Auto VoIP Mode list, select **Enable** to enable Auto VoIP on the selected interfaces.

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

6. Click the **Apply** button.

Configure OUI-Based Auto-VoIP

With Organizationally Unique Identifier (OUI)-based Auto VoIP, voice prioritization is provided based on OUI bits.

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

•   OUI-Based Properties on page 149
•   OUI-Based Port Settings on page 150
•   OUI-Based OUI Table on page 150

OUI-Based Properties

To configure OUI based properties:

1. Select **Switching** > **Auto-VoIP**> **OUI-based > Properties**.

2. In the VoIP VLAN ID list, select the VLAN to use to segregate VoIP traffic from other non-voice traffic.

    All VoIP traffic that matches a value in the known OUI list gets assigned to this VoIP VLAN.

3. In the OUI-based priority list, select the 802.1p priority value to use for traffic that matches a value in the known OUI list.

    If the Auto VoIP mode is enabled and the interface detects an OUI match, the device assigns the traffic in that session to the traffic class mapped to this priority value. Traffic classes with a higher value are generally used for time-sensitive traffic.

4. Click the **Apply** button.

OUI-Based Port Settings

The port settings screen allows you to configure the OUI port settings.

To configure OUI port settings:

1. Select **Switching** > **Auto-VoIP > OUI-based** > **Port Settings**.
2. Select the interfaces to configure.

    For information about how to select and configure one or more ports, see Configuring Interface Settings on page 28.

3. In the Auto VoIP Mode list, select **Enable** to enable Auto VoIP on the selected interfaces.

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

4. Click the **Apply** button.

OUI-Based OUI Table

Device hardware manufacturers can include an OUI in a network adapter to help identify a hardware device. The OUI is a unique 24-bit number assigned by the IEEE registration authority. The switch comes preconfigured with the following OUIs that identify the IP phone manufacturer:

- 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

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

To add a new OUI prefix:

1. Select **Switching** > **Auto-VoIP> OUI-based** > **OUI Table**.
2. In the Telephony OUI(s) field, specify the VOIP OUI prefix.

    The OUI prefix must be in the format AA:BB:CC.

3. In the Description field, type a description that identifies the manufacturer or vendor associated with the OUI.

   The maximum length of description is 32 characters.

4. Click the **Add** button.

   To delete one or more OUI prefixes from the table:

1. Select the check box next to each OUI prefix to remove.

2. Click the **Delete** button.

Display Auto-VoIP Status

Use this screen to display Auto-VoIP status.To display the screen, click **Switching > Auto-VoIP > Auto-VoIP Status**. A screen similar to the following is displayed.

Auto-VoIP Status	
Auto-VoIP VLAN ID	0
Maximum Number of Voice Channels Supported	288
Number of Voice Channels Detected	0

Figure 86. Auto-VoIP Status

The following table shows the non-configurable information displayed on the screen.

Table 48. Auto-VoIP Status

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

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

Spanning Tree Protocol

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

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information about configuring Common STP, see CST Port Configuration on page 155.

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 that 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 with both RSTP and STP. An MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge.

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

The Spanning Tree menu contains the links described in the following sections.

- STP Configuration
- CST Configuration
- CST Port Configuration
- CST Port Status
- Rapid STP
- MST Configuration
- MST Port Configuration
- STP Statistics

STP Configuration

The STP Configuration screen contains fields for enabling STP on the switch.

To configure STP settings on the switch:

1. Select **Switching** > **STP** > **Basic** > **STP Configuration**.
2. Next to Spanning Tree State, specify whether to enable or disable Spanning Tree operation on the switch.
3. From the STP Operation Mode field, specify the Force Protocol Version parameter for the switch.

   Options are:

   - **STP** (Spanning Tree Protocol). IEEE 802.1D
   - **RSTP** (Rapid Spanning Tree Protocol). IEEE 802.1w
   - **MSTP** (Multiple Spanning Tree Protocol). IEEE 802.1s

4. Specify the configuration name and revision level.
   - **Configuration Name**. Name used to identify the configuration currently being used. It can be up to 32 alphanumeric characters.
   - **Configuration Revision Level**. Number used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0.

5. Next to Forward BPDU while STP Disabled, select **Enable** to allow spanning tree BPDUs to be forwarded while spanning-tree is disabled on the switch, or select **Disable** to prevent BPDUs from being forwarded when STP is disabled on the switch.
6. Click the **Apply** button.

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

Table 49. STP status information

Field	Description
Configuration Digest Key	This is used to identify the configuration currently being used.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time in seconds since the topology of the CST last changed.
Topology Change Count	The number of times the topology has changed for the CST.
Topology Change	The value of the topology change parameter for the switch indicating if a topology change is in progress on any port assigned to the CST. The value is either True or False.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Path cost to the Designated Root for the CST.
Root Port	Port to access the Designated Root for the CST.

Table 49. STP status information (continued)

Field	Description
Max Age (secs)	Specifies the bridge maximum age for CST. The value must be less than or equal to (2 X Bridge Forward Delay) – 1 and greater than or equal to 2 X (Bridge Hello Time +1).
Forward Delay (secs)	Derived value of the Root Port Bridge Forward Delay parameter.
Hold TIme (secs)	Minimum time between transmission of Configuration BPDUs.
CST Regional Root	Priority and base MAC address of the CST regional root.
CST Path Cost	Path Cost to the CST tree regional root.

CST Configuration

Use the CST Configuration screen to configure Common Spanning Tree (CST) and Internal Spanning Tree on the switch.

To configure CST settings:

1. Select **Switching** > **STP** > **Advanced** > **CST Configuration**.

2. Specify values for CST in the appropriate fields:

    *   **Bridge Priority**. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. Specifies the bridge priority value for the Common and Internal Spanning Tree (CST). The valid range is 0–61440. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. The default priority is 32768.

    *   **Bridge Max Age (secs)**. Specify 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)**. Specify the switch Hello time for the Common and Internal Spanning Tree (CST), which indicates the amount of time in seconds a root bridge waits between configuration messages. The value is fixed at 2 seconds.

    *   **Bridge Forward Delay (secs)**. Specify the switch forward delay time, which indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The value must be greater or equal to (Bridge Max Age / 2) + 1. The time range is from 4 seconds to 30 seconds. The default value is 15.

    *   **Spanning Tree Maximum Hops**. Specify the maximum number of bridge hops the information for a particular CST instance can travel before being discarded. The valid range is 6–40

3. Click the **Apply** button**.**

The following MSTP status information is displayed on the Spanning Tree CST Configuration screen.

Table 50. MSTP status information

Field	Description
MST ID	Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID	Table consisting of the VLAN IDs and the corresponding FID associated with each of them
FID	Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

CST Port Configuration

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

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

To display the CST Port Configuration screen, click **Switching** > **STP** > **Advanced** > **CST Port Configuration**. A screen similar to the following is displayed.

Figure 87. CST Port Configuration

To configure CST port settings:

1. To configure CST settings for a physical port, enter the interface and click the **Go** button to select that particular interface.

2. Select the interfaces for which you want to configure the CST settings.

    For information about how to select and configure one or more ports or LAGs, see Configuring Interface Settings on page 28.

3. Configure the CST values for the selected port(s) or LAG(s):

- **STP Status**. Enable or disable the Spanning Tree Protocol Administrative Mode associated with the port or port channel.

- **Fast Link**. Specifies if the specified port is an Edge Port with the CST. Possible values are Enable or Disable. The default is Disable.

- **BPDU Forwarding**. Specifies whether spanning tree BPDUs should be forwarded while spanning-tree is disabled on the switch. The value is enabled or disabled.

- **Auto Edge**. Configure the auto edge mode of a port by selecting to enable or disable allowing the port to become an edge port if it does not see BPDUs for some duration.

- **Path Cost**. Set the Path Cost to a new value for the specified port in the common and internal spanning tree. It takes a value in the range of 0–200000000.

- **Priority**. The priority for a particular port within the CST. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the priority is automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16. Priority range is 0-240. The default value is 128.

- **External Port Path Cost**. Set the External Path Cost to a new value for the specified port in the spanning tree. It takes a value in the range of 0–200000000.

4. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

Table 51, Advanced CST Port Configuration describes the non-configurable fields.

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

Table 51. Advanced CST Port Configuration

Field	Description
Port State	The Forwarding state of this port. The default is disabled.
Port ID	The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
Hello Timer	Specifies the switch Hello time, which indicates the amount of time in seconds a port waits between configuration messages. The default is 2 seconds.

CST Port Status

Use the Spanning Tree CST Port Status screen to display Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

To display the Spanning Tree CST Port Status screen, click **Switching** > **STP** > **Advanced** > **CST Port Status**.

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

Table 52. CST port status information

Field	Description
Interface	The port associated with the VLAN(s) associated with the CST.
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
Designated Root	Root Bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	Bridge Identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Topology Change Acknowledge	Identifies whether the next BPDU to be transmitted for this port would have the topology change acknowledgement flag set. It is either *True* or *False*.
Edge Port	Indicates whether the port is enabled as an edge port. Possible values are Enabled or Disabled.
Point-to-point MAC	Derived value of the point-to-point status.
CST Regional Root	The bridge priority and base MAC address of the CST regional root.
CST Path Cost	The path cost to the CST tree regional root.
Port Forwarding State	The forwarding state of this port.

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

Rapid STP

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

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

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

Table 53. Rapid STP status information

Field	Description
Interface	The physical or port channel interfaces associated with VLANs associated with the CST.
Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.

Table 53. Rapid STP status information (continued)

Field	Description
Mode	Specifies the spanning tree operation mode. Different modes are STP, RSTP, and MSTP.
Fast Link	Indicates whether the port is enabled as an edge port.
Status	The Forwarding State of this port.

MST Configuration

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

To configure an MST instance:

1. Select **Switching** > **STP** > **Advanced** > **MST Configuration**.
2. Configure the MST values:
   - **MST ID**. Specify the ID of the MST to create. Valid values for this are between 1 and 4094.
   - **Priority**. Specifies the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. The default priority is 32768.The valid range is 0–61440.
   - **VLAN ID**. The menu contains all VLANs configured on the switch. Select a VLAN to associate with the MST instance.
3. Click the **Add** button.

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

Table 54. MST instance information

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 total amount of time since the topology of the selected MST instance last changed. The time is displayed in hour/minute/second format, for example, 5 hours, 10 minutes, and 4 seconds.
Topology Change Count	The total number of times topology has changed for the selected MST instance.
Topology Change	Indicates whether a topology change is in progress on any port assigned to the selected MST instance. The possible values are True or False.

Table 54. MST instance information (continued)

Field	Description
Designated Root	The bridge identifier of the root bridge, which is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	The path cost to the Designated Root for this MST instance.
Root Port	Indicates the port to access the Designated Root for this MST instance.

To delete an MST instance:

1. Select the check box next to the instance.

2. Click the **Delete** button.

MST Port Configuration

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

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

To configure MST port settings:

1. Select **Switching** > **STP** > **Advanced** > **MST Port Configuration**.

   Note: If no MST instances have been configured on the switch, the screen displays a "No MSTs Available" message.

2. Select the ports or LAGs to configure.

   For information about how to select and configure one or more ports or LAGs, see .

3. Configure the MST values for the selected port(s) or LAG(s):

   • **Port Priority**. The priority for a particular port within the selected MST instance. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the priority is automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16. It takes a value in the range of 0–240.

   • **Port Path Cost**. Set the Path Cost to a new value for the specified port in the selected MST instance. It takes a value in the range of 0–200000000.

4. Click the **Apply** button.

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

Table 55. MST port status information

Field	Description
Auto-calculated Port Path Cost	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
Port ID	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Up Time Since Counters Last Cleared	Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.
Port Mode	Spanning Tree Protocol Administrative Mode associated with the port or port channel. Possible values are Enable or Disable.
Port Forwarding State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are: • Disabled. STP is currently disabled on the port. The port forwards traffic while learning MAC addresses. • Blocking. The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. • Listening. The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses. • Learning. The port is currently in the learning mode. The port cannot forward traffic, however, it can learn new MAC addresses. • Forwarding. The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses
Port Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
Designated Root	Root Bridge for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

STP Statistics

Use the Spanning Tree Statistics screen to view information about the number and type of bridge protocol data units (BPDUs) transmitted and received on each port.

To display the Spanning Tree Statistics screen, select **Switching** > **STP** > **Advanced** > **STP Statistics**.

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

Table 56. STP statistics

Field	Description
Interface	The physical or port channel interface to view its statistics.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.

Multicast

Multicast IP traffic is traffic that is destined to a host group. Host groups for IPv4 multicast are identified by class D addresses, which range from 224.0.0.0 to 239.255.255.255. Host groups for IPv6 multicast are identified by the prefix ff00::/8.

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

- MFDB Table
- MFDB Statistics
- Auto-Video
- IGMP Snooping
- IGMP Snooping Querier
- MLD Snooping

MFDB Table

The Multicast Forwarding Database (MFDB) 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 search the MFDB table:

1. Select **Switching** > **Multicast** > **MFDB** > **MFDB Table**.
2. Next to Search By MAC Address, specify the MAC Address whose MFDB table entry you want to view.

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

3. Click the **Go** button.

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

The MFDB Table screen displays the information shown in the following table.

Table 57. MFDB table information

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.
Component	This is the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, Static Filtering and MLD Snooping.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
Interface	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:) for the selected address.
Forwarding Interfaces	The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

MFDB Statistics

This screen displays the MFDB statistics for the system.

To view the MFDB statistics:

Select **Switching** > **Multicast** > **MFDB** > **MFDB Statistics**.

The MFDB Statistics screen displays the information shown in the following table.

Table 58. MFDB statistics

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

Auto-Video

Use this screen to configure the Auto-Video parameters.

To configure Auto-Video:

1. Select **Switching** > **Multicast** > **Auto-Video**.
2. Select one of the following radio buttons:
   - Select the **Disable** radio button to globally disable Auto-Video administrative mode for the switch.
   - Select the **Enable** radio button to globally enable Auto-Video administrative mode for the switch.

   The Auto-Video VLAN field shows the number of Auto-configured IGMP snooping VLANs.

3. Click the **Apply** button.

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 has any interest in receiving the packet. While nodes rarely incur any processing overhead to filter packets addressed to unrequested group addresses, they are unable to transmit new packets onto the shared media for the period of time that the multicast packet is flooded. The problem of wasting bandwidth is even worse when the LAN segment is not shared, for example in full-duplex links.

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

IGMP Snooping Configuration

Use the IGMP Snooping Configuration screen to configure the parameters for IGMP snooping. These parameters are used to build forwarding lists for multicast traffic.

To configure IGMP snooping:

1. Select **Switching** > **Multicast** > **IGMP Snooping** > **IGMP Snooping Configuration**.
2. Enable or disable IGMP snooping on the switch:
   - **Enable**. The switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address.
   - **Disable**. The switch does not snoop IGMP packets.
3. Select whether to validate the IGMP IP header.
   - **Enable**. The switch checks the IP header of all IGMP messages for the Router Alert option. If the option is not present, the packet is dropped.
   - **Disable**. The IGMP IP header is not checked for Router Alert option.
4. Click the **Apply** button.

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

Table 59. IGMP snooping status and statistics

Field	Description
Multicast Control Frame Count	The number of multicast control frames that have been processed by the CPU.
Interfaces Enabled for IGMP Snooping	Lists the interfaces currently enabled for IGMP snooping. For information about how to enable interfaces for IGMP snooping, see IGMP Snooping Interface Configuration on page 165.
VLAN Ids Enabled For IGMP Snooping	Displays VLAN IDs enabled for IGMP snooping. For information about how to enable VLANs for IGMP snooping, see IGMP Snooping VLAN Configuration on page 166.
VLAN Ids Enabled For IGMP Snooping Querier	Displays VLAN IDs enabled for IGMP snooping querier.

IGMP Snooping Interface Configuration

Use the IGMP Snooping Interface Configuration screen to configure IGMP snooping settings on specific interfaces.

To configure IGMP snooping interface settings:

1. Select **Switching** > **Multicast** > **IGMP Snooping** > **IGMP Snooping Interface Configuration**.

2. Select the ports or LAGs to configure.

    For information about how to select and configure one or more ports or LAGs, see Configuring Interface Settings on page 28.

3. Configure the IGMP snooping values for the selected ports or LAGs:

    • **Admin Mode**. Select the interface mode for the selected interface for IGMP snooping for the switch from the menu. The default is Disable.

    • **Host Timeout**. Specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group. Enter a value between 2 and 3600 seconds. The default is 260 seconds.

    • **Max Response Time**. Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Host Timeout, in seconds. The default is 10 seconds.

    • **MRouter Timeout**. Specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite time-out; no expiration.

    • **Fast Leave Admin Mode**. Select the Fast Leave mode for a particular interface from the menu. The default is Disable.

4. Click the **Apply** button.

IGMP Snooping Table

Use the IGMP Snooping Table screen to view all of the entries in the Multicast Forwarding Database that were created for IGMP snooping.

To view the entries in the IGMP snooping table:

1. Select **Switching** > **Multicast** > **IGMP Snooping** > **IGMP Snooping Table**.

2. Next to Search By MAC Address, specify the MAC Address whose MFDB table entry you want to view.

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

The following table describes the information in the IGMP snooping table.

Table 60. IGMP snooping table information

Field	Description
MAC Address	A multicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example, 01:00:5e:45:67:89.
VLAN ID	A VLAN ID for which the switch has forwarding and filtering information.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured, and Network Assisted.
Interface	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address.

IGMP Snooping VLAN Configuration

Use the IGMP Snooping VLAN Configuration screen to configure IGMP snooping settings for VLANs on the system.

To configure IGMP snooping settings for VLANs:

1. Select **Switching** > **Multicast** > **IGMP Snooping** > **IGMP Snooping VLAN Configuration**.
2. Enter the VLAN ID in the appropriate field and configure the IGMP snooping values:
   - **Fast Leave Admin Mode**. Enable or disable the IGMP snooping Fast Leave Mode for the specified VLAN ID. Enabling fast-leave allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.
   - **Host Timeout**. Sets the value for group membership interval of IGMP snooping for the specified VLAN ID. The valid range is (Maximum Response Time + 1) to 3600 seconds.
   - **Maximum Response Time**. Sets the value for maximum response time of IGMP snooping for the specified VLAN ID. Valid range is 1 to 25. The configured value must be less than the Group Membership Interval. The default is 10 seconds.
   - **MRouter Timeout**. Enter the amount of time that a switch waits to receive a query on the VLAN before removing it from the list of VLANs with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds, which means there is no expiration.
   - **Query Mode**. Enable or disable the IGMP Querier Mode for the specified VLAN ID.

- **Query Interval**. Enter the value for IGMP Query Interval for the specified VLAN ID. The valid range is 1–1800 seconds. The default is 60 seconds.

3. Click the **Add** button.

To disable IGMP snooping on one or more VLANs:

1. Select the check box next to each VLAN ID on which IGMP snooping is to be disabled.
2. Click the **Delete** button.

Multicast Router Configuration

If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure an interface as a multicast router interface, which is an interface that faces a multicast router or IGMP querier and receives multicast traffic. Use this screen to manually configure an interface as a static multicast router interface. All IGMP packets snooped by the switch will be forwarded to the multicast router reachable from this interface. The configuration is not needed most of the time since the switch will automatically detect the presence of multicast router and forward IGMP packet accordingly. It is needed only when you want to make sure the multicast router always receives IGMP packets from the switch in a complex network.

To configure the multicast router mode for one or more interfaces:

1. Select **Switching > Multicast > IGMP Snooping > Multicast Router Configuration**.
2. Select each interface to configure.

   For information about how to select and configure one or more ports or LAGs, see Configuring Interface Settings on page 28.

3. Use the Multicast Router menu to enable or disable Multicast Router on the selected interfaces.
4. Click the **Apply** button.

Multicast Router VLAN Configuration

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

To configure a multicast routing VLAN:

1. Select **Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration**.
2. Select the Interface for which you want Multicast Router to be enabled or to be disabled.
3. Enter the VLAN ID for which the Multicast Router Mode is to be Enabled or Disabled.
4. Enable the VLAN ID for the multicast router.
5. Click the **Apply** button.

IGMP Snooping Querier

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

These screens enable you to configure and display information on IGMP snooping queriers on the network and, separately, on VLANs.

The IGMP Snooping Querier menu contains links described in the following sections.

- IGMP Snooping Querier Configuration
- IGMP Snooping Querier VLAN Configuration
- IGMP Snooping Querier VLAN Status

IGMP Snooping Querier Configuration

Use this screen to enable or disable the IGMP snooping querier feature, specify the IP address of the router to perform the querying, and configure the related parameters.

To configure IGMP snooping querier settings:

1. Select **Switching** > **Multicast** > **IGMP Snooping Querier** > **IGMP Snooping** > **Querier Configuration**.
2. Next to the Querier Admin Mode field, enable or disable the administrative mode for IGMP snooping querier.
3. In the Snooping Querier Address field, specify the IP address to be used as source address in periodic IGMP queries.

   This address is used when no address is configured on the VLAN on which the query is being sent.

4. In the IGMP Version field, specify the IGMP protocol version used in periodic IGMP queries.
5. In the Query Interval field, specify the time interval in seconds between periodic queries sent by the snooping querier.

   The Query Interval must be a value in the range of 1–1800 seconds. The default value is 60.

6. In the Querier Expiry Interval field, specify the time interval in seconds after which the last querier information is removed.

   The Querier Expiry Interval must be a value in the range of 60–300 seconds. The default value is 125.

7. Click the **Apply** button.

IGMP Snooping Querier VLAN Configuration

To create a new VLAN ID for IGMP snooping:

1. Select **Switching** > **Multicast** > **IGMP Snooping Querier** > **Querier VLAN Configuration**.
2. From the VLAN ID list, select New Entry and complete the following fields:
    *   **VLAN ID**. Specify 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.
3. Click the **Apply** button.

IGMP Snooping Querier VLAN Status

Use this screen to view the operational state and other information for IGMP snooping queriers for VLANs on the network.

To view operational information on IGMP snooping queriers:

Select **Switching** > **Multicast** > **IGMP Snooping Querier** > **Querier VLAN Status**.

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

Table 61. IGMP snooping querier VLAN status

Field	Description
VLAN ID	Specifies the VLAN ID on which the IGMP snooping querier is administratively enabled and for which VLAN exists in the VLAN database.
Operational State	Specifies the operational state of the IGMP snooping querier on a VLAN: • Querier. The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode. • Non-Querier. The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. • Disabled. The snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when IGMP snooping is not operational on the VLAN, when the querier address is not configured, or the network management address is not configured.
Operational Version	The IGMP protocol version of the operational querier.
Last Querier Address	The IP address of the last querier from which a query was snooped on the VLAN.

Table 61. IGMP snooping querier VLAN status (continued)

Field	Description
Last Querier Version	The IGMP protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	The maximum response time to be used in the queries that are sent by the snooping querier.

MLD Snooping

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

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

MLD Snooping Configuration

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

To configure MLD snooping:

1. Select **Switching** > **Multicast** > **MLD Snooping** > **MLD Snooping Configuration**.
2. From the MLD Snooping Admin Mode list, select **Enable** to enable the administrative mode for MLD snooping on the switch.
3. Click the **Apply** button.

The following table describes the MLD snooping status information the screen displays.

Table 62. MLD snooping status information

Field	Description
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.

Table 62. MLD snooping status information (continued)

Field	Description
Interfaces Enabled for MLD Snooping	A list of all the interfaces currently enabled for MLD snooping. For information about how to enable an interface for MLD snooping, see MLD Interface Configuration on page 171.
VLAN IDs Enabled For MLD Snooping	The VLANs enabled for MLD snooping. For information about how to enable a VLAN for MLD snooping, see MLD VLAN Configuration on page 172.

MLD Interface Configuration

For MLD snooping to be active on an interface, it must be enabled both globally and on the interface (physical or LAG).

To configure an interface for MLD snooping:

1. Select **Switching** > **Multicast** > **MLD Snooping** > **Interface Configuration**.

2. Select each interface to configure.

   For information about how to select and configure one or more ports or LAGs, see Configuring Interface Settings on page 28.

3. In the Admin Mode field, select the interface mode for the selected interface for MLD snooping for the switch.

   The default is disable.

4. In the Group Membership Interval (secs) field, specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group.

   The valid range is from (2 to 3600) seconds. The configured value must be greater than Max Response Time. The default is 260 seconds.

5. In the Max Response Time (secs) field, specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface.

   Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds. The default is 10 seconds. The configured value must be less than the Group Membership Interval.

6. In the Present Expiration Time (secs) field, specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached.

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

7. From the Fast Leave Admin Mode list, select the Fast Leave mode for a particular interface from the menu.

   The default is Disable.

8. Click the **Apply** button.

MLD VLAN Configuration

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

To configure the MLD VLAN:

1. Select **Switching** > **Multicast** > **MLD Snooping** > **MLD VLAN Configuration**.

2. In the VLAN ID field, specify the on which MLD snooping is enabled.

3. In the Admin Mode list, select **Enable**.

4. In the Fast Leave Admin Mode list, enable or disable the MLD snooping fast leave mode for the specified VLAN.

   If fast leave is enabled, the VLAN can be immediately removed from the layer 2 forwarding table entry when the switch receives an MLD leave message for a multicast group without first sending out MAC-based general queries.

5. In the Group Membership Interval field, specify the number of seconds the VLAN should to wait for a report for a particular group on the VLAN before the MLD snooping feature deletes the VLAN from the group.

6. In the Maximum Response Time field, specify the number of seconds the VLAN should wait after sending a query if does not receive a report for a particular group. The specified value should be less than the group membership Interval.

7. In the Multicast Router Expiry Time field, specify the number of seconds the VLAN should wait to receive a query before it is removed from the list of VLANs with multicast routers attached.

8. Click the **Add** button.

To disable MLD snooping on a VLAN:

1. Select the check box next to each VLAN on which MLD snooping should be disabled.

2. Click the **Delete** button.

Multicast Router Configuration

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

To configure the Multicast Router:

1. Select **Snooping** > **Multicast Router Configuration**.

2. Select each interface to configure.

   For information about how to select and configure one or more ports or LAGs, see Configuring Interface Settings on page 28.

3. Use the Multicast Router field to enable or disable Multicast Router on the selected interface.

4. Click the **Apply** button.

Multicast Router VLAN Configuration

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

To configure the multicast router VLAN:

1. Select **Switching** > **Multicast** > **MLD Snooping** > **Multicast Router Configuration VLAN Configuration**.

2. From the Interface menu, select the interface to configure.

3. In the VLAN ID field, specify the VLAN ID for which the multicast router mode is to be enabled or disabled.

4. From the Multicast Router field, select **Enable** to enable the multicast router on the selected interface, or select **Disable** to disable the multicast router on the interface.

5. Click the **Apply** button.

Querier Configuration

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

To configure the querier settings:

1. Select **Switching** > **Multicast** > **MLD Snooping** > **Querier Configuration**.

2. Next to the Querier Admin Mode field, enable or disable the administrative mode for MLD snooping querier.

3. In the Querier Address field, specify the snooping querier address to be used as source address in periodic MLD queries.

   This address is used when no address is configured on the VLAN on which query is being sent. The supported IPv6 formats are x:x:x:x:x:x:x:x and x::x.

4. In the MLD Version field, the MLD protocol version used in periodic MLD queries is displayed.

The supported MLD Version is 1.

5. In the Query Interval field, specify the time interval in seconds between periodic queries sent by the snooping querier.

   The Query Interval must be a value in the range of 1–1800 seconds. The default value is 60.

6. In the Querier Expiry Interval field, specify the time interval in seconds after which the last querier information is removed.

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

7. Click the **Apply** button.

Querier VLAN Configuration

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

To configure MLD queriers:

1. Select **Switching** > **Multicast** > **MLD Snooping Querier** > **Querier VLAN Configuration**.
2. In the VLAN ID field, specify the VLAN ID for which the MLD snooping querier is to be enabled.
3. From the Querier Election Participate Mode list, select the mode:
   - **Disable**. Upon seeing another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
   - **Enable**. 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.
4. In the Querier VLAN Address field, specify the snooping querier IP address to be used as the source address in periodic MLD queries sent on the specified VLAN.
5. Click the **Add** button.

The following table describes the MLD snooping querier status information on the screen.

Table 63.

Field	Description
Operational State	Specifies the operational state of the IGMP snooping querier on a VLAN: • Querier. The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode. • Non-Querier. The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. • Disabled. The snooping Querier is not operational on the VLAN. The Snooping Querier moves to disabled mode when MLD Snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.
Operational Version	The MLD protocol version of the operational 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	The maximum response time to be used in the queries that are sent by the snooping querier.

To remove an MLD snooping querier configuration:

1. Select the check box next to each entry to remove.
2. Click the **Delete** button.

MVR Configuration

IGMP snooping helps limit multicast traffic when member ports are in the same VLAN; however, when ports belong to different VLANs, a copy of the multicast stream is sent to each VLAN that has member ports in the multicast group. MVR eliminates the need to duplicate the multicast traffic when multicast group member ports belong to different VLANs.

MVR uses a dedicated multicast VLAN to forward multicast traffic over the L2 network. Only one MVLAN can be configured per switch, and it is used only for certain multicast traffic, such as traffic from an IPTV application, to avoid duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the multicast VLAN without interfering with their membership in other VLANs.

MVR, like IGMP snooping, allows a layer 2 switch to listen to IGMP messages to learn about multicast group membership.

From the MVR configuration menu, you can access the following links:

MVR Configuration

Use the MVR Configuration screen to enable MVR and to configure global MVR settings on the switch.

To configure basic MVR settings:

1. **Select Switching** > **MVR** > **Basic** > **MVR Configuration**
2. Next to **MVR Running** select **Enable.**
3. In the **MVR Multicast VLAN field, s**pecify the VLAN on which MVR multicast data will be received.

    All source ports belong to this VLAN. The value can be set in a range of 1 to 4093. The default value is 1.

4. In the **MVR Global query response time** field, 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.

5. From the **MVR Mode** list, select the MVR mode of operation.
    *   **Dynamic**. The MVR switch learns existing multicast groups by snooping the IGMP queries from router on source ports and forwarding the IGMP reports from the hosts to the IGMP router on the Multicast VLAN (with appropriate translation of the VLAN ID).
    *   **Compatible**. The MVR switch does not learn multicast groups; the groups have to be configured by the operator because MVR does not forward IGMP reports from the hosts (RP port) to the IGMP router (SP port). To operate in this mode, the IGMP router has to be statically configured to transmit all required multicast streams to the MVR switch.

The following table describes the global MVR status fields on the screen.

Table 64. MVR status

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

MVR Group Configuration

Use the MVR Group Configuration screen to create and manage MVR groups on the switch. In this example, five MVR groups are created. To create multiple MVR groups in the same step, the groups must have contiguous IP addresses, such as 239.1.1.1, 239.1.1.2, 239.1.1.3, and so on.

To configure five contiguous MVR groups:

1. **Select Switching** > **MVR Configuration** > **Advanced** > **MVR Group Configuration**.
2. In the **MVR Group IP** field, specify the lowest multicast IP group address in the block of MVR group addresses.
3. In the Count field, specify the number of addresses in the contiguous block.

   In this example, the count is 5.

4. Click the **Add** button to add the five new MVR groups.

   The following figure shows the five MVR groups that are created in this procedure.


Figure 88. MVR Group Configuration

The following table describes the status information that is displayed for each MVR group.

Table 65. MVR group status information

Field	Definition
Status	The status of the MVR group, which is either active or inactive.
Members	The list of ports that participate in the MVR group.

MVR Interface Configuration

Use the MVR Interface Configuration screen to configure the ports that belong to the MVR groups and their roles within the groups.

To configure the MVR interfaces:

1. Select **Switching** > **MVR** > **Advanced** > **MVR Interface Configuration**.
2. Select the ports to configure.

   For information about how to select and configure one or more ports, see Configuring Interface Settings on page 28.
3. From the Admin Mode list, select **Enable** to enable MVR on the selected ports.
4. From the Type list, specify the MVR type for the selected ports:
   - **Source**. The port to which the multicast traffic flows using the multicast VLAN.
   - **Receiver**. The port where a listening host is connected to the switch. It can utilize any (or no) VLAN, except the multicast VLAN. This implies that the MVR switch performs VLAN tag substitution from the multicast VLAN source port to the VLAN tag used by the receiver port.
5. (Optionally for receiver ports) From the **Immediate Leave** list, select **Immediate Leave** mode to allow the receiver port to be removed from the multicast group membership when an IGMP leave message is received without sending an IGMP query message and waiting for the IGMP group membership report.
6. Click the **Apply** button.

MVR Group Membership

Use the MVR Configuration screen to add or remove ports from MVR groups.

To configure MVR group membership:

1. Select **Switching** > **MVR** > **Advanced** > **MVR Group Membership**.
2. From the **Group IP list, select the IP address of the MVR group to configure.**
3. Click under Group IP to display the ports.
4. To add a port to the selected MVR group, click the box directly below the port number so that a check mark appears in the box.
5. Click the **Apply** button.

MVR Statistics

Use the MVR Statistics screen to view information about the IGMP messages and IGMP packages the switch has transmitted.

To view MVR statistics, select **Switching** > **MVR** > **Advanced** > **MVR Statistics**.

The following table describes the MVR statistics.

Table 66. 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.

Address Table

The address table maintains a list of MAC addresses after having received a packet from this MAC address. The transparent bridging function uses the forwarding database entries to determine how to forward a received frame.

The Address Table link contains links described in the following sections.

- MAC Address Table
- Dynamic Address Configuration
- Static MAC Address

MAC Address Table

The MAC Address Table contains information about unicast entries for which the switch has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame. Use the search function of the MAC Address Table screen to display information about the entries in the table.

The MAC Address Table contains information about unicast entries for which the switch has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame. Use the search function of the MAC Address Table screen to display information about the entries in the table.

To search for an entry in the MAC address table:

1. Select **Switching** > **Address Table** > **Basic** > **Address Table**.

2. From the Search By list, select the criteria to use for the search:
   - **MAC Address**. Select **MAC Address** from the menu and enter a 6-byte hexadecimal MAC address in 2-digit groups separated by colons, then click the **Go** button. If the address exists, that entry will be displayed. An exact match is required.
   - **VLAN ID**. Select **VLAN ID** from the menu, enter the VLAN ID, for example, 100. Then click the **Go** button. If any entries with that VLAN ID exist they are displayed.
   - **Interface**. Select **Interface** from the menu, enter the interface ID in g1, g2... format, then, click the **Go** button. If any entries learned on that interface exist, they are displayed.

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

Table 67. Address Table

Field	Description
VLAN ID	Specifies the VLAN ID on which the IGMP Snooping Querier is administratively enabled and for which VLAN exists in the VLAN database.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address with each byte separated by colons. For example, 00:0F:89:AB:CD:EF.
Interface	The port where this address was learned: that is, this field displays the port through which the MAC address can be reached.
Status	The status of this entry. The possible values are: • Static. The entry was added when a static MAC filter was defined. • Learned. The entry was learned by observing the source MAC addresses of incoming traffic, and is currently in use. • Management. The system MAC address, which is identified with interface c1.

Dynamic Address Configuration

Use the Dynamic Addresses screen to set the amount of time to keep a learned MAC address entry in the forwarding database. The forwarding database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time.

To configure the dynamic address aging time-out value:

1. Select **Switching** > **Address Table** > **Advanced** > **Dynamic Addresses**.

2. In the Address Aging Timeout field, specify the number of seconds the forwarding database should wait before deleting a learned entry that has not been updated.

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

3. Click the **Apply** button.

Static MAC Address

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

To add a static MAC address:

1. Select **Switching** > **Address Table** > **Advanced** > **Static MAC Address**.
2. From the Interface list, select the port to associate with the statically configured MAC address.
3. In the MAC Address field, specify the MAC address to add.
4. From the VLAN ID list, select the VLAN ID corresponding to the MAC address to add.
5. Specify the interface associated with the MAC address.
6. Click the **Add** button.

To delete a static MAC address:

1. Select the check box next to each entry to remove.
2. Click the **Delete** button.

Multiple Registration Protocol Configuration[1]

Note: The Multiple Registration Protocol (MRP) feature is only supported on a standalone S3300 switch. Standalone here means that all four stack ports are running in Ethernet mode.

Multiple Registration Protocol (MRP) is a base registration protocol that enables devices running an MRP application to register attributes to other devices in a network. MRP provides an application to register attributes such as bandwidth requirement for a given AV stream and MAC address information. It is used by various applications to propagate the registration. The switch supports the following MRP applications:

- Multiple MAC Reservation Protocol (MMRP)
- Multiple Stream Reservation Protocol (MSRP)
- Multiple VLAN Registration Protocol (MVRP)

MMRP allows for the propagation MAC address information in the network, and allows for the registration and deregistration of both individual MAC address information and group MAC address membership. End stations may request to join or leave a multicast group, or to

---

1. The Multiple Registration Protocol (MRP) feature is available only with a valid license. To activate this feature, you must purchase a license.

register an individual MAC address with a specific VLAN. MAC address entries can be dynamically registered and deregistered if MMRP is administratively enabled on the switch.

MSRP reserves necessary resources in the network to facilitate time sensitive traffic to flow end to end. In a typical network, there are multiple Talkers (those who transmit streams) and multiple Listeners (those who receive streams from one or many Talkers). Each flow has specific bandwidth, frame rate, and time sync requirements. With the use of MSRP these resources are guaranteed through all intermediate devices that are between any talker and listener.

MVRP registers VLANs in the network, enabling automatic VLAN configuration on the switch. In a typical network, VLAN tagging is common. Many nodes require ingress traffic to be tagged with specific VLAN ID, and other nodes require egress traffic to be transmitted with a specific VLAN ID. With the use of MVRP on both ingress and egress, no manual VLAN configuration is required to pass tagged traffic through the network.

Note: MRP framework must be available and enabled in all intermediate devices to ensure that the propagation of the attributes occurs throughout the network.

With MRP, network attributes are declared, registered, withdrawn, and removed completely dynamically without any user intervention. This dynamic nature is especially useful in networks where:

- Network attributes are likely to change frequently, requiring reconfiguration of the intermediate devices.
- Recipients of these attributes frequently increase or decrease in number.
- Each of these changes without a dynamic self-adjusting framework would require constant attention from the network administrator.

From the MRP link, you can access the following screens:

- MRP Configuration
- MRP Port Settings
- MMRP Statistics
- MVRP Statistics
- MSRP Statistics
- MSRP Reservation Parameters
- Qav Parameters
- MSRP Streams Information

MRP Configuration

Use the MRP Configuration screen to configure global MRP settings for the switch.

To configure global MRP settings:

1. Select **Switching > MRP** > **Basic** > **MRP Configuration**.
2. Next to MVRP Mode, select **Enable** to enable MVRP globally on the switch.

   MVRP provides an application to dynamically register VLAN information. The default mode is Disable.

3. Next to MMRP Mode, select **Enable** to enable MMRP globally on the switch.

   MMRP provides an application to register MAC address information. The default mode is Disable.

4. Next to MSRP Mode, select **Enable** to enable MSRP globally on the switch.

   MSRP provides an application to register bandwidth requirement for a given AV stream. The default mode is Disable.

5. (Optionally) Configure the following settings:
   a. Enable MSRP talker pruning.

      The MSRP talker is the source of an AV stream. The administrative mode of talker pruning can be changed only when the MSRP mode is disabled.

   b. Enable the periodic state machine for MVRP on the system.
   c. Enable the periodic state machine for MMRP on the system.
   d. In the MSRP Max Fan In Ports field, specify the maximum number of the ports where MSRP registrations are allowed.
   e. Enable MSRP boundary propagation.

      The boundary propagation mode can be changed only when the global MSRP mode is administratively disabled.

6. Configure the 802.1Qav mapping for the Class A and/or Class B EAV streams.

   Class A streams have a higher transmission priority than Class B traffic.

   a. In the EAV Priority field, specify the priority for each EAV stream class.
   b. In the EAV Remap Priority field, specify the remap priority for non-EAV traffic.

7. Click the **Apply** button.

MRP Port Settings

Use the MRP Port Settings screen to configure the per-port MRP mode and timer settings. The timers control when and how often various messages are transmitted on each interface.

To configure the MRP port parameters:

1. Select **Switching** > **MRP** > **Advanced** > **Port Settings.**

2. Select the interfaces to configure.

   For information about how to select and configure one or more ports, see Configuring Interface Settings on page 28.

3. Configure the following MRP port settings:

   a. Enable or disable MVRP on the interface.

   b. Enable or disable MMRP on the interface.

   c. Enable or disable MSRP on the interface.

   d. Specify the value, in centiseconds, of the MRP Join Timer.

   e. Specify the value, in centiseconds, of the MRP Leave Timer.

   f. Specify the value, in centiseconds, of the MRP LeaveAll Timer.

   g. In the MSRP SR class PVID field, specify the default VLAN ID to be used for MSRP stream traffic.

   ClassA/ClassB Boundary Port fields are not configurable and show whether the interface is a boundary port.

4. Click the **Apply** button.

MMRP Statistics

The MMRP Statistics screen displays information regarding the MMRP frames transmitted and received by the switch and by each interface.

To view the MMRP Statistics screen, select **Switching > MRP** > **Advanced** > **MMRP Statistics**.

The following table describes the fields on the MMRP Statistics screen.

Table 68. MMRP statistics

Field	Description
Global MMRP Statistics	
Frames Received	The number of MMRP frames which were received on the switch.
Bad Header	The number of MMRP frames with bad headers which were received on the switch.
Bad Format	The number of MMRP frames with bad PDUs body formats which were received on the switch.

Table 68. MMRP statistics (continued)

Field	Description
Frames Transmitted	The number of MMRP frames which were transmitted on the switch.
Transmission Failures	The number of MMRP frames that the switch failed to transmit.
Per-Interface MMRP Statistics	
Interface	The interface associated with the rest of the MMRP statistics in the row.
Frames Received	The number of MMRP frames which were received on particular interface.
Bad Header	The number of MMRP frames with bad headers which were received on the particular interface.
Bad Format	The number of MMRP frames with bad PDUs body formats which were received on the particular interface.
Frames Transmitted	The number of MMRP frames which were transmitted on the interface.
Transmission Failures	The number of MMRP frames transmitting of which were failed on particular interface.

MVRP Statistics

The MVRP Statistics screen displays information regarding the MVRP frames transmitted and received by the switch and by each interface.

To view the MVRP Statistics screen, select **Switching > MRP** > **Advanced** > **MVRP Statistics**.

The following table describes the fields on the MVRP Statistics screen.

Table 69. MVRP statistics

Field	Description
Global MVRP Statistics	
Frames Received	The number of MVRP frames which were received on the switch.
Bad Header	The number of MVRP frames with bad headers which were received on the switch.
Bad Format	The number of MVRP frames with bad PDUs body formats which were received on the switch.
Frames Transmitted	The number of MVRP frames which were transmitted on the switch.
Transmission Failures	The number of MVRP frames that the switch failed to transmit.
Message Failures	The number of messages that failed to be added to the queue.
Per-Interface MVRP Statistics	
Interface	The interface associated with the rest of the MVRP statistics in the row.

Table 69. MVRP statistics (continued)

Field	Description
Frames Received	The number of MVRP frames which were received on particular interface.
Bad Header	The number of MVRP frames with bad headers which were received on the particular interface.
Bad Format	The number of MVRP frames with bad PDUs body formats which were received on the particular interface.
Frames Transmitted	The number of MVRP frames which were transmitted on the interface.
Transmission Failures	The number of MVRP frames transmitting of which were failed on particular interface.
Registration Failures	The number of MVRP frames that failed to register on a device or particular interface.

MSRP Statistics

The MSRP Statistics screen displays information about the MSRP frames transmitted and received by the switch and by each interface.

To view the MMRP Statistics screen, select **Switching > MRP** > **Advanced** > **MSRP Statistics**.

The following table describes the fields on the MSRP Statistics screen.

Table 70. MSRP statistics

Field	Description
Global MSRP Statistics	
Frames Received	The number of MSRP frames that have been received on the switch.
Bad Header	The number of MSRP frames with bad headers that have been received on the switch.
Bad Format	The number of MSRP frames with bad PDUs body formats that have been received on the switch.
Frames Transmitted	The number of MSRP frames which that have been transmitted on the switch.
Transmission Failures	The number of MSRP frames the switch failed to transmit.
Message Failures	The number of messages that failed to be added to the queue.
Per-Interface MSRP Statistics	
Interface	The interface associated with the rest of the MSRP statistics in the row.
Frames Received	The number of MSRP frames which were received the interface.
Bad Header	The number of MSRP frames with bad header which were received on the interface.

Table 70. MSRP statistics (continued)

Field	Description
Bad Format	The number of MSRP frames with bad PDUs body format which were received on the interface.
Frames Transmitted	The number of MSRP frames which were transmitted on the interface.
Transmission Failures	The number of MSRP frames that an interface attempted to transmit but failed.
Registration Failures	The number of MSRP frames that failed to register on a device or particular interface.

MSRP Reservation Parameters

Use the MSRP Reservation Parameters screen to view information about the talker, listener, and intermediate device status for the devices involved in each MSRP stream flowing through the switch.

To view the MSRP Reservation Parameters screen, select **Switching** > **MRP** > **Advanced** > **MSRP Reservation Parameters**.

The following table describes status fields on the MSRP Reservation Parameters screen.

Table 71. MSRP Reservation Parameters

Field	Description
Interface	The interface associated with the rest of the information in the row.
Stream ID	A 16-bit unsigned integer value, Unique ID, used to distinguish among multiple streams sourced by the same system.
Listener Declaration Status	The MSRP declaration status of the listener attribute.
Listener Declaration Type	The MSRP declaration type of the listener attribute.
Talker Declaration Status	The MSRP declaration status of the talker attribute.
Talker Declaration Type	The MSRP declaration type of the talker attribute.
Accumulated Latency	Identifies how much latency, in nanoseconds, the stream has suffered in its path from the Talker to a given Listener. It starts as a 0 in a Talker Advertise Declaration at the Talker, and its value is increased by one for each bridge as the Talker Advertise Declaration propagates through the network.
Failure Bridge Interface	The interface on the Bridge where the failure occurred.

Table 71. MSRP Reservation Parameters (continued)

Field	Description
Failure Code	The number that represents the reason for the failure. The switch supports the following codes: • 1—Insufficient bandwidth • 3—Insufficient bandwidth for the traffic class • 5—Stream destination_address is already in use • 7—Reported latency has changed • 8—Egress port is not Audio/Video Bridging (AVB) capable • 9—Use a different destination_address (i.e. MAC DA hash table full) • 12—Cannot store destination_address (i.e., Bridge is out of MAC DA resources) • 13—Requested priority is not an SR Class priority • 14—MaxFrameSize is too large for media • 15—msrpMaxFanInPorts limit has been reached • 16—Changes in FirstValue for a registered StreamID • 17—VLAN is blocked on this egress port (Registration Forbidden)
Failure Bridge MAC	The MAC address of the switch where the failure occurred.
Stream Age	The time, in seconds, since the stream destination address was added to the Dynamic Reservations Entries table. A value of zero indicates the destination address has not been added to the table.

Qav Parameters

Use the Qav Parameters screen to configure and view the per-port IEEE 802.1Qav settings. The IEEE 802.1Qav standard supports time-sensitive traffic streams by pacing all switch traffic, including legacy asynchronous Ethernet traffic, through queuing and forwarding. When a Talker declares a stream, it identifies whether the stream is Class A or Class B and specifies the stream's bandwidth requirements. Class A traffic has a higher transmission priority than Class B traffic.

On the Qav Parameters screen, you can view and configure selected bandwidth allocations for Class A and Class B traffic.

To configure the Qav parameters:

1. Select **Switching** > **MRP** > **Advanced** > **Qav Parameters**.

2. Select the ports to configure.

   For information about how to select and configure one or more ports, see Configuring Interface Settings on page 28.

3. Configure the Class A MSRP delta bandwidth.

   Class A Delta bandwidth is the additional bandwidth represented as a percentage of port transmit rate which can be reserved for the traffic class A and traffic class B. Class A traffic has a higher priority. The range is 0–100.

4. Configure the Class B MSRP delta bandwidth.

   Class B Delta bandwidth is the additional bandwidth represented as a percentage of port transmit rate which can be reserved for the traffic class B. The range is 0–100.

5. Click the **Apply** button.

The following table provides information about the status fields on the screen.

Table 72. Qav Parameter Status Information

Field	Description
Bandwidth Allocated	The current rate of the class A or B traffic on interface (in Bps).
Remaining Bandwidth	The maximum rate of the class A or B traffic available on interface (in Bps)
Total Bandwidth Allocated	The Sum of the allocated Class A and Class B traffic rates on interface (in Bps).
Total Remaining Bandwidth	75% of the interface speed minus total allocated bandwidth (in Bps/sec).

MSRP Streams Information

Use the MSRP Stream Information screen to view information about MSRP streams flowing through each interface.

To view MSRP Stream Information screen, select **Switching** > **MRP** > **Advanced** > **MSRP Stream Information**.

The following table describes the fields on the MSRP Stream Information screen.

Table 73. MSRP Streams Information

Field	Description
Stream ID	A 16-bit unsigned integer value, Unique ID, used to distinguish among multiple streams sourced by the same system.
Stream Source MAC Address	The MAC address of the traffic stream's source.
Received Accumulated Latency	The 32-bit unsigned Accumulated Latency component is used to determine the worst-case latency that a Stream can suffer in its path from the Talker to a given Listener. It starts as a 0 in a Talker Advertise Declaration at the Talker, and its value is increased by each Bridge as the Talker Advertise Declaration propagates through the network.
Traffic Class	Identifies whether the stream is Class A or Class B. Class A traffic has a higher priority than Class B traffic.
Rank	The 5-bit unsigned Rank component is used by systems to decide which streams can and cannot be served, when the MSRP registrations exceed the capacity of a Port to carry the corresponding data streams. If a Bridge becomes oversubscribed (e.g. network reconfiguration, 802.11 bandwidth reduction) the Rank will also be used to help determine which Stream or Streams can be dropped. A lower numeric value is more important than a higher numeric value.

Table 73. MSRP Streams Information (continued)

Field	Description
TSpec Max Frame Size	The 32-bit unsigned Bandwidth component is used to allocate resources and adjust queue selection parameters in order to supply the quality of service requested by an MSRP Talker Declaration. It represents the maximum rate, in units of 1024 octets per second, at which frames in the Stream referenced by the Talker Declaration may be transmitted.
TSpec Max Interval Frames	The 32-bit unsigned Frame Rate component is used to allocate resources and adjust queue selection parameters in order to supply the quality of service requested by an MSRP Talker Declaration. It represents the maximum number of frames that the Talker may transmit in one second.
Stream VLAN	The VLAN ID of the traffic stream.
Destination MAC	The MAC address of the traffic stream's destination.
Received Failure Bridge Interface	The interface on the Bridge where the failure occurred.
Received Failure Code	The code value of the failure. For more information about the failure codes, see Failure Code on page 188.
Received Failure Bridge MAC	The MAC address of the switch where the failure occurred.
Talker Interface	The interface on which the Talker is present.
Listeners	The interface on which Listeners are present.

802.1AS[1]

Note: The 802.1AS feature is only supported on a standalone S3300 switch. Standalone here means that all four stack ports are running in Ethernet mode.

The IEEE 802.1AS standard specifies the protocol and procedures used to ensure that the QoS requirements are guaranteed for time-sensitive applications, such as audio and video. The IEEE 1588 Precision Time Protocol (PTP) forms the basis of the IEEE 802.1AS standard. PTP specifies a precise clock synchronization protocol that relies on time-stamped packets. The PTP protocol is applicable to distributed systems consisting of one or more nodes communicating over some set of communication media. The distribution of synchronous time information is performed in a hierarchical manner with a grandmaster clock at the root of the hierarchy. The grandmaster provides a common and precise time reference for one or more directly-attached slave devices by periodically exchanging timing information. In other words, all slave devices synchronize their clocks with the grandmaster clock. The

---

1. The 802.1AS feature is available only with a valid license. To activate this feature, you must purchase a license.

slave devices can, in-turn, act as master devices for further hierarchical layers of slave devices.

From the 802.1AS link, you can access the following screens:

- 802.1AS Configuration
- 802.1AS (EAV) in a Stacking Environment
- 802.1AS Statistics

802.1AS Configuration

Use the 802.1AS Configuration screen to enable the 802.1AS mode on the switch and configure local clock priorities. The 802.1AS feature calculates the time delay between devices on a given link and maintains an accurate view of a network clock.The screen also displays various global 802.1AS information.

To configure the global 802.1AS settings on the switch:

1. Select **Switching** > **802.1AS** > **Basic** > **802.1AS Configuration**.
2. Next to 802.1AS status, select **Enable**.
3. In the Local Clock Priority1 field, specify the Priority1 value of the local clock (this time-aware bridge).
4. In the Local Clock Priority2 field, specify the Priority2 value of the local clock (this time-aware bridge).
5. Click the **Apply** button.

The following table shows the non-configurable information on the 802.1AS Configuration screen.

Table 74. 802.1AS Global Status

Field	Description
GrandMaster Present	Identifies whether Grand Master Clock is present. The default is False.
Best Clock Identity	The Best Clock Identity detected by this time-aware bridge.
Best Clock Priority1	The Priority1 value of the best clock on the switch.
Best Clock Priority2	The Priority2 value of the best clock on the switch.
Steps to Best Clock	The number of links in the path from the Best Clock to this time-aware bridge. If this time-aware bridge is the best, the value is zero.
Local Clock Identity	The Clock Identity of this time-aware bridge.
Last GM Change Timestamp	The system time when the most recent grandmaster clock change occurred.

802.1AS (EAV) in a Stacking Environment

If all the four Uplink ports are configured in Stacking mode, then the EAV pages are disabled and the 802.1AS (EAV) unavailable message is displayed:

- On the **Switching > 802.1AS > Basic > 802.1AS Configuration** screen as shown in Figure 89, Switching > 802.1AS (EAV) Unavailable.
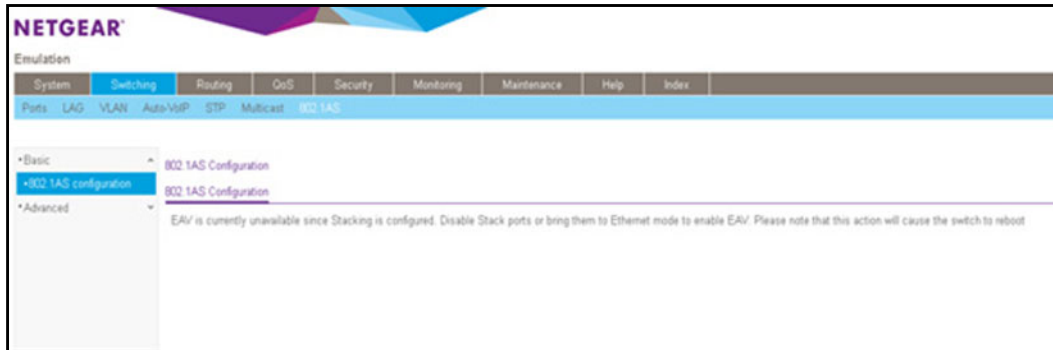

Figure 89. Switching > 802.1AS (EAV) Unavailable

- On the **Switching > MRP > Basic > MRP Configuration** screen as shown in Figure 90, Switching > MRP > 802.1AS (EAV) Unavailable.

Figure 90. Switching > MRP > 802.1AS (EAV) Unavailable

In a similar manner, if EAV is enabled, then the stack port pages are disabled.

When stack ports are not configured (in other words, the 10G ports are configured as Ethernet) and EAV is enabled globally:

1. Configure the Uplink ports in Ethernet mode and reload the switch, using the **System > Stacking > Advanced > Stack-port Configuration** screen as shown in Figure 91, Configure Uplink Ports in Ethernet Mode. See Advanced Stack Configuration on page 79

Figure 91. Configure Uplink Ports in Ethernet Mode

2. Next, enable 802.1AS using the **Switching > 802.1AS > Basic > 802.1AS Configuration** screen, as shown in Figure 92, Enable 802.1AS. See 802.1AS Configuration on page 191.


Figure 92. Enable 802.1AS

3. After enabling 802.1AS (EAV), the Stacking page becomes unavailable.
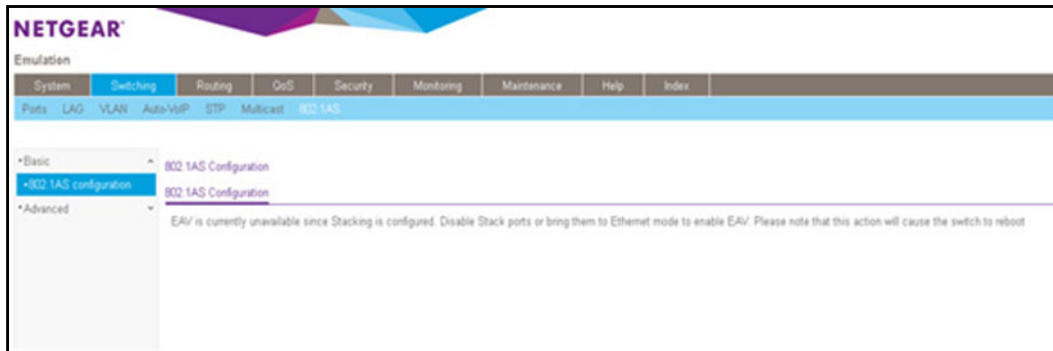
Figure 93. Stack Configuration is Unavailable

802.1AS Port Settings

Use the 802.1AS Port Settings screen to configure and view per-port 802.1AS settings.

To configure the 802.1AS port settings:

1. Select **Switching** > **802.1AS** > **Advanced** > **802.1AS Port Settings**.

2. Select the ports to configure.

   For information about how to select and configure one or more ports, see Configuring Interface Settings on page 28.

3. From the Admin Mode list, select **Enable**.

4. In the Pdelay Threshold field, specify the propagation delay threshold on the interface.

   The threshold determines whether the port is capable of participating in the 802.1AS protocol. If the propagation delay on the interface is above the threshold you configure, the interface is not considered capable of participating in the 802.1AS protocol. The peer delay must be less than the threshold value configured on the interface. The default value is 2500 nanoseconds. The range is 0–1,000,000,000 ns.

5. In the Allowed Lost Responses field, specify the allowed loss response value.

   If the interface does not receive valid responses to PDELAY_REQ messages above the value of the allowed lost responses, a port is considered to not be exchanging peer delay messages with its neighbor.

6. In the Initial Sync Interval field, specify the desired transmission rate of SYNC messages.

   This value is the logarithm to the base 2 of the mean-time interval between successive SYNC messages sent on this interface. The configured initial interval becomes the current interval only after the port is initialized or re-initialized for 802.1AS operation.

7. In the Pdelay Interval field, specify the desired transmission rate of PDELAY_REQ messages.

   This value is the logarithm to the base 2 of the mean time interval between successive PDELAY_REQ messages sent on this interface. The configured initial interval becomes the current interval only after the port is initialized or re-initialized for 802.1AS operation.

8. In the Announce Interval field, specify the desired transmission rate of ANNOUNCE messages.

    This value is the logarithm to the base 2 of the mean time interval between successive ANNOUNCE messages sent on this interface. The configured initial interval becomes the current interval only after the port is initialized or re-initialized for 802.1AS operation.

9. Configure the SyncRx Timeout.

    This value sets the number of SYNC intervals that have to pass without receipt of SYNC information before considering that the master is no longer transmitting.

10. Configure the AnnounceRx Timeout.

    This value sets the number of ANNOUNCE intervals that have to pass without receipt of ANNOUNCE PDU before considering that the master is no longer transmitting.

11. Click the **Apply** button.

The following table describes the non-configurable information on the 802.1AS Port Settings screen.

Table 75. 802.1AS port settings

Field	Description
Port Role	The 802.1AS role of the interface. The possible roles are as follows: • Disabled (default) • Master • Slave • Passive
Propagation Delay	The mean propagation delay on the interface
Measuring Pdelay	Indicates whether the interface is receiving PDELAY response messages from other end of the link.
802.1AS Capable	Indicates whether the interface is 802.1AS capable. By default, the interface is not 802.1AS capable.
Neighbor Rate Ratio	An estimated ratio of the frequency of the local clock entity of the time-aware system at the other end of the link attached to this port, to the frequency of the local clock entity of this time-aware system.
Current Sync Interval	The current mean time interval between successive SYNC messages sent over a link, in logarithm to base 2 format.
Current Pdelay Interval	The current mean time interval between successive PDELAY_REQ messages sent over a link, in logarithm to base 2 format.
Current Announce Interval	The current mean time interval between successive ANNOUNCE messages sent over a link, in logarithm to base 2 format.

802.1AS Statistics

The 802.1AS Statistics screen displays information regarding the 802.1AS messages transmitted and received by each interface.

If all 802.1AS statistics do not fit on the screen, use the horizontal scroll bar to view additional settings.

To display the 802.1AS Statistics screen, select **Switching** > **802.1AS** > **Advanced** > **802.1AS Statistics**.

The following table describes the information the 802.1AS Statistics screen displays.

Table 76. 802.1AS statistics

Field	Description
Interface	The interface associated with the rest of the 802.1AS statistics in the row.
Sync Tx	The total number of SYNC packets transmitted without error.
Sync Rx	The total number of SYNC packets received without error.
Followup Tx	The total number of FOLLOWUP packets transmitted without error.
Followup Rx	The total number of FOLLOWUP packets received without error.
Announce Tx	The total number of ANNOUNCE packets transmitted without error.
Announce Rx	The total number of ANNOUNCE packets received without error.
Pdelay Req Tx	The total number of PDELAY_REQ packets transmitted without error.
Pdelay Req Rx	The total number of PDELAY_REQ packets received without error.
Pdelay Resp Tx	The total number of PDELAY_RESP packets transmitted without error.
Pdelay Resp Rx	The total number of PDELAY_RESP packets received without error.
Pdelay Resp Followup Tx	The total number of PDELAY_RESP_FOLLOWUP packets transmitted without error.
Pdelay Resp Followup Rx	The total number of PDELAY_RESP_FOLLOWUP packets received without error.
Signaling Tx	The total number of SIGNALING packets transmitted without error.
Signaling Rx	The total number of SIGNALING packets received without error.
Sync Timeouts	The total number of SYNC receipt time-outs occurred.
Sync Discards	The total number of SYNC packets discarded.
Announce Timeouts	The total number of ANNOUNCE receipt time-outs occurred.
Announce Discards	The total number of ANNOUNCE packets discarded.
Pdelay Timeouts	The total number of PDELAY receipt time-outs occurred.

Table 76. 802.1AS statistics (continued)

Field	Description
Pdelay Discards	The total number of PDELAY packets discarded.
Bad Headers	The total number of packets received with bad header.

4

Configuring Routing

The switch supports IP routing. Use the menus under the Routing tab to manage routing on the system.

When a packet enters the switch, the destination MAC address is checked to see if it matches any of the configured routing interfaces. If it does, then the switch searches the host table for a matching destination IP address. If an entry is found, then the packet is routed to the host. If there is no matching entry, then the switch performs a longest prefix match on the destination IP address. If an entry is found, then the packet is routed to the next hop. If there is no match, then the packet is routed to the next hop specified in the default route. If there is no default route configured, then the packet is passed to the software to be handled appropriately.

The routing table can have entries added statically by the administrator. The host table can have entries added either statically by the administrator or dynamically via ARP.

This chapter contains the following sections.

Configure IP Settings

For information about how to configure and display IP routing data, see the following sections:

- IP Configuration on page 199
- VLAN Routing Wizard on page 203
- IP Statistics on page 200

IP Configuration

Use the IP Configuration screen to configure routing parameters for the switch.

To enable routing on the switch:

1. Select **Routing** > **IP** > **IP Configuration**.
2. Next to Routing Mode, select **Enable**.

   You must enable routing for the switch before you can route through any of the interfaces. Routing is also enabled or disabled per VLAN interface. The default value is Disable.

3. Click the **Apply** button.

The following table describes the IP configuration information displayed on the screen.

Table 77. Global IP Status Information

Field	Description
Default Time to Live	The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol. The default value is 64.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a compile-time constant. The default value is 1.

IP Statistics

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

To display the IP statistics screen, select **Routing** > **IP** >**Statistics**.

The following table describes the IP statistics information displayed on the screen.

Table 78. IP routing statistics

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
IpInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter includes only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.

Table 78. IP routing statistics (continued)

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

Table 78. IP routing statistics (continued)

Field	Description
IcmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there can be no types of error which contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object is always zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.

Configure VLAN Routing

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

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

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required. This section shows how to configure switch software to support VLAN routing. A port can be either a VLAN port or a router port, but not both. However, a VLAN port can be part of a VLAN that is itself a router port.

VLAN Routing Wizard

The VLAN Routing Wizard creates a VLAN routing interface, configure the IP address and subnet mask for the interface, and add selected ports or LAGs to the VLAN. With this wizard, you can:

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

To configure VLAN routing using the VLAN routing wizard:

1. Click **Routing** > **VLAN** > **VLAN Routing Wizard**.
2. In the VLAN ID field, specify the VLAN Identifier (VID) associated with this VLAN. The VID is 1 to 4093 characters in length.
3. In the IP Address field, define the IP address of the VLAN interface.
4. In the Network Mask field, define the subnet mask of the VLAN interface.
5. Click to view the ports or LAGs.
6. Click the box under each port or LAG to add to the VLAN as a VLAN member.

   Each port or LAG has three modes:

   - **T(Tagged)**. Select the ports on which all frames transmitted for this VLAN will be tagged. The ports that are selected will be included in the VLAN.
   - **U(Untagged)**. Select the ports on which all frames transmitted for this VLAN will be untagged. The ports that are selected will be included in the VLAN.
   - **BLANK(Autodetect)**. Select the ports that can be dynamically registered in this VLAN via GVRP. This selection has the effect of excluding a port from the selected VLAN.

7. Click the **Apply** button.

VLAN Routing Configuration

Use the VLAN Routing Configuration screen to view information about the VLAN routing interfaces configured on the system or to assign an IP address and subnet mask to VLANs on the system.

To configure VLAN routing:

1. Select **Routing** > **VLAN** > **VLAN Routing**.

2. From the VLAN list, select the VLAN you want to configure for VLAN routing.

   This field will display the all IDs of VLANs configured on this switch.

3. Enter an IP address of the VLAN routing interface.

4. Enter a subnet mask for the VLAN routing interface.

5. In the IP MTU field, specify the maximum size of IP packets sent on an interface.

   A valid range is from 68 bytes to the link MTU. The default value is 1500. A value of 0 indicates that the IP MTU is unconfigured. When the IP MTU is unconfigured, the router uses the link MTU as the IP MTU. The link MTU is the maximum frame size minus the length of the layer 2 header.

6. Click the **Add** button.

The following table describes the VLAN routing interface status information available on the screen.

Table 79. VLAN routing interface information

Field	Description
Port	The port number assigned to the VLAN Routing Interface.
MAC Address	The MAC Address assigned to the VLAN Routing Interface.

Configure Router Discovery

The Router Discovery protocol is used by hosts to identify operational routers on the subnet. Router discovery messages are of two types: router advertisements and router solicitations. The protocol mandates that every router periodically advertise the IP addresses it is associated with. Hosts listen for these advertisements and discover the IP addresses of neighboring routers.

Use the Router Discovery Configuration screen to enter or change router discovery parameters.

To configure the router discovery parameters:

1. Select **Routing** > **Router Discovery**.

2. Select the router interface for which data is to be configured.

   To perform the same configuration on all interfaces, select the check box in the heading row. To configure a single interface, select the check box associated with the interface. The interface number displays in the Interface field in the table heading row.

3. From the Advertise Mode list, select **Enable**.

Router advertisements are transmitted from the selected interface.

4. In the Advertise Address field. specify the IP address to be used to advertise the router.

5. In the Maximum Advertise Interval field, specify the maximum time (in seconds) allowed between router advertisements sent from the interface.

6. In the Minimum Advertise Interval field, specify the minimum time (in seconds) allowed between router advertisements sent from the interface.

7. In the Advertise Lifetime field, specify the value (in seconds) to be used as the lifetime field in router advertisements sent from the interface.

   This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.

8. In the Preference Level field, specify the preference level of the router as a default router relative to other routers on the same subnet.

   Higher numbered addresses are preferred. You must enter an integer.

9. Click the **Apply** button.

Configure and View Routes

From the Route Configuration screen, you can configure static and default routes and view the routes that the switch has already learned.

To configure a static route:

1. Select **Routing** > **Route Configuration**.

2. From the Route Type field, select **Static**.

   When you create a default route, you must specify only the next hop IP address. By default, the default route has a preference of 1.

3. In the Network Address field, specify the IP route prefix for the destination.

   To create a route, a valid routing interface must exist, and the next hop IP Address must be on the same network as the routing interface.

4. In the Subnet Mask field, specify the subnet mask.

   Also referred to as the subnet/network mask, this indicates the portion of the IP address that identifies the attached network.

5. In the Next Hop IP Address field, specify the next hop IP address.

   This is the outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network. When creating a route, the next hop IP must be on the same network as the routing interface. Valid next hop IP Addresses can be seen in the Route Status table.

6. In the Preference field, specify the preference value for the route.

Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you can control whether a static route is more or less preferred. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

7. (Optionally) In the Description field, specify a description to help identify the route.

8. Click the **Add** button.

The Route Status table provides information about the static routes configured on the switch and the dynamic routes the switch has learned.

Table 80. Routing table information

Field	Description
Route Type	Indicates whether the learned route is a static or default route.
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are one of the following: • Local • Static
Route Type	This field can be Connected or Static or Dynamic based on the protocol.
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
Preference	The preference is an integer value from 1 to 255. You can specify the preference value of an individual static route.
Metric	Administrative cost of the path to the destination.

To delete one or more static routes:

1. Select the check box next to each route to remove.

2. Click the **Delete** button.

Configure ARP

The address resolution protocol (ARP) associates a layer 2 MAC address with a layer 3 IPv4 address. Switch software features both dynamic and manual ARP configuration. With manual ARP configuration, you can statically add entries into the ARP table.

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

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

The switch supports 512 ARP entries, which includes dynamic and static ARP entries.

Devices can be moved in a network, which means the IP address that was at one time associated with a certain MAC address is now found using a different MAC address, or can have disappeared from the network altogether (in other words, it has been reconfigured, disconnected, or powered off). This leads to stale information in the ARP cache unless entries are updated in reaction to new information seen on the network, periodically refreshed to determine if an address still exists, or removed from the cache if the entry has not been identified as a sender of an ARP packet during the course of an ageout interval, usually specified via configuration.

To configure and display ARP details, see the following sections:

- ARP Cache on page 208
- Create a Static ARP Entry on page 209
- Configure Global ARP Settings on page 209
- Remove an ARP Entry From the ARP Cache on page 210

ARP Cache

Use the ARP Cache screen to view entries in the ARP table, a table of the remote connections most recently seen by this switch.

To display entries in the ARP table, select **Routing** > **ARP** > **Basic** > **ARP Cache**.

The following table provides information included in the management VLAN ARP cache section.

Table 81. ARP cache information

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

The following table provides information included in the routing VLANs ARP cache section.

Table 82. ARP cache information for routing VLANs

Field	Description
Interface	The routing interface associated with the ARP entry.
IP Address	The associated IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
MAC Address	The unicast MAC address of the device.
Type	The type of the ARP entry. Possible values are: • **Local.** An ARP entry associated with one of the switch's routing interface's MAC addresses. • **Gateway.** A dynamic ARP entry whose IP address is that of a router. • **Static.** An ARP entry configured by the user. • **Dynamic.** An ARP entry which has been learned by the router.
Age	Age since the entry was last refreshed in the ARP Table. The format is hh:mm:ss.

Create a Static ARP Entry

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

To add an entry to the ARP table:

1. Select **Routing** > **ARP** > **Advanced** > **ARP Create**.
2. In the IP Address field, specify the IP address to add.

    It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.

3. In the MAC Address field, specify the unicast MAC address of the device.

    The format is six 2-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

4. Click the **Add** button.

For information about the information in the Routing VLANs ARP Cache table, see <u>Table 82, ARP cache information for routing VLANs on page 208</u>.

Configure Global ARP Settings

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

To display or change the parameters of the ARP table:

1. Select **Routing** > **ARP > Advanced** > **Global ARP Configuration**.
2. In the Age Time field, specify the number of seconds it will take for an ARP entry to age out.
3. In the Response Time field, specify the number of seconds the switch will wait for a response to an ARP request.
4. In the Retries field, specify the maximum number of times an ARP request will be retried.
5. In the Cache Size field, specify the maximum number of entries for the ARP cache.
6. Next to Dynamic Renew, select **Enable** to allow the ARP component to automatically attempt to renew dynamic ARP entries c when they age out.
7. Click the **Apply** button.

Remove an ARP Entry From the ARP Cache

Use this screen to remove certain entries from the ARP Table.

To remove entries from the ARP table:

1. Select **Routing** > **ARP** > **Advanced** > **ARP Entry Management**.

2. From the Remove From Table list, select the type of ARP entry to be removed.

    The choices listed specify the type of ARP Entry to be deleted:

    - All Dynamic Entries
    - All Dynamic and Gateway Entries
    - Specific Dynamic/Gateway Entry
    - Specific Static Entry
    - None Select this option if you do not want to delete any entry from the ARP Table.

3. If Specific Dynamic/Gateway Entry or Specific Static Entry is the selected type, enter the IP address of the entry to remove from the ARP table.

4. Click the **Apply** button.

5

Configuring Quality of Service

In a typical switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets have no place to be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS-capable. The presence of at least one node that is not QoS-capable creates a deficiency in the network path, and the performance of the entire packet flow is compromised.

Use the features you access from the QoS tab to configure Quality of Service (QoS) settings on the switch. The QoS tab contains links to the features described in the following sections.

Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, or transmission rate shaping are user configurable at the queue (or port) level.

Eight queues per port are supported.

From the Advanced link, the Class of service menu under the QoS tab, you can access the screens described in the following sections:

- CoS Configuration on page 212
- CoS Interface Configuration on page 213
- Interface Queue Configuration on page 214
- 802.1p to Queue Mapping on page 215
- DSCP to Queue Mapping on page 216

CoS Configuration

Use the CoS Configuration screen to set the class of service trust mode of an interface. Each port in the switch can be configured to trust one of the packet fields (802.1p or IP DSCP), or to not trust any packet's priority designation (untrusted mode). If the port is set to a trusted mode, it uses a mapping table appropriate for the trusted field being used. This mapping table indicates the CoS queue to which the packet should be forwarded on the appropriate egress port. 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, in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping is unable to be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

To configure CoS trust mode settings on all interfaces:

1. Select **QoS** > **Basic** > **CoS Configuration**.
2. Select the **Global** radio button to configure the same CoS trust mode settings to all interfaces

3. From the Global Trust Mode drop down list, select the trust mode for ingress traffic on the switch.

   Global Trust Mode can be one of the following:

   • **Untrusted**. Do not trust any CoS packet marking at ingress.

   • **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues.

   • **DSCP**. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

4. Click the **Apply** button.

To configure the CoS trust mode on a specific interface:

1. Select the **Interface** radio button to apply trust mode settings to an individual interface. The per-interface setting overrides the global settings.

2. From the interface list, select the port or LAG to configure.

3. From the Interface Trust Mode list, select the trust mode for ingress traffic on the interface.

   Interface Trust Mode can be one of the following:

   • **Untrusted**. Do not trust any CoS packet marking at ingress.

   • **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues.

   • **DSCP**. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

4. Click the **Apply** button.

CoS Interface Configuration

Use the CoS Interface Configuration screen to configure the trust mode for one or more interfaces and to apply an interface shaping rate to all interfaces or to a specific interface.

To configure CoS settings for an interface:

1. Select **QoS** > **CoS** > **Advanced** > **CoS Interface Configuration**.

2. Select the interfaces to configure.

   For information about how to select and configure one or more ports and LAGs, see <u>Configuring Interface Settings on page 28</u>.

3. From the Interface Trust Mode drop down list, select the trust mode for ingress traffic on the selected interfaces.

   • **Untrusted**. Do not trust any CoS packet marking at ingress.

- **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues.

- **DSCP**. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

4. In the Interface Shaping Rate field, 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. The valid range is 0 to 100 in increments of 1. The value 0 means the maximum is unlimited.

   The expected shaping at egress interface is calculated as:

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

   Setting the value to 0 resets the configured traffic-shape rate.

5. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

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

Interface Queue Configuration

Use the Interface Queue Configuration screen to define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port. Each port has its own CoS queue-related configuration.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally or per-port. A global configuration change is automatically applied to all ports in the system.

To configure CoS queue settings for an interface:

1. Select **QoS** > **CoS** > **Advanced** > **Interface Queue Configuration**.

2. Select the interfaces to configure.

   For information about how to select and configure one or more ports and LAGs, see Configuring Interface Settings on page 28.

3. Configure any of the following settings:

   - **Queue ID**. Select the queue to be configured.

   - **Minimum Bandwidth**. Enter a percentage of the maximum negotiated bandwidth for the selected queue on the interface. Specify a percentage from 0–100, in increments of 1.

- **Scheduler Type**. Select the type of queue processing. Defining on a per-queue basis allows you to create the desired service characteristics for different types of traffic.

  - **Weighted**. Weighted round robin associates a weight to each queue. This is the default.

  - **Strict**. Services traffic with the highest priority on a queue first.

- **Queue Management Type**. The type of packet management used for all packets, which is Taildrop. All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.

4. Click the **Apply** button.

802.1p to Queue Mapping

Use this screen to view or change which internal traffic classes are mapped to the 802.1p priority class values in Ethernet frames the device receives. The priority-to-traffic class mappings can be applied globally or per-interface. The mapping allows the switch to group various traffic types (for example, data or voice) based on their latency requirements and give preference to time-sensitive traffic.

To map 802.1p priorities to queues:

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

2. Select one of the following radio buttons:

   - Select the **Global** radio button to apply the same 802.1p priority mapping to all CoS configurable interfaces.

   - Select the **Interface** radio button to apply 802.1p priority mapping to on a per-interface basis.

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

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

   The 802.1p Priority row contains traffic class selectors for each of the eight 802.1p priorities to be mapped. The priority goes from low (0) to high (7). For example, traffic with a priority of 0 is for most data traffic and is sent using "best effort." Traffic with a higher priority, such as 7, might be time-sensitive traffic, such as voice or video.

   The values in each drop-down 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.

4. Click the **Apply** button.

DSCP to Queue Mapping

Use the DSCP to Queue Mapping screen to specify which internal traffic class to map the corresponding DSCP value.

To map DSCP values to queues:

1. Select **QoS** > **CoS** > **Advanced** > **DSCP to Queue Mapping**.

2. For each DSCP value, select a hardware queue to associate with the value.

    The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent.

3. Click the **Apply** button.

Differentiated Services

The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Standard IP-based networks are designed to provide "best effort" data delivery service. "Best effort" service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets can be delayed, sent sporadically, or dropped. For typical Internet applications, such as e-mail and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. Conversely, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Defining DiffServ

To use DiffServ for QoS, you must first use the links accessible from the Differentiated Services configuration menu to define the following categories and their criteria:

1. Class: Create classes and define class criteria.

2. Policy: Create policies, associate classes with policies, and define policy statements.

3. Service: Add a policy to an inbound interface

Packets are classified and processed based on defined criteria. The classification criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes 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.

The Differentiated Services menu contains links to the various DiffServ configuration and display features described in the following sections:

- Diffserv Configuration on page 217
- Class Configuration on page 218
- IPv6 Class Configuration on page 221
- Policy Configuration on page 222
- Service Configuration on page 225
- Service Statistics on page 225

Diffserv Configuration

Use the DiffServ Configuration screen to display DiffServ general status group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables.

To configure the global DiffServ mode:

1. Select **QoS** > **DiffServ** > **Advanced** > **DiffServ Configuration**.
2. Next to DiffServ Admin Mode, select **Enable**.

   If you disable DiffServ after it has been configured and enabled, the DiffServ configuration is retained and can be changed, but it is not active.

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

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

Table 83. DiffServ MIB table information

Field	Description
Class Table	The current and maximum number of rows of the class table. The max size is 32.
Class Rule Table	The current and maximum number of rows of the class rule table. The max size is 192.
Policy Table	The current and maximum number of rows of the policy table. The max size is 32.
Policy Instance Table	The current and maximum number of rows of the policy instance table. The max size is 320.
Policy Attributes Table	The current and maximum number of rows of the policy attributes table. The max size is 320.
Service Table	The current and maximum number of rows of the service table. The max size is 338.

Class Configuration

Use the Class Configuration screen to add a new DiffServ class name, or to rename or delete an existing class. The screen also allows you to define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can have multiple match criteria in a class. The logic is a Boolean logical-and for this criteria. After creating a Class, click the class link to the Class screen.

To create a DiffServ class:

1. Select **QoS** > **DiffServ** > **Advanced** > **Class Configuration**.
2. In the Class Name field, enter a class name.
3. Select the class type
4. Click the **Add** button.

   The switch supports only the Class Type value All, which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria.

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

To rename an existing class:

1. Select the check box next to the configured class.
2. In the Class Name field, update the name.
3. Click the **Apply** button.

To delete a class:

1. Select the check box next to the class name.
2. Click the **Delete** button.

To configure the class match criteria:

1. Click the class name for an existing class.

Figure 94. DiffServ Class Name

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

Figure 95. DiffServ Class Configuration Criteria

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

- **Match Every**. This adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

- **Reference Class**. Selects a class to start referencing for criteria. A specified class can reference at most one other class of the same type.

- **Class of Service**. Select the field and enter a class of service 802.1p user priority value to be matched for the packets. The valid range is 0–7.

- **VLAN**. Select the field and enter a VLAN ID to be matched for packets. The VLAN ID range is 1–4093.

- **Ethernet Type**. This lists the keywords for the Ether Type from which one can be selected.

- **Source MAC Address**. This is the source MAC address specified as six, two-digit hexadecimal numbers separated by colons.

- **Source MAC Mask**. This is a bit mask in the same format as MAC Address indicating which part(s) of the source MAC Address to use for matching against packet content.

- **Destination MAC Address**. This is the destination MAC address specified as six, two-digit hexadecimal numbers separated by colons.

- **Destination MAC Mask**. This is a bit mask in the same format as MAC Address indicating which part(s) of the destination MAC Address to use for matching against packet content.
- **Protocol Type**. Requires a packet's layer 4 protocol to match the protocol you select. If you select Other, enter a protocol number in the field that displays. The valid range is 0–255.
- **Source IP Address**. Requires a packet's source port IP address to match the address listed here. In the IP Address field, enter a valid source IP address in dotted decimal format.
- **Source Mask**. Enter a valid subnet mask to determine which bits in the IP address are significant. Note that this is not a wildcard mask.
- **Source L4 Port**. Requires a packet's TCP/UDP source port to match the port you select. Select the desired L4 keyword from the list on which the rule can be based. If you select Other, the screen refreshes and a Port ID field displays. Enter a user-defined Port ID by which packets are matched to the rule.
- **Destination IP Address**. Requires a packet's destination port IP address to match the address listed here. In the IP Address field, enter a valid destination IP address in dotted decimal format.
- **Destination Mas**k. Enter a valid subnet mask to determine which bits in the IP address are significant. This is not a wildcard mask.
- **Destination L4 Port**. Requires a packet's TCP/UDP destination port to match the port you select. Select the desired L4 keyword from the list on which the rule can be based. If you select Other, the screen refreshes and a Port ID field displays. Enter a user-defined Port ID by which packets are matched to the rule.
- **IP DSCP**. Matches the packet's DSCP to the class criteria's when selected. Select the DSCP type from the menu or enter a DSCP value to match. If you select Other, enter a custom value in the DSCP Value field that displays.
- **IP Precedence**. Matches the packet's IP Precedence value to the class criteria's when Enter a value in the range of 0–7.
- **IP ToS**. Matches the packet's Type of Service bits in the IP header to the class criteria's when selected and a value is entered. In the ToS Bits field, enter a two-digit hexadecimal number to match the bits in a packet's ToS field. In the ToS Mask field, specify the bit positions that are used for comparison against the IP ToS field in a packet.

3. Click the **Apply** button.
4. Click the **Cancel** button to cancel the configuration on the screen, and reset the data on the screen to the latest value of the switch.

IPv6 Class Configuration

The IPv6 Class Configuration feature extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification. An Ethernet IPv6 packet is distinguished from an IPv4 packet by its unique EtherType value, so all IPv6 classifiers include the EtherType field. An IPv6 access list serves the same purpose as its IPv4 counterpart.

Prior to the IPv6 class feature, any DiffServ class definition was assumed to apply to an IPv4 packet. That is, any match item in a class rule was interpreted in the context of an IPv4 header. An example is a class rule that specifies an L4 Port match value. With the introduction of the IPv6 match capability, it must be specified if this class rule is for IPv4 or for IPv6 packets. To facilitate this distinction, a class configuration parameter is added to specify whether a class applies to IPv4 or IPv6 packet streams.

The Destination and Source IPv6 addresses use a prefix length value instead of an individual mask to qualify it as a subnet address or a host address. The flow label is a 20-bit number that is unique to an IPv6 packet, used by end stations to signify some form of quality-of-service (QoS) handling in routers.

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

IPv6 ACL/DiffServ assignment is appropriate for LAG interfaces. The procedures described by an ACL or DiffServ policy are equally applicable on a LAG interface.

To create a new IPv6 class:

1. Select **QoS** > **DiffServ** > **Advanced** > **IPv6 Class Configuration**.
2. Enter a class name in the Class Name field.
3. Select the class type to associate with the policy.
4. Click the **Add** button.

   The switch supports only the Class Type value All, which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria.

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

To rename an existing class:

1. Select the check box next to the configured class.
2. In the Class Name field, specify the new name.
3. Click the **Apply** button.

To delete a class:

1. Select the check box next to the class name.
2. Click the **Delete** button.

The same set of fields described for IPv6 ACL classification are also supported as match criteria for DiffServ classes. Prior to the introduction of IPv6 class rule fields, any layer 3 or layer 4 item was interpreted as a field in an IPv4 packet. To properly interpret the match criteria fields and create classifier entries, it is necessary for the configuration to specify what type of packet a class defines.

Policy Configuration

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

To create a new DiffServ policy:

1. Select **QoS** > **DiffServ** > **Advanced** > **Policy Configuration**.
2. Enter a policy name in the Policy Name field.
3. Select the existing DiffServ class to associate with the policy.
4. Click the **Add** button.

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

To rename an existing policy or add a new member class to the policy:
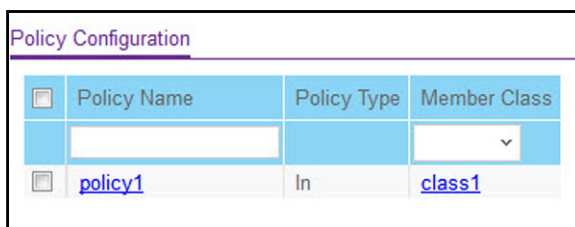
1. Select the check box next to the configured class.
2. Update the desired fields.
3. Click the **Apply** button.
4. Click the **Cancel** button to cancel the configuration on the screen, and reset the data on the screen to the latest value of the switch.

To delete a policy:

1. Click the check box associated with the policy to remove.
2. Click the **Delete** button.

To configure the policy attributes:

1. Click the name of the policy.

Figure 96. Policy Name

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

Figure 97. Policy Configuration

2. Configure the policy attributes:

- **Assign Queue**. Select this value from the drop-down list. This is an integer value in the range 0 to 6.

- **Drop**. Select this option to drop every inbound packet.

- **Mark VLAN CoS**. Select this value from the drop-down list. This is an integer value in the range from 0 to 7 for setting the VLAN priority.

- **Mark IP Precedence**. Select this value from the drop-down list. This is an IP Precedence value in the range from 0 to 7.

- **Mirror**. This flag indicates that the policy attribute is defined to mirror every inbound packet.

- **Redirect**. This flag indicates that the policy attribute is defined to redirect every inbound packet to the specified interface.

- **Mark IP DSCP**. This lists the keywords for the known DSCP values from which one can be selected.

- **Simple Policy**. This lists the keywords for the known DSCP values from which one can be selected.

3. **Color Conform Class**. This field is visible only if you select Color Aware Color Mode on the Policing Attributes screen, this lists the DiffServ classes that are valid for use as a conform color-aware specifier.

One of the classes must be selected from this list.

4. If you select the Simple Policy attribute, configure the following fields:

- **Color Mode**. Color Aware mode requires the existence of one or more color classes that are valid for use with this policy instance; otherwise, the color mode is color blind, which is the default.

- **Color Conform Mode**. The match-criteria of the color Conform class.

- **Committed Rate**. The committed rate is specified in kilobits-per-second (Kbps) and is an integer from 1–4294967295.

- **Committed Burst Size**. The committed burst size is specified in kilobytes (KB) and is an integer from 1–128.

- **Conform Action**. Determines what happens to packets that are considered conforming (below the police rate). Select one of the following actions:

  - **Send**. (default) These packets are presented unmodified by DiffServ to the system forwarding element.

  - **Drop**. These packets are immediately dropped.

  - **Mark CoS**. These packets are marked by DiffServ with the specified CoS value before being presented to the system forwarding element. This selection requires that the Mark CoS value field be set.

  - **Mark IP Precedence**. These packets are marked by DiffServ with the specified IP Precedence value before being presented to the system forwarding element. This selection requires that the Mark IP Precedence value field be set.

  - **Mark IP DSCP**. These packets are marked by DiffServ with the specified DSCP value before being presented to the system forwarding element. This selection requires that the DSCP value field be set. If you select **Other**, enter a custom value in the DSCP Value field that displays.

- **Violate Action**. Determines what happens to packets that are considered non-conforming (above the police rate). Select one of the following actions:

  - **Send**. (default) These packets are presented unmodified by DiffServ to the system forwarding element.

  - **Drop**. (default) These packets are immediately dropped.

  - **Mark CoS**. These packets are marked by DiffServ with the specified CoS value before being presented to the system forwarding element. This selection requires that the Mark CoS value field be set.

  - **Mark IP Precedence**. These packets are marked by DiffServ with the specified IP Precedence value before being presented to the system forwarding element. This selection requires that the Mark IP Precedence value field be set.

  - **Mark IP DSCP**. These packets are marked by DiffServ with the specified DSCP value before being presented to the system forwarding element. This selection requires that the DSCP value field be set.

5. Click the **Apply** button.

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

Service Configuration

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

To attach a DiffServ policy to an interface:

1. Select **QoS** > **DiffServ** > **Advanced** > **Service Configuration**.

2. Select the interfaces to attach to the policy.

   For information about how to select and configure one or more ports and LAGs, see Configuring Interface Settings on page 28.

3. From the Policy In Name list, select the policy to attach to the interface.

4. Click the **Apply** button.

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

To remove a policy from an interface:

1. Select the interface(s) on which the policy is to be removed.

2. From the Policy In Name list, select **None**.

3. Click the **Apply** button.

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

Service Statistics

Use the Service Statistics screen to display service-level statistical information about all interfaces that have DiffServ policies attached.

To display the service statistics screen:

Select **QoS** > **DiffServ** > **Advanced** > **Service Statistics**.

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

Table 84. Service statistics

Field	Description
Interface	The interface for which service statistics are to display.
Direction	The direction of packets for which service statistics display, which is always *In*.
Policy Name	The policy associated with the selected interface.

Table 84. Service statistics (continued)

Field	Description
Operational Status	The operational status of this service interface, which is either Up or Down.
Discarded Packets	The total number of packets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.
Member Classes	Selects the member class for which octet statistics are to display.

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

6

Managing Device Security

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

Management Security Settings

From the Management Security menu, 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.

The Management Security folder contains links described in the following sections.

- Change Password on page 228
- RADIUS Configuration on page 229
- Configure TACACS+ on page 233
- Authentication List Configuration on page 235
- Smart Control Center Utility on page 237

Change Password

Use this screen to change the login password.

To change the login password for the management interface:

1. Select **Security** > **Management Security** > **User Configuration** > **Change Password**.
2. Specify the current password in the Old Password field.

   The entered password is displayed in asterisks (*). Passwords are 1–20 alphanumeric characters in length and are case sensitive.

3. Enter the new password.

   It does not display as it is typed, and only asterisks (*) will show on the screen. Passwords are 1–20 alphanumeric characters in length and are case sensitive.

4. To confirm the password, enter it again to make sure you entered it correctly.

   The password does not display, but will show asterisks (*)

5. Click the **Apply** button.

To reset the password to the default value:

1. Select the **Reset Password** check box.
2. Click the **Apply** button.

Note: In you have forgotten the password and are unable to log in to the switch management interface, press the **Factory Defaults** button on the front panel of the switch for more than 1 second. The device reboots, and all switch settings, including the password, are reset to the factory default values. If you press the button for less than 1 second, the switch reboots, but the switch loads the saved configuration.

RADIUS Configuration

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

• Web access

• Port access control (802.1X)

The RADIUS menu contains links to the features described in the following sections.

Global Configuration

Use the Global Configuration screen to add information about one or more RADIUS servers on the network.

Consideration to maximum delay time should be given when configuring RADIUS maximum retransmit and RADIUS time-out. If multiple RADIUS servers are configured, the maximum retransmit value on each will run out before the next server is attempted. A retransmit will not occur until the configured time-out value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the product of retransmit × time-out for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.

To configure global RADIUS server settings:

1. Select **Security** > **Management Security** > **RADIUS** > **Global Configuration**.

    The Current Server IP Address field is blank if no servers are configured (see RADIUS Server Configuration on page 230). The switch supports up to three configured RADIUS servers. If more than one RADIUS servers are configured, the current server is the server configured as the primary server. If no servers are configured as the primary server, the current server is the most recently added RADIUS server.

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

3. In the Timeout Duration field, specify the time-out value, in seconds, for request retransmissions.

4. From the Accounting Mode list, select whether the RADIUS accounting mode is enabled or disabled on the current server.

5. Click the **Apply** button.

RADIUS Server Configuration

Use the RADIUS Server Configuration screen to view and configure various settings for the current RADIUS server configured on the system.

To add a primary RADIUS server with a shared secret:

1. Select **Security** > **Management Security** > **RADIUS** > **Server Configuration**.

2. In the Server Address field, specify the IP address of the RADIUS server to add.

3. In the Authentication Port field, specify the UDP port number the server uses to verify the RADIUS server authentication. The valid range is 1–65535. The default value is 1812.

4. From the Secret Configured list, select **Yes**.

   You must select **Yes** before you can configure the RADIUS secret. After you add the RADIUS server, this field indicates whether the shared secret for this server has been configured.

5. In the Secret field, type the shared secret text string used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server.

   This secret must match the RADIUS encryption.

6. From the Active list, select **Primary**.

7. From the Message Authenticator list, enable or disable the message authenticator attribute for the selected server.

   The message authenticator adds protection to RADIUS messages by using an MD5 hash to encrypt each message. The shared secret is used as the key, and if the message fails to be verified by the RADIUS server, it is discarded.

8. Click the **Add** button.

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

Table 85. RADIUS server statistics

Field	Description
Server Address	This displays all configured RADIUS servers.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.

Table 85. RADIUS server statistics (continued)

Field	Description
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access-responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication time-outs to this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

To modify settings for a RADIUS server that is already configured on the switch:

1. Select the check box next to the server IP address.
2. Update the desired fields for the selected server.
3. Click the **Apply** button.

To delete a configured RADIUS server:

1. Select the check box next to the IP address of the server to remove.
2. Click the **Delete** button.

Accounting Server Configuration

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

To add a RADIUS accounting server with a shared secret:

1. Select **Security** > **Management Security** > **RADIUS** > **Accounting Server Configuration**.

2. In the Accounting Server Address field, specify the IP address of the RADIUS accounting server to add.

3. In the Port field, specify the UDP port number the server uses to verify the RADIUS accounting server authentication. The default UDP port number is 1813.

4. From the Secret Configured menu, select **Yes** to add a RADIUS secret in the next field.

    You must select **Yes** before you can configure the RADIUS secret. After you add the RADIUS accounting server, this field indicates whether the shared secret for this server has been configured.

5. In the Secret field, type the shared secret to use with the specified accounting server.

6. From the Accounting Mode menu, select **Enable** to enable the RADIUS accounting mode.

7. Click the **Apply** button.

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

Table 86. RADIUS accounting server statistics

Field	Description
Accounting Server Address	The IP address of the supported RADIUS accounting server.
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 to this server. This number does not include retransmissions.
Accounting Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this 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 destined for this server that have not yet timed out or received a response.
Timeouts	The number of accounting time-outs to this server.

Table 86. RADIUS accounting server statistics

Field	Description
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

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

- Click the **Clear Counters** button to reset all statistics to their default value.
- Click **Update** to update the page with the latest information on the switch.

Configure TACACS+

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication**. Provides authentication during login and 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.

The TACACS+ folder contains links to the features described in the following sections.

- Configure TACACS+ on page 233
- TACACS+ Server Configuration on page 234

TACACS+ Configuration

The TACACS+ Configuration screen contains the TACACS+ settings for communication between the switch and the TACACS+ server you configure by using the inband management port.

To configure global TACACS+ settings:

1. Select **Security** > **Management Security** > **TACACS+** > **TACACS+ Configuration**.
2. In the Key String field, specify the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server.

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

3. In the Connection Timeout field, specify the maximum number of seconds allowed to establish a TCP connection between the switch and the TACACS+ server.

   The valid range is 1–30 seconds. Default is 5 seconds.

4. Click the **Apply** button.

TACACS+ Server Configuration

Use the TACACS+ Server Configuration screen to configure up to five TACACS+ servers with which the switch can communicate.

To configure TACACS+ server:

1. Select **Security** > **Management Security** > **TACACS+** > **Server Configuration**.

2. In the TACACS Server field, specify the IP address of the TACACS server.

3. In the Priority field, specify the priority for the TACAS+ server.

The priority determines the order in which the TACACS+ servers are contacted when attempting to authenticate a user. A value of 0 is the highest priority.

4. (Optionally) In the Port field, specify the authentication port value for TACAS+ server sessions.

If you do not specify a value, the switch uses the standard TCP port 49 for sessions with the server.

5. In the Key String field, specify the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server.

This key must match the encryption used on the TACACS+ server. The valid range is 0–128 characters.

6. (Optionally) In the Connection Timeout field, specify the amount of time that passes before the connection between the device and the TACACS+ server times out.

If you do not specify a value, the switch uses a default value of 5.

7. Click the **Apply** button.

Authentication List Configuration

Use the Authentication List screen to configure the default login list. A login list specifies one or more authentication methods to validate switch or port access for the admin user.

Note: Admin is the only user on the system and is assigned to a preconfigured list named defaultList, which you cannot delete.

HTTP Authentication List

Use the HTTP Authentication List to configure the default HTTP login list.

To change the HTTP authentication method for the defaultList:

1. Select **Security** > **Management Security** > **Authentication List** > **HTTP Authentication List**.

2. Select the check box next to the httpList name.

3. From the list in the **1** column, select the authentication method that should appear first in the selected authentication login list.

    If you select a method that does not time out as the first method, such as Local, no other method will be tried, even if you have specified more than one method. User authentication occurs in the order the methods are selected. Possible methods are as follows:

    • **Local**. The user's locally stored ID and password will be used for authentication. Since the local method does not time out, if you select this option as the first method, no other method will be tried, even if you have specified more than one method.

    • **RADIUS**. The user's ID and password will be authenticated using the RADIUS server. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user.

    • **TACACS+**. The user's ID and password will be authenticated using the TACACS+ server. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.

    • **None**. The authentication method is unspecified. This option is available only for Method 2 and Method 3.

4. From the list in the **2** column, select the authentication method, if any, that should appear second in the selected authentication login list.

    This is the method that is used if the first method times out. If you select a method that does not time out as the second method, the third method is not tried.

5. From the list in the **3** column, select the authentication method, if any, that should appear third in the selected authentication login list.

6. From the list in the **4** column, select the method, if any, that should appear fourth in the selected authentication login list.

This is the method that will be used if all previous methods time out.

7. Click the **Apply** button.

HTTPS Authentication List

Use the HTTPS Authentication List to configure the default login list for secure HTTP (HTTPS).

To configure the HTTPS authentication method for the defaultList:

1. Select **Security** > **Management Security** > **Authentication List** > **HTTPS Authentication List**.

2. Select the check box next to the httpsList name.

3. From the list in the **1** column, select the authentication method that should appear first in the selected authentication login list.

    If you select a method that does not time out as the first method, such as Local, no other method will be tried, even if you have specified more than one method. This parameter will not appear when you first create a new login list. User authentication occurs in the order the methods are selected. Possible methods are as follows:

    • **Local**. The user's locally stored ID and password will be used for authentication. Since the local method does not time out, if you select this option as the first method, no other method will be tried, even if you have specified more than one method.

    • **RADIUS**. The user's ID and password will be authenticated using the RADIUS server. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user.

    • **TACACS+**. The user's ID and password will be authenticated using the TACACS+ server. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.

    • **None**. The authentication method is unspecified. This option is only available for Method 2 and Method 3.

4. From the list in the **2** column, select the authentication method, if any, that should appear second in the selected authentication login list.

    This is the method that is used if the first method times out. If you select a method that does not time out as the second method, the third method is not tried.

5. From the list in the **3** column, select the authentication method, if any, that should appear third in the selected authentication login list.

6. From the list in the **4** column, select the method, if any, that should appear fourth in the selected authentication login list.

    This is the method that will be used if all previous methods time out.

7. Click the **Apply** button.

Dot1x Authentication List

The Dot1x authentication list defines the IEEE 802.1X authentication method used for the default list.

To change the Dot1x authentication method for the defaultList:

1. Select **Security** > **Management Security** > **Authentication List** > **Dot1x Authentication List**.

2. Select the check box next to the dot1xList name.

3. From the list in the **1** column, select the method that should appear first in the selected authentication login list.

   The options are:

   - **Local**. The user's locally stored ID and password will be used for authentication.
   - **Radius**. The user's ID and password will be authenticated using the RADIUS server instead of locally.
   - **None**. The user will not be authenticated.

4. Click the **Apply** button.

Smart Control Center Utility

Use the Smart Control Center (SCC) Control page to enable or disable the Smart Control Center Utility admin mode.

To configure the Smart Control Center (SCC) Utility

1. Select **Security** > **Management Security** > **SCC Control**
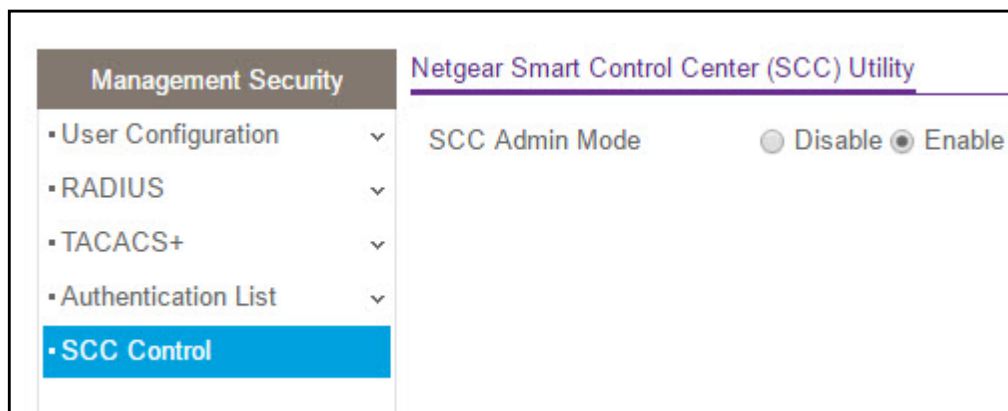
Figure 98. Smart Control Center Utility

2. If the **Disable** option is chosen, the SCC Utility will only be able to discover the switch, but will not be able to perform any action on the switch. This eliminates a security concern about the switch admin password contained in each NSDP packet. The factory default is Enable.

3. Click the **Apply** button. The updated configuration is sent to the switch. Configuration changes take effect immediately.

4. Click the **Cancel** button to cancel the configuration on the page and reset the data on the page to the latest value on the switch.

Configuring Management Access

From the Access menu, you can configure HTTP and secure HTTP access to the switch management interface. You can also configure access control profiles and access rules.

The Access menu contains links to the features described in the following sections.

- HTTP Configuration on page 238
- Secure HTTP Configuration on page 239
- Certificate Management on page 240
- Certificate Download on page 240
- Access Control on page 241

HTTP Configuration

Use the HTTP Configuration screen to configure the HTTP server settings on the system.

To configure the HTTP server settings:

1. Select **Security** > **Access > HTTP** > **HTTP Configuration**.
2. Enable or disable the Web Java mode.

   This applies to both secure and unsecure HTTP connections.

3. In the HTTP Session Soft Timeout field, specify the number of minutes an HTTP session can be idle before a timeout occurs. The value must be in the range of 0–60 minutes. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.

   After the session is inactive for the configured amount of time, the administrator is automatically logged out and must re-enter the password to access the management interface. A value of zero corresponds to an infinite time-out.

4. In the HTTP Session Hard Timeout field, specify 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 (0–168) hours. A value of zero corresponds to an infinite time-out. The default value is 24 hours.

5. In the Maximum Number of HTTP Sessions field, specify the maximum number of HTTP sessions that can exist at the same time.

6. Click the **Apply** button.

Secure HTTP Configuration

Secure HTTP enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. When you manage the switch by using the web management interface, secure HTTP can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks.

Use the HTTPS Configuration screen to configure the settings for HTTPS communication between the management station and the switch.

To configure HTTPS settings:

1. Select **Security** > **Access** > **HTTPS** > **HTTPS Configuration**.

2. Next to HTTPS Admin Mode, enable or disable the administrative mode of Secure HTTP.

   The default value is Disable. You can download SSL certificates only when the HTTPS Admin mode is disabled.

3. Next to SSL Version 3, enable or disable Secure Sockets Layer Version 3.0.

   The default value is Enable.

4. Next to TLS Version 1, enable or disable Transport Layer Security Version 1.0.

   The default value is Enable.

5. In the HTTPS Port field, specify the TCP port to use for HTTPS data.

   The value must be in the range of 1025–65535. Port 443 is the default value.

6. In the HTTPS Session Soft Timeout (Minutes) field, specify the number of minutes an HTTPS session can be idle before a time-out occurs.

   After the session is inactive for the configured amount of time, the administrator is automatically logged out and must re-enter the password to access the management interface. A value of zero corresponds to an infinite time-out. The valid range is 1—60 minutes. The default value is 5 minutes.

7. In the HTTPS Session Hard Timeout (Hours) field, specify the number of hours an HTTPS session can remain active, regardless of session activity.

   The value must be in the range of (1–168) hours. The default value is 24 hours.

8. In the Maximum Number of HTTPS Sessions field, specify the maximum number of HTTPS sessions that can be open at the same time.

   The value must be in the range of (0–4). The default value is 4.

9. Click the **Apply** button.

Certificate Management

Use this screen to generate or delete certificates.

To generate an SSL certificate:

1. Select **Security** > **Access > HTTPS** > **Certificate Management**.

    From the Certificate Present field, a Yes or No status displays.

2. In the Certificate Management area, select **Generate Certificates**.

3. Click the **Apply** button. The switch begins generating an SSL certificate.

4. The Certificate Generation Status field shows information about the progress.

To delete an SSL certificate:

1. Select **Security** > **Access > HTTPS** > **Certificate Management**.

    From the Certificate Present field, a Yes or No status displays.

2. In the Certificate Management area, select **Delete Certificates**.

3. Click the **Apply** button.

Certificate Download

For the web server on the switch to accept HTTPS connections from a management station, the web server needs a public key certificate. You can generate a certificate externally (for example, off-line) and download it to the switch.

Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.

To configure the certificate download settings for HTTPS sessions:

1. Select **Security** > **Access** > **HTTPS** > **Certificate Download**.

2. From the File Type list, select the type of SSL certificate to download, which can be one of the following:
    - **SSL Trusted Root Certificate PEM File**. SSL Trusted Root Certificate File (PEM Encoded).
    - **SSL Server Certificate PEM File**. SSL Server Certificate File (PEM Encoded).
    - **SSL DH Weak Encryption Parameter PEM File**. SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
    - **SSL DH Strong Encryption Parameter PEM File**. SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).

3. From the Server Address Type list, specify either IPv4 or DNS to indicate the format of the TFTP Server Address field.

   The default is IPv4.

4. In the TFTP Server IP field, specify the address of the TFTP server.

   The address can be an IP address in standard x.x.x.x format or a hostname. The hostname must start with a letter of the alphabet. Make sure that the software image or other file to be downloaded is available on the TFTP server.

5. Enter the path of the file which you want to download in the Remote File Path field.

   You can enter up to 96 characters. The factory default is blank.

6. In the Remote File Name field, specify the name of the file to download, including the path.

   You can enter up to 32 characters.

7. Select the Start File Transfer check box.

8. Click the **Apply** button.

   The file transfer starts. A status message displays during the transfer and upon successful completion of the transfer.

Access Control

Access control allows you to configure a profile and set access rules.

Access Profile Configuration

Use the Access Profile Configuration screen to set up a security access profile.

To configure an access profile:

1. Select **Security** > **Access** > **Access Control** > **Access Profile Configuration**.

2. In the Access Profile Name field, specify the name of the access profile to be added.

3. Select one of the following options:
   - **Activate Profile**. Activate an access profile.
   - **Deactivate Profile.** Deactivate an access profile.
   - **Remove Profile.** Remove an access profile. The access profile should be deactivated before removing the access profile.

4. Click the **Apply** button.

The following table describes the access profile status information and the profile summary information the screen displays.

Table 87. Access Profile Configuration

Field	Description
Packets Filtered	The number of packets filtered.
Profile Summary	
Rule Type	The action to be performed when the rules selected are matched.
Service Type	The policy is restricted by the management chosen from the list. Possible methods include HTTP, Secure HTTP (SSL), and SNMP.
Source IP Address	The Source IP Address of the client originating the management traffic.
Mask	The Source IP Address Mask of the client originating the management traffic.
Priority	The rule priority value. The rules are validated against the incoming management request in the ascending order of their priorities. If a rule matches, action is performed and subsequent rules below are ignored. For example, if a Source IP 10.10.10.10 is configured with priority 1 to permit, and Source IP 10.10.10.10 is configured with priority 2 to Deny, then access is permitted if the profile is active, and the second rule is ignored.

Access Rule Configuration

Use the Access Rule Configuration screen to add security access rules.

To configure access rules:

1. Select **Security** > **Access** > **Access Control** > **Access Rule Configuration**.
2. From the **Rule Type** field, select the action to be performed when the rules selected are matched.

   A *permit* rule allows access by traffic that matches the rule criteria. A *deny* rule blocks traffic that matches the rule criteria.

3. From the **Service Type** field, select the access method to which the rule is applied. THe policy is restricted by the management chosen from the menu. Possible access methods are:
   - HTTP
   - Secure HTTP (SSL)
   - SNMP
   - JAVA

4. In the **Source IP Address** field, specify the IP address of the client from which the management traffic originates
5. In the **Mask** field, specify the subnet mask of the client that originates the management traffic.
6. In the **Priority** field, assign a priority to the rule.

The rules are validated against the incoming management request in the ascending order of their priorities. If a rule matches, action is performed and subsequent rules below are ignored. For example, if a Source IP 10.10.10.10 is configured with priority 1 to permit, and Source IP 10.10.10.10 is configured with priority 2 to Deny, then access is permitted if the profile is active, and the second rule is ignored.

7. Click the **Apply** button.

Port Authentication

In port-based authentication mode, when 802.1X is enabled globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

The 802.1X network has three components:

- **Authenticators.** Specifies the port that is authenticated before permitting system access.
- **Supplicants.** Specifies the host connected to the authenticated port requesting access to the system services.
- **Authentication Server.** Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

The Port Authentication menu contains links to the features described in the following sections.

802.1X Configuration

Use the 802.1X Configuration screen to configure global port access control settings on the switch. The switch software supports.

To globally enable all 802.1X features:

1. Select **Security** > **Port Authentication** > **Basic** > **802.1X Configuration**.
2. Next to Port Based Authentication State, select **Enable**.

Note: If 802.1X is enabled, authentication is performed by a RADIUS server. This means the primary authentication method must be RADIUS. To set the method, select **Security** > **Management Security** > **Authentication List** and select **RADIUS** as method 1 for defaultList. For more information, see .

When port-based authentication is globally disabled, 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.

3. In the VLAN Assignment Mode field, select **Enable**.

    When enabled, this feature allows a port to be placed into a particular VLAN based on the result of the authentication or type of 802.1X authentication a client uses when it accesses the device. The authentication server can provide information to the device about which VLAN to assign the supplicant.

4. Next to Dynamic VLAN Creation Mode, select **Enable**.

    If RADIUS-assigned VLANs are enabled, the RADIUS server is expected to include the VLAN ID in the 802.1X tunnel attributes of its response message to the device. If dynamic VLAN creation is enabled on the device and the RADIUS-assigned VLAN does not exist, then the assigned VLAN is dynamically created. This implies that the client can connect from any port and can get assigned to the appropriate VLAN. This feature gives flexibility for clients to move around the network without much additional configuration required.

5. Next to EAPOL Flood Mode, select **Enable.**

    Extensible Authentication Protocol (EAP) over LAN (EAPOL) flood support is enabled on the switch.

6. Click the **Apply** button.

Port Authentication

Use the Port Authentication screen to enable and configure port access control on one or more ports.

To configure 802.1X settings for the port:

1. Select **Security** > **Port Authentication** > **Advanced** > **Port Authentication**.

Note: Use the horizontal scroll bar at the bottom of the browser to view all the fields on the Port Authentication screen.

---

2. Select one or more ports to configure.

For information about how to select and configure one or more ports, see <u>Configuring Interface Settings on page 28</u>.

3. Specify the following settings:

- **Port Control**. Defines the port authorization state. The control mode is set only if the link status of the port is link up. Select one of the following options:

    - **Auto**. The system automatically detects the mode of the interface.

    - **Authorized**. The system places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.

    - **Unauthorized**. The system denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface.

    - **MAC based**. This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses.

- **Guest VLAN ID**. Specify the VLAN ID for the guest VLAN. The valid range is 0–4093. The default value is 0. Enter 0 to reset the Guest VLAN ID on the interface. The guest VLAN allows the port to provide a distinguished service to unauthenticated users. This feature provides a mechanism to allow users access to hosts on the guest VLAN.

- **Guest VLAN Period**. Specify the number of seconds that the selected port remains in the quiet state following a failed authentication exchange. The guest VLAN timeout must be a value in the range of 1–300. The default value is 90.

- **Unathenticated VLAN ID**. Specify the VLAN ID of the unauthenticated VLAN for the selected port. The valid range is 0–3965. The default value is 0. Hosts that fail the authentication might be denied access to the network or placed on a VLAN created for unauthenticated clients. This VLAN might be configured with limited network access.

- **Periodic Reauthentication**. Select **Enable** to allow periodic reauthentication of the supplicant for the specified port.

- **Reauthentication Period**. Specify the amount of time, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthentication period must be a value in the range of 1–65535. The default value is 3600. Changing the value will not change the configuration until the **Submit** button is pressed. If this field is disabled, connected clients are not forced to reauthenticate periodically.

- **Quiet Period**. Specify the number of seconds that the port remains in the quiet state following a failed authentication exchange.While in the quite state, the port does not attempt to acquire a supplicant.

- **Resending EAP**. Specify the transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identify frame to the supplicant.

- **Max EAP Requests**. Specify the maximum requests for the selected port. The maximum requests value is the maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant.
- **Supplicant Timeout**. Specify 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.
- **Server Timeout**. Specify the amount of time that lapses before the switch resends a request to the authentication server.

4. Click the **Apply** button.

The following table describes the 802.1X status information available on the screen.

Table 88. Port Authentication Status Information

Field	Description
Control Direction	The control direction for the specified port, which is always Both. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator.The unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames). This field is not configurable.
Protocol Version	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.
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

To initialize the 802.1X state machine on a port:

1. Select the check box associated with the port to initialize.

2. Click the **Initialize** button.

    The 802.1X state machine on the selected interface is reset to the initialization state. Traffic sent to and from the port is blocked during the authentication process. This button is available only if the control mode is *auto*. When this button is clicked, the action is immediate. It is not required to click the Apply button for the action to occur.

To restart the 802.1X authentication process on a port:

1. Select the check box associated with the port to reauthenticate.

2. Click the **Reauthenticate** button.

    The selected port is forced to restart the authentication process.This button is available only if the control mode is *auto*. If the button is not selectable, it will be grayed out. When this button is pressed, the action is immediate. It is not required to click the Apply button for the action to occur.

Port Summary

Use the Port Summary screen to view summary information about the port-based authentication settings for each port.

To access the port Summary screen, select **Security** > **Port Authentication** > **Advanced** > **Port Summary**.

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

Table 89. IEEE 802.1X port summary information

Field	Description
Port	The port whose settings are displayed in the current table row.
Control Mode	The port authorization state. The control mode is only set if the link status of the port is link up. The possible field values are: • Auto**.** Automatically detects the mode of the interface. • Force Authorized**.** Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication. • Force Unauthorized**.** Denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface. • **MAC Based**. Selects MAC Based authentication.
Operating Control Mode	The control mode under which the port is actually operating. Possible values are: • ForceUnauthorized • ForceAuthorized • Auto • N/A: If the port is in detached state it cannot participate in port access control.

Table 89. IEEE 802.1X port summary information (continued)

Field	Description
Reauthentication Enabled	Displays if reauthentication is enabled on the selected port. This is a configurable field. The possible values are *true* and *false*. If the value is *true*, reauthentication will occur. Otherwise, reauthentication will not be allowed.
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 will be *N/A* since the port cannot participate in port access control.

Client Summary

This screen displays information about supplicant devices that are connected to the local authenticator ports. If there are no active 802.1X sessions, the table is empty.

To access the Client Summary screen, select **Security** > **Port Authentication** > **Advanced** > **Client Summary**. The Client Summary screen for the 802.1X feature displays.

The following table describes the fields on the Client Summary screen.

Table 90. IEEE 802.1X client summary information

Field	Description
Port	The port associated with the rest of the data in the row.
User Name	The name the client uses to identify itself as a supplicant to the authentication server.
Supplicant MAC Address	The MAC address of the supplicant that is connected to the port.
Session Time	The amount of time that has passed since the connected supplicant was granted access to the network through the authenticator port.
Filter ID	The policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID	The ID of the VLAN the supplicant was placed in as a result of the authentication process.
VLAN Assigned	The reason why the supplicant was placed in the VLAN.
Session Timeout	The reauthentication timeout period set by the RADIUS server to the supplicant device.
Termination Action	The termination action set by the RADIUS server that indicates the action that will take place once the supplicant reaches the session timeout value.

Traffic Control

From the Traffic Control menu, you can configure MAC Filters, Storm Control, Port Security, and Protected Port settings.

The Traffic Control menu contains links to the features described in the following sections.

MAC Filter Configuration

Use the MAC Filter Configuration screen to create MAC filters that limit the traffic allowed into and out of specified ports on the system.

To configure MAC filter settings:

1. Select **Security** > **Traffic Control** > **MAC Filter** > **MAC Filter Configuration**.
2. From the MAC Filter list, select Create Filter

   If no filters have been configured, this is the only option available.

3. From the VLAN ID list, select the VLAN to use with the MAC address to fully identify packets you want filtered.

   You can change this field only when the Create Filter option is selected from the MAC Filter menu.

4. In the MAC Address field, specify the MAC address of the filter in the format 00:01:1A:B2:53:4D.

   You can only change this field when you have selected the Create Filter option.

   You cannot define filters for the following MAC addresses:

   - 00:00:00:00:00:00
   - 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
   - 01:80:C2:00:00:20 to 01:80:C2:00:00:21
   - FF:FF:FF:FF:FF:FF

5. From the list of Source Port Members, select the ports to include in the inbound filter.

If a packet with the MAC address and VLAN ID you specify is received on a port that is not in the list, it will be dropped.

6. From the list of Destination Port Members, select the ports to include in the outbound filter. Packets with the MAC address and VLAN ID you selected will be transmitted only out of ports that are in the list. Destination ports can be included only in the Multicast filter.

7. Click the **Apply** button.

To delete a configured MAC filter:

1. In the MAC Filter list, select the filter to remove.

2. Click the **Delete** button.

MAC Filter Summary

Use the MAC Filter Summary screen to view the MAC filters that are configured on the system.

To display the MAC filter summary screen, select **Security** > **Traffic Control** > **MAC Filter** > **MAC Filter Summary**.

The following table describes the information displayed on the screen:

Table 91. MAC filter summary information

Field	Description
MAC Address	Identifies the MAC address that is filtered.
VLAN ID	The VLAN ID used with the MAC address to fully identify packets you want filtered. You can only change this field when you have selected the Create Filter option.
Source Port Members	The ports included in the inbound filter.
Destination Port Members	The ports included in the outbound filter.

Storm Control

A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources and/or cause the network to time out.

The switch measures the incoming broadcast/multicast/unknown unicast packet rate per port and discards packets when the rate exceeds the defined value. Storm control is enabled per interface, by defining the packet type and the rate at which the packets are transmitted.

To configure storm control settings:

1. Select **Security** > **Traffic Control** > **Storm Control**.

2. Select the check box next to the port to configure.

For information about how to select and configure one or more ports, see Configuring Interface Settings on page 28.

3. From the Ingress Control Mode list, select the mode of broadcast affected by storm control.

    •   **Disable**. Do not use storm control.

    •   **Unknown Unicast**. If the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

    •   **Multicast**. If the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

    •   **Broadcast**. If the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

4. When the selected ingress control mode is an option other than Disable, select **Enable** or **Disable** from the Status list to specify the administrative status of the mode.

5. In the Control Action mode list, select one of the following options:

    •   **None**. This is the default setting.

    •   **Trap**. If the threshold of the configured broadcast storm is exceeded, a trap is sent.

    •   **Shutdown**. If the threshold of the configured broadcast storm is exceeded, the port is shut down.

6. In the Threshold field, specify the maximum rate at which unknown packets are forwarded.

    The range is a percent of the total threshold between 0–100%. The default is 5%.

7. From the Flow Control list, select **Enable** or **Disable**.

8. Click the **Apply** button.

Port Security Configuration

Use the Port Security feature to lock one or more ports on the system. When a port is locked, only packets with an allowable source MAC addresses can be forwarded. All other packets are discarded.

To configure the global port security mode:

1. Select **Security** > **Traffic Control** > **Port Security** > **Port Security Configuration**.

2. In the Port Security Mode field, select the appropriate radio button to enable or disable port security on the switch. The default is **Disable**.

3. Click the **Apply** button.

The Port Security Violation table shows information about violations that occurred on ports that are enabled for port security. The following table describes the fields in the Port Security Violation table.

Table 92. Port security violation information

Field	Description
Port	Identifies the port where a violation occurred.
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.

Port Security Interface Configuration

A MAC address can be defined as allowable by one of two methods: dynamically or statically. Both methods are used concurrently when a port is locked.

Dynamic locking implements a first arrival mechanism for port security. You specify how many addresses can be learned on the locked port. If the limit has not been reached, then a packet with an unknown source MAC address is learned and forwarded normally. When the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

To configure port security settings:

1. Select **Security > Traffic Control > Port Security > Interface Configuration**.
2. Select the ports or LAGs to configure.

   For information about how to select and configure one or more ports or LAGs, see Configuring Interface Settings on page 28.

3. Specify the following settings:
   - **Port Security**. Enable or Disable the port security feature for the selected port. The default is Disable.
   - **Max Allowed Dynamically Learned MAC**. Specify the maximum number of dynamically learned MAC addresses on the selected interface.
   - **Max Allowed Statically Locked MAC**. Specify the maximum number of statically locked MAC addresses on the selected interface.
   - **Enable Violation Traps**. Enable or disable the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port. The default value is No.
4. Click the **Apply** button.

Security MAC Address

Use the Security MAC Address screen to convert a dynamically learned MAC address to a statically locked address.

To convert learned MAC addresses:

1. Select **Security** > **Traffic Control** > **Port Security** > **Security MAC Address**.
2. Select the Convert Dynamic Address to Static check box.
3. Use the Port List menu to select the interface for which you want to display data.
4. Click the **Apply** button.

    The Dynamic MAC Address entries are converted to Static MAC address entries in a numerically ascending order until the Static limit is reached.

The Number of Dynamic MAC Addresses Learned field displays the number of dynamically learned MAC addresses on a specific port.

To view dynamic MAC address table information for a port:

From the Port List list, select the port with the information to view.

The Dynamic MAC Address Table shows the MAC addresses and their associated VLANs learned on the selected port.

Table 93. Dynamic MAC address table information

Field	Description
VLAN ID	The VLAN ID corresponding to the Last Violation MAC address.
MAC Address	The MAC addresses learned on a specific port.

Protected Ports Membership

If a port is configured as protected, it does not forward traffic to any other protected port on the switch, but it will forward traffic to unprotected ports. Use the Protected Ports Membership screen to configure the ports as protected or unprotected.

To configure protected ports:

1. Select **Security** > **Traffic Control** > **Protected Ports**.
2. Click the box to display the available ports.
3. Click the box below each port to configure as a protected port.

    Protected ports are marked with a check mark. No traffic forwarding is possible between two protected ports.

4. Click the **Apply** button.

Configure Access Control Lists

Access control lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network. Switch software supports IPv4 and MAC ACLs.

To configure an ACL, first create an IPv4-based or MAC-based ACL ID. Then, create a rule and assign it to a unique ACL ID. Next, 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.

To view ACL configuration examples, see Access Control Lists on page 322.

The **ACL** configuration menu contains links to the features described in the following sections.

- ACL Wizard on page 254
- Basic
  - MAC ACL on page 258
  - MAC Rules on page 259
  - MAC Binding Configuration on page 261
  - MAC Binding Table on page 262
- Advanced
  - IP ACL on page 262
  - IP Rules on page 263
  - IP Extended Rules on page 265
  - IPv6 ACL on page 268
  - IPv6 Rules on page 269
  - IP Binding Configuration on page 271
  - IP Binding Table on page 272
  - VLAN Binding Table on page 272

ACL Wizard

The ACL Wizard helps you to create a simple ACL and apply it to the selected ports easily and quickly. First, you can select an ACL type. Then, you can add an ACL rule to this ACL, and a rule can be applied this ACL on the selected ports. The ACL Wizard allows you to create, but not modify, the ACL. For information about how to modify the rule, see Access Rule Configuration on page 242.

S3300 Gigabit Ethernet Stackable Smart Switch

To create an ACL by using the ACL Wizard:

1. Select **Security** > **ACL**> **ACL Wizard**.
2. In the ACL Type field, specify the ACL type used to create the ACL.

   You can select one type from 10 optional types:

   • **ACL Based on Destination MAC**. Use this to create an ACL based on the destination MAC address, destination MAC mask and VLAN.

   • **ACL Based on Source MAC**. Use this to create an ACL based on the source MAC address, source MAC mask and VLAN.

   • **ACL Based on Destination IPv4**. Use this to create an ACL based on the destination IPv4 address and IPv4 address mask.

   • **ACL Based on Source IPv4**. Use this to create an ACL based on the source IPv4 address and IPv4 address mask.

   • **ACL Based on Destination IPv6**. Use this to create an ACL based on the destination IPv6 prefix and IPv6 prefix length.

   • **ACL Based on Source IPv6**. Use this to create an ACL based on the source IPv6 prefix and IPv6 prefix length.

   • **ACL Based on Destination IPv4 L4 Port**. Use this to create an ACL based on the destination IPv4 layer4 port number.

   • **ACL Based on Source IPv4 L4 Port**. Use this to create an ACL based on the source IPv4 layer4 port number.

   • **ACL Based on Destination IPv6 L4 Port**. Use this to create an ACL based on the destination IPv6 layer4 port number.

   • **ACL Based on Source IPv6 L4 Port**. Use this to create an ACL based on the source IPv6 layer4 port number.

3. In the Sequence Number field, enter a whole number in the range of 1 to 2147483647 that will be used to identify the rule.
4. From the Action list, select the action to take if a packet matches the rule's criteria.

   If a packet matches a rule with a *permit* action, the packet is allowed to continue toward its destination. If a packet matches a rule with a *deny* action, the packet is dropped.

5. From the Match Every list, select **True** or **False**.

   If the Match Every value is True, all packets will match the rule and will be either permitted or denied. This option is exclusive to all other match criteria, so if Every is selected, no other match criteria can be configured. To configure specific match criteria, this option must be clear.

6. Specify the additional match criteria for the selected ACL type.

The rest of the rule match criteria fields available for configuration depend on the selected ACL type. For information about the possible match criteria fields, see Table 94.

Table 94. ACL fields according to selected ACL type

ACL Based On	Fields
Destination MAC	• Destination MAC. Specify the destination MAC address to compare against an ethernet frame. The valid format is (xx:xx:xx:xx:xx:xx). The BPDU keyword might be specified using a destination MAC address of 01:80:C2:xx:xx:xx. • Destination MAC Mask. Specify the destination MAC address mask specifying which bits in the destination MAC to compare against an ethernet frame. The valid format is (xx:xx:xx:xx:xx:xx). The BPDU keyword might be specified using a destination MAC mask of 00:00:00:ff:ff:ff. • VLAN. Specify the VLAN ID to match within the Ethernet frame.
Source MAC	• Source MAC. Specify the source MAC address to compare against an ethernet frame. The valid format is (xx:xx:xx:xx:xx:xx). • Source MAC Mask. 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). • VLAN. Specify the VLAN ID to match within the Ethernet frame.
Destination IPv4	• Destination IP Address. Specify the destination IP address. • Destination IP Mask. Specify the destination IP address mask.
Source IPv4	• Source IP Address. Specify the source IP address. • Source IP Mask. Specify the source IP address mask.
Destination IPv6	• Destination Prefix. Specify the destination prefix. • Destination Prefix Length. Specify the destination prefix length.
Source IPv6	• Source Prefix. Specify the source destination prefix. • Source Prefix Length. Specify the source prefix length.
Destination IPv4 L4 Port	• Destination L4 port (protocol). Specify the destination IPv4 L4 port protocol. • Destination L4 port (value). Specify the destination IPv4 L4 port value.
Source IPv4 L4 Port	• Source L4 port (protocol). Specify the source IPv4 L4 port protocol. • Source L4 port (value). Specify the source IPv4 L4 port value.
Destination IPv6 L4 Port	• Destination L4 port (protocol). Specify the destination IPv6 L4 port protocol. • Destination L4 port (value). Specify the destination IPv6 L4 port value.
Source IPv6 L4 Port	• Source L4 port (protocol). Specify the source IPv6 L4 port protocol. • Source L4 port (value). Specify the source IPv6 L4 port value.

7. In the Binding Configuration area, specify the packet filtering direction for an ACL in the Direction field.

   Only the inbound direction is valid for the switches.

8. In the Port Selection Table area, select each port and LAG to which the ACL is applied.

   In Figure 99 on page 257, the ACL rule is configured to check for packet matches on ports 8, 9, 13, and LAG 1. Packets that have a source address in the 192.168.3.0/24

network are permitted to be forwarded by the interfaces. All other packets are dropped because every ACL has an implicit *deny all* rule as the last rule.

Figure 99. ACL Wizard

9. Click the **Add** button.

To modify a rule:

1. Select check box associated with the rule to remove.
2. Update the match criteria as needed.
3. Click the **Apply** button.

To remove a rule:

1. Select check box associated with the rule to remove.
2. Click the **Delete** button.

MAC ACL

A MAC ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match.

There are multiple steps involved in defining a MAC ACL and applying it to the switch:

1. Create the ACL ID. See <u>MAC ACL on page 258</u>.
2. Create a MAC rule. See <u>MAC Rules on page 259</u>.
3. Associate the MAC ACL with one or more interfaces. See <u>MAC Binding Configuration on page 261</u>.

To add a MAC ACL:

1. Select **Security** > **Basic > MAC ACL**.

   The MAC ACL table displays the number of ACLs currently configured in the switch and the maximum number of ACLs that can be configured. The current size is equal to the number of configured IPv4 ACLs plus the number of configured MAC ACLs.

2. In the Name field, specify a name for the MAC ACL.

   The name string can include alphabetic, numeric, dash, underscore, or space characters only. The name must start with an alphabetic character.

3. Click the **Add** button.

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.

To change the name of a MAC ACL:

1. Select the check box next to the Name field for the ACL to modify.
2. In the Name field, specify the new name.
3. Click the **Apply** button**.**

To delete a MAC ACL:

1. Select the check box next to the Name field.
2. Click the **Delete** button.

MAC Rules

Use the MAC Rules screen to define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. A default *deny all* rule is the last rule of every list.

Note: To create a new MAC ACL, use the MAC ACL screen. See <u>MAC ACL on page 258</u>.

To add rules to a MAC ACL:

1. Select **Security** > **ACL** > **Basic** > **MAC Rules**.
2. From the ACL Name list, select the MAC ACL for which to create or update a rule.
3. In the Sequence Number field, specify ID for the rule.
4. Configure the ACL rule criteria by selecting options or specifying values as follows:
    - **Action**. Specify what action should be taken if a packet matches the rule's criteria:
        - **Permit**. Forwards packets that meet the ACL criteria.
        - **Deny**. Drops packets that meet the ACL criteria.
    - **Assign Queue**. Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Enter an identifying number from 0–7 in this field.
    - Mirror Interface. Specifies the specific egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch. This field cannot be set if a redirect interface is already configured for the ACL rule. This field is visible for a Permit action.
    - **Redirect Interface**. Specifies the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device.
    - **Match Every**. Requires a packet to match the criteria of this ACL. Select True or False from the drop-down menu. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.
    - **CoS**. Requires a packet's class of service (CoS) to match the CoS value listed here. Enter a CoS value between 0–7 to apply this criteria.
    - **Destination MAC**. Requires an Ethernet frame's destination port MAC address to match the address listed here. Enter a MAC address in this field. The valid format is xx:xx:xx:xx:xx:xx.
    - **Destination MAC Mask**. If desired, enter the MAC Mask associated with the Destination MAC to match. The MAC address mask specifies which bits in the destination MAC to compare against an Ethernet frame. Use Fs and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is 00:00:ff:ff:ff:ff, all

MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). A MAC mask of 00:00:00:00:00:00 matches a single MAC address.

- **EtherType Key**. Requires a packet's EtherType to match the EtherType you select. Select the EtherType value from the drop-down menu. If you select User Value, you can enter a custom EtherType value.

- **EtherType User Value**. This field is configurable if you select User Value from the EtherType drop-down menu. The value you enter specifies a customized EtherType to compare against an Ethernet frame. The valid range of values is 0x0600–0xFFFF.

- **Source MAC**. Requires a packet's source port MAC address to match the address listed here. Enter a MAC address in the this field. The valid format is xx:xx:xx:xx:xx:xx.

- **Source MAC Mask**. If desired, enter the MAC mask for the source MAC address to match. Use Fs and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. The valid format is xx:xx:xx:xx:xx:xx. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.

- **VLAN**. Requires a packet's VLAN ID to match the ID listed here. Enter the VLAN ID to apply this criteria. The valid range is 1–4093.

- **Logging**. When set to Enable, logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was hit during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is only supported for a Deny action.

5. Click the **Add** button.

To change the match criteria for a rule:

1. Select the check box associated with the rule.
2. Modify the fields as desired.
3. Click the **Apply** button.

To delete a rule:

1. Select the check box associated with the rule to remove.
2. Click the **Delete** button.

MAC Binding Configuration

When an ACL is bound to an interface, all the rules that have been defined are applied to the selected interface. Use the MAC Binding Configuration screen to assign MAC ACL lists to ACL priorities and interfaces.

To configure MAC ACL interface bindings:

1. Select **Security** > **ACL** > **Basic** > **MAC Binding Configuration**.
2. From the ALC ID menu, select the MAC ACL to bind to one or more interfaces.

   The packet filtering direction for ACL is Inbound, which means the MAC ACL rules are applied to traffic entering the port.

3. Specify an optional sequence number to indicate the order of this access list relative to other access lists already assigned to this interface and direction.

   A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction will be used. The valid range is 1–4294967295.

4. Click the appropriate selection to expose the available ports or LAGs.
   - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that a check mark displays in the box.
   - To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. A check mark in the box indicates that the ACL is applied to the interface.

5. Click the **Apply** button.

The Interface Binding Status section on the MAC Binding Configuration screen displays the following information:

- **Interface**. The interface associated with the rest of the data.
- **Direction**. The packet filtering direction for ACL.
- **ACL Type**. The type of ACL assigned to selected interface and direction.
- **ACL ID**. The ACL number or name 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.

MAC Binding Table

Use the MAC Binding Table screen to view or delete the MAC ACL bindings.

The following table describes the information displayed in the MAC Binding Table.

Table 95. MAC binding table information

Field	Description
Interface	The interface to which the MAC ACL is bound.
Direction	The packet filtering direction for ACL. The only valid direction is Inbound, which means the MAC ACL rules are applied to traffic entering the port.
ACL Type	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 No	The sequence number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

To delete a MAC ACL-to-interface binding:

1. Select **Security** > **ACL** > **Basic** > **Binding Table**.
2. Select the check box next to the interface associated with the MAC ACL.
3. Click the **Delete** button.

IP ACL

IP ACLs allow network managers to define classification actions and rules for specific ingress ports. Packets can be filtered on ingress (inbound) ports only. If the filter rules match, then some actions can be taken, including dropping the packet or disabling the port. For example, a network administrator defines an ACL rule that says port number 20 can receive TCP packets. However, if a UDP packet is received the packet is dropped.

ACLs are composed of access control entries (ACE), or rules, that consist of the filters that determine traffic classifications.

Use the IP ACL screen to add or remove IP-based ACLs.

To configure an IP ACL:

1. Select **Security** > **ACL** > **Advanced** > **IP ACL**.

   The IP ACL area shows the current size of the ACL table compared to the maximum size of the ACL table. The current size is equal to the number of configured IPv4 ACLs plus the number of configured MAC ACLs. The maximum size is 100.

2. In the IP ACL ID field, specify the ACL ID. The ID is an integer in the following range:
   - **1–99**. Creates an IP Standard ACL, which allows you to permit or deny traffic from a source IP address.

- **100–199**. Creates an IP extended ACL, which allows you to permit or deny specific types of Layer 3 or Layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the standard IP ACL.

3. Click the **Add** button.

   Each configured ACL displays the following information:

   - **Rules**. The number of rules currently configured for the IP ACL.
   - **Type**. Identifies the ACL as either a standard or extended IP ACL.

To delete an IP ACL:

1. Select the check box next to the IP ACL ID field.
2. Click the **Delete** button.

# IP Rules

Use the IP Rules screen to define rules for IP-based standard ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: There is an implicit deny all rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit "deny all" rule applies and the packet is dropped.

To add IP rules:

1. Select **Security** > **ACL** > **Advanced** > **IP Rules**.

   In the following figure, an IP ACL exists, and one rule has been configured.

Figure 100. ACL IP Rules

2. From the ACL ID list, select the IP ACL for which to create a rule.

3. Click the **Add** button.

   The screen refreshes, and additional fields appear.

Standard ACL Rule Configuration(1-99)

ACL ID   1

Rule ID   0

Action   ○ Permit   Egress Queue   ⌄ (0-6)
                    ◉ Deny
Logging   ◉ Disable   ○ Enable
Match Every   ◉ Disable   ○ Enable
Mirror Interface   ⌄
Redirect Interface ⌄
Src IP Address
Src IP Mask

Figure 101. Standard ACL Rule Configuration

4. In the Sequence Number field, specify a number in the range from 1 to 2147483647 to identify the IP ACL rule.

5. Select or specify values for one or more of the following match criteria:

   • **Sequence Number**. Specify a number in the range of 1 to 2147483647 to identify the IP ACL rule. You can create up to 50 rules for each ACL.

   • **Action**. Select the ACL forwarding action, which is one of the following:

      - **Permit**. Forward packets which meet the ACL criteria.

      - **Deny**. Drop packets which meet the ACL criteria.

   • **Egress Queue**. The hardware egress queue identifier used to handle all packets matching this ACL rule.

   • **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, then 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.

   • **Match Every**. Require a packet to match the criteria of this ACL. Select **True** or **False** from the drop-down list. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.

- **Src IP Address**. Require a packet's source IP address to match the address listed here. Enter an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's source IP Address.

- **Src IP Mask**. Specify the source IP address wildcard mask. Wild card masks determine which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, enter 0.0.0.255 in the Source IP Mask field. This field is required when you configure a source IP address.

6. Click the **Apply** button.

To modify the match criteria for an ACL rule:

1. From the ACL Name list on the IP Rules screen, select the ACL that includes the rule to update.

2. In the Basic ACL Rule Table, click the rule ID.

   The rule ID is a hyperlink to the Standard ACL Rule Configuration screen.

3. Modify the ACL rule information.

4. Click the **Apply** button.

To delete and IP ACL rule:

1. In the Basic ACL Rule Table on the IP Rules screen, select the check box associated with the rule to remove.

2. Click the **Delete** button.

IP Extended Rules

Use the IP Extended Rules screen to define rules for IP-based extended ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: There is an implicit *deny all* rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit deny all rule applies and the packet is dropped.

To add rules to an IP ACL:

1. Select **Security** > **ACL** > **Advanced** > **IP Extended Rules**.

2. In the ACL ID/Name list, select the ACL to add the rule to.

3. Click the **Add** button.

The screen displays the extended ACL rule configuration fields.

Figure 102. Extended ACL Rule Configuration

4. Next to Sequence Number, specify a number in the range of 1 to 2147483647 to identify the IP ACL rule.

   You can create up to 50 rules for each ACL.

5. Select or specify values for one or more of the following match criteria:

   - **Action**. Select the ACL forwarding action, which is one of the following:

     - **Permit**. Forwards packets which meet the ACL criteria.

     - **Deny**. Drops packets which meet the ACL criteria.

   - **Egress Queue**. Specify the hardware egress queue identifier used to handle all packets matching this ACL rule.

   - **Match Every**. Require a packet to match the criteria of this ACL. Select True or False from the drop-down menu. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.

   - **Protocol Type**. Require a packet's protocol to match the protocol listed here. Select a type from the drop-down menu or enter the protocol number in the available field.

   - **Src IP Address**. Require a packet's source IP address to match the address listed here. Type an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's source IP Address.

   - **Src IP Mask**. Specify the source IP address wildcard mask. Wild card masks determines which bits are used and which bits are ignored. A wild card mask of

255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, you type 0.0.0.255 in the Source IP Mask field. This field is required when you configure a source IP address.

- **Src L4 Port**. Require a packet's TCP/UDP source port to match the port listed here. Click Complete one of the following fields:

  - **Source L4 Keyword**. Select the desired L4 keyword from a list of source ports on which the rule can be based.

  - **Source L4 Port Number**. If the source L4 keyword is Other, enter a user-defined Port ID by which packets are matched to the rule.

- **Dst IP Address**. Require a packet's destination port IP address to match the address listed here. Enter an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's destination IP Address.

- **Dst IP Mask**. Specify the destination IP address wildcard mask. Wild card masks determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, you type 0.0.0.255 in the Source IP Mask field. This field is required when you configure a source IP address.

- **Dst L4 Port**. Require a packet's TCP/UDP destination port to match the port listed here. Complete one of the following fields:

  - **Destination L4 Keyword**. Select the desired L4 keyword from a list of destination ports on which the rule can be based.

  - **Destination L4 Port Number**. If the destination L4 keyword is Other, enter a user-defined Port ID by which packets are matched to the rule.

- **Service Type**. Select one of the Service Type match conditions for the extended IP ACL rule. The possible values are IP DSCP, IP precedence, and IP TOS, which are alternative ways of specifying a match criterion for the same Service Type field in the IP header, however each uses a different user notation. After you select the service type, specify the value associated with the type.

  - **IP DSCP**. Specify the IP DiffServ Code Point (DSCP) value. The DSCP is defined as the high-order six bits of the Service Type octet in the IP header. Select an IP DSCP value from the menu. To specify a numeric value in the available field, select Other from the menu and type an integer from 0 to 63 in the field.

  - **IP Precedence**. The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 7.

  - **IP TOS Bits**. Matches on the Type of Service bits in the IP header when checked. In the first TOS field, specify the two-digit hexadecimal TOS number. The second field is for the TOS Mask, which specifies the bit positions that are used for

comparison against the IP TOS field in a packet. The TOS Mask value is a two-digit hexadecimal number from 00 to ff, representing an inverted (wildcard) mask. The zero-valued bits in the TOS Mask denote the bit positions in the TOS Bits value that are used for comparison against the IP TOS field of a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of a0 and a TOS Mask of 00.

6. Click the **Apply** button.

To modify the match criteria for an ACL rule:

1. From the ACL Name list on the Extended ACL Rules screen, select the ACL that includes the rule to update.

2. In the Extended ACL Rule Table, click the rule.

   The rule is a hyperlink to the Extended ACL Rule Configuration screen.

3. Modify the ACL rule information.

4. Click the **Apply** button.

To delete and IP ACL rule:

1. In the Extended ACL Rule Table on the IP Rules screen, select the check box associated with the rule to remove.

2. Click the **Delete** button.

IPv6 ACL

An IPv6 ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match. On this menu, the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the IPv6 ACL are specified/created using the IPv6 Rules screen.

To add an IPv6 ACL:

1. Select **Security** > **ACL** > **Advanced** > **IPv6 ACL**.

   The current number of the IP ACLs configured on the switch is displayed in the Current Number of ACL area. The maximum number of IP ACLs that can be configured on the switch is displayed in the Maximum ACL field, depending on the hardware. The name of IPv6 ACL can be configured in IPv6 ACL field. The number of the rules associated with the IP ACL is displayed in the Rules field. The ACL type is IPv6 ACL and displayed in the Type field.

2. In the IPv6 ACL field, specify a name to identify the IPv6 ACL.

3. Click the **Add** button.

To delete an IPv6 ACL:

1. Select the check box associated with the ACL.

2. Click the **Delete** button.

IPv6 Rules

Use the IPv6 Rules screen to configure the rules for the IPv6 Access Control Lists. The IPv6 Access Control Lists are created using the IPv6 Access Control List Configuration screen. By default, no specific value is in effect for any of the IPv6 ACL rules.

To add a rule to an IPv6 ACL:

1. Select **Security** > **ACL** > **Advanced** > **IPv6 Rules**.

2. In the ACL Name list, select the name of the ACL to add a rule to.

3. Click the **Add** button.

   The screen displays the IPv6 ACL Rule Configuration fields.

Figure 103. IPv6 ACL Rule Configuration

4. Next to Sequence Number, specify a number in the range of 1 to 2147483647 to identify the IPv6 ACL rule.

   You can create up to 50 rules for each ACL.

5. Select or specify values for one or more of the following match criteria:

   • **Rule ID**. Enter a whole number in the range of 1 to 2147483647 that will be used to identify the rule. An IPv6 ACL can have up to 50 rules.

   • **Action**. Specify what action should be taken if a packet matches the rule's criteria. The choices are Permit or Deny.

- **Logging**. When set to Enable, logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, then 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**. Specifies the hardware egress queue identifier used to handle all packets matching this IPv6 ACL rule. The valid range of Queue IDs is from 0 to 6. This field is visible for a Permit Action.

- **Mirror Interface**. Specifies the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. This field cannot be set if a Redirect Interface is already configured for the ACL rule. This field is visible for a Permit action.

- **Redirect Interface**. Specifies the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field cannot be set if a Mirror Interface is already configured for the ACL rule. This field is visible for a Permit Action.

- **Match Every**. Select true or false from the pull down menu. True signifies that all packets will match the selected IPv6 ACL and Rule and will be either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria will not be offered. To configure specific match criteria for the rule, remove the rule and recreate it, or reconfigure Match Every to False for the other match criteria to be visible.

- **Protocol**. There are two ways to configure IPv6 protocol:

  - Specify an integer ranging from 0 to 255 after selecting protocol keyword "other". This number represents the IPv6 protocol.

  - Select name of a protocol from the existing list of IPv6, ICMPv6, TCP, and UDP.

- **Source Prefix/Prefix Length**. Specify IPv6 Prefix combined with IPv6 Prefix length of the network or host from which the packet is being sent. Prefix length can be in the range (0 to 128).

- **Source L4 Port**. Specify a packet's source layer 4 port as a match condition for the selected IPv6 ACL rule. Source port information is optional. Source port information can be specified in two ways:

  - Select keyword "other" from the drop-down menu and specify the number of the port in the range from 0 to 65535.

  - Select one of the keyword from the list: DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

- **Destination Prefix/Prefix Length**. Enter up to 128-bit prefix combined with prefix length to be compared to a packet's destination IP Address as a match criteria for the selected IPv6 ACL rule. Prefix length can be in the range (0 to 128).

- **Destination L4 Port**. Specify a packet's destination layer 4 port as a match condition for the selected IPv6 ACL rule. Destination port information is optional. Destination port information can be specified in two ways:

- Select keyword "other" from the drop-down menu and specify the number of the port in the range from 0 to 65535.

- Select one of the keyword from the list: DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

- **Flow Label**. Flow label is 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers. Flow label can be specified within the range (0 to 1048575).

- **IPv6 DSCP Service**. Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IPv6 header. This is an optional configuration. Enter an integer from 0 to 63. The IPv6 DSCP is selected by possibly selection one of the DSCP keyword from a drop-down menu. If a value is to be selected by specifying its numeric value, then select the **Other** option in the drop-down menu and a text box will appear where the numeric value of the DSCP can be entered.

6. Click the **Apply** button.

To delete an IPv6 rule:

1. On the IPv6 Rules screen in the ACL Name list, select the name of the ACL that includes the rule to remove.

2. In the IPv6 Rule Table, select the check box of the rule to delete.

3. Click the **Delete** button.

IP Binding Configuration

When an ACL is bound to an interface, all the rules that have been defined are applied to the selected interface. Use the IP Binding Configuration screen to assign ACL lists to ACL Priorities and Interfaces.

To bind an IP ACL to one or more interfaces:

1. Select **Security** > **ACL** > **Advanced** > **IP Binding Configuration**.

2. From the ACL ID list, select an existing IP ACL in which you want to add an IP ACL interface binding.

   The packet filtering direction for ACL is Inbound, which means the IP ACL rules are applied to traffic entering the port.

3. (Optionally) In the Sequence Number field, specify a 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, then the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, then a sequence number that is one greater than the highest sequence

number currently in use for this interface and direction will be used. The valid range is 1–4294967295.

4. Click the appropriate icon to expose the available ports or LAGs.

    • To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that a check mark displays in the box.

    • To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. A check mark in the box indicates that the ACL is applied to the interface.

5. Click the **Apply** button.

IP Binding Table

Use the IP Binding Table screen to view or delete the IP ACL bindings.

The following table describes the information displayed in the IP binding table.

Table 96. IP binding table information

Field	Description
Interface	The interface to which the IP ACL is bound.
Direction	Specifies the packet filtering direction for ACL. The only valid direction is Inbound, which means the IP ACL rules are applied to traffic entering the port.
ACL Type	The type of ACL assigned to selected interface and direction.
ACL ID	The ACL Number identifying the ACL assigned to selected interface and direction.
Seq No.	The Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

To delete an IP ACL binding:

1. Select **Security** > **ACL** > **Advanced** > **Binding Table**.

2. Select the check box associated with the ACL-to-interface binding to remove.

3. Click the **Delete** button.

VLAN Binding Table

Use the VLAN binding table screen to associate an ACL with a VLAN. When an ACL is associated with a VLAN, it is applied to all interfaces that are members of the VLAN.

To configure an ACL-to-VLAN binding:

1. Select **Security** > **ACL** > **Advanced** > **VLAN Binding Table**.

2. In the VLAN ID field, specify a VLAN ID for ACL mapping.

3. In the Direction field, select **In Bound**.

The IP ACL rules are applied to traffic entering the port.

4. (Optionally) In the Sequence Number field, specify the sequence number of the access lists.

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

5. From the ACL Type list, select the type of ACL:
    *   IP ACL
    *   MAC ACL
    *   IPv6 ACL

6. From the ACL ID list, select the ID of the ACL to bind to the specified VLAN.

    The ACL ID field displays all the ACLs configured, depending on the ACL Type selected.

7. Click the **Add** button.

To delete a VLAN binding:

1. Select the check box next to the VLAN with the ACL binding to remove.
2. Click the **Delete** button.

7

Maintenance

Use the features available from the Maintenance tab to help you manage the switch. The Maintenance tab contains links to the features described in the following sections.

Reset

The Reset menu contains links to the features described in the following sections.

- Device Reboot on page 275
- Factory Default on page 275

Device Reboot

Use the Device Reboot screen to reboot the switch.

To reboot the switch:

1. Select **Maintenance** > **Reset** > **Device Reboot**.
2. In the **Reboot Unit No**. field, select the unit to reset. When multiple units are connected in a stack, select **All** to reset all the units in the stack (in other words, the whole stack) or select the unit number to reset only the specific unit.
3. Select the check box.
4. Click the **Apply** button.

   The switch resets immediately. The management interface is not available until the switch completes the boot cycle. After the switch resets, the login screen displays.

Factory Default

Use the Factory Default screen to reset the system configuration to the factory default values.

Note: If you reset the switch to the default configuration, the IP address is reset to 192.168.0.239, and the DHCP client is enabled. If you loose network connectivity after you reset the switch to the factory defaults, see Connect the Switch to the Network on page 12.

To reset the switch to the factory default settings:

1. Select **Maintenance** > **Reset** > **Factory Default**.

Factory Default

Check this box and click APPLY above to return all configuration settings to default values ☐
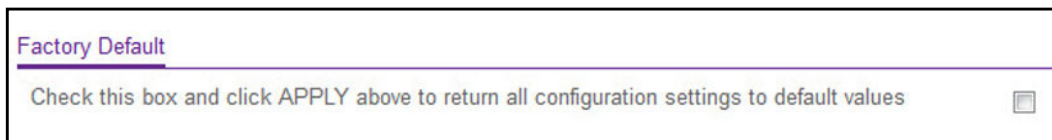
Figure 104. Factory Default

2. Select the check box on the screen.

---

3. Click the **Apply** button.

   The switch resets immediately.

Export (Upload) a File From the Switch

The switch supports system file exports (uploads) from the switch to a remote system by using either TFTP or HTTP.

The Export menu contains links to the features described in the following sections.

Export a File to the TFTP Server

Use the TFTP File Export screen to export (upload) configuration (ASCII), log (ASCII), and image (binary) files from the switch to a TFTP server on the network.

To export a file from the switch to the TFTP server:

1. Select **Maintenance** > **Export** > **TFTP File Export**.
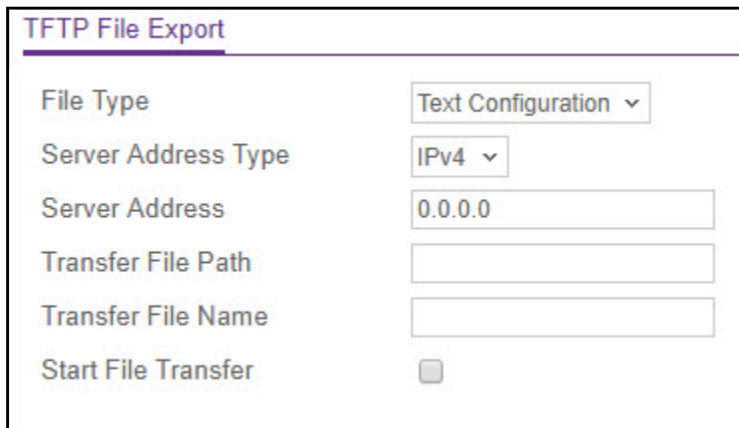
Figure 105. TFTP File Export

2. From the File Type list, specify the type of file you want to export. The factory default is **Text Configuration**.
   - **Text Configuration**. Retrieve the stored text configuration.
   - **Error Log**. Retrieve the system error (persistent) log, sometimes referred to as the event log.
   - **Trap Log**. Retrieve the system trap records.
   - **Buffered Log**. Retrieve the system buffered (in-memory) log.

- **Tech Support**. Retrieve the tech support file, which contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
- **Crash Logs**. Specify crash logs to retrieve them.

3. From the **Server Address Type** list, select the format to use for the address you type in the TFTP Server Address field. The default is **IPv4**.

- **IPv4**. Indicates that the TFTP server address is an IP address in dotted-decimal format.
- **DNS**. Indicates that the TFTP server address is a host name.

4. In the **Server Address** field, specify the IP address or host name of the TFTP server.

The address you type must be in the format indicated by the TFTP server address type.

5. In the **Transfer File Path** field, specify the path on the TFTP server where you want to put the file.

You can enter up to 32 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.

6. In the **Transfer File Name** field, specify a destination filename for the file to export.

You can enter up to 32 characters. The transfer fails if you do not specify a filename.

7. Select the **Start File Transfer** check box.

8. Click the **Apply** button.

The file transfer begins.

Note: The file transfer will not begin until you click **Apply**.

The last row of the table displays information about the file transfer progress. The screen refreshes automatically until the file transfer completes or fails.

HTTP File Export

Use the HTTP File Export screen to export (upload) files of various types from the switch to the management system through an HTTP session by using your web browser.

To export a file from the switch to another system by using HTTP:

1. Select **Maintenance** > **Export** > **HTTP File Export**.
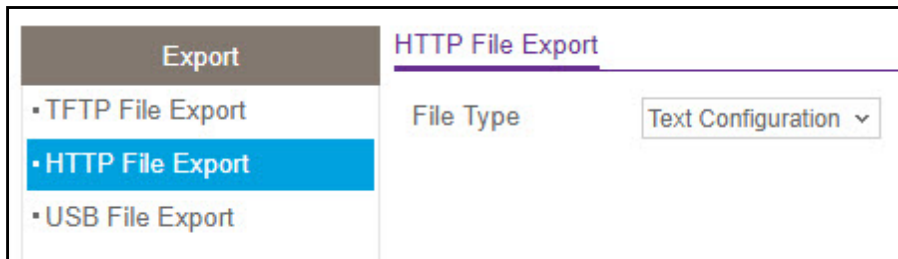
Figure 106. HTTP File Export

2. From the File Type list, specify what type of file you want to export from the switch. The factory default is **Text Configuration**.

   • **Text Configuration**. A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for the switch to understand. The most common usage of text-based configuration is to export a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.

   • **Tech Support**. The tech support file is a text-base file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.

   • **Crash Logs**. Specify crash logs to retrieve them.

3. Click the **Apply** button.

   A window displays to allow you to open the text file on the management system or to save the image or text file to the management system.

USB File Export

Use the USB File Export screen to export (upload) files of various types from the switch to a USB device.

To access the USB File Export page, click **Maintenance** > **Export** > **USB File Export.** The following page is displayed.

Figure 107. USB File Export

To export a file from the switch to a USB device:

1. Select **Maintenance** > **Export** > **USB File Export**.

2. From the **File Type** list, specify what type of file you want to export from the switch. The factory default is **Text Configuration**.

    •   **Text Configuration**. A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for the switch to understand. The most common usage of text-based configuration is to export a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.

3. In the **File Path** field, enter the path for the file to export. You may enter up to 139 characters. The factory default is blank.

4. In the **USB File** field, specify a destination filename for the file to export.

    You can enter up to 32 characters. The factory default is blank. The transfer fails if you do not specify a filename.

5. Click the **Apply** button. The file transfer begins.

The last row of the table displays non-configurable information about the progress of the file transfer. This information is displayed only after the file transfer process starts.

Download

The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.

The **Download** menu contains links to the features described in the following sections.

TFTP File Download

Use the Download File to switch screen to download device software, the image file, the configuration files, and SSL files from a TFTP server 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.

You can also download files by using HTTP. See for additional information.

Downloaded code is validated with a CRC check and a version check to protect against download of malicious code. Export of image file (.stk) is not allowed.

To download a file to the switch from a TFTP server:

1. Select **Maintenance** > **Download** > **TFTP File Download**.

Figure 108. TFTP File Download

2. From the **File Type** list, specify what type of file you want to download to the switch. The factory default is **Software**.

   - **Software**. The system software image (STK) that is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the upgrade process.

   - **Text Configuration**. A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for the switch to understand. The most common usage of text-based configuration is to export a working configuration from a device, edit it offline to personalize it for another

---

similar device (for example, change the device name, serial number, IP address), and download it to that device.

- **SSL Trusted Root Certificate PEM File**. SSL Trusted Root Certificate File (PEM Encoded).

- **SSL Server Certificate PEM File**. SSL Server Certificate File (PEM Encoded).

- **SSL DH Weak Encryption Parameter PEM File**. SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).

- **SSL DH Strong Encryption Parameter PEM File**. SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).

Note: We recommended that you do not overwrite the active image. The system will display a warning that you are trying to overwrite the active image.

Note: To download SSH key files, SSH must be administratively disabled, and there can be no active SSH sessions.

Note: To download SSL PEM files, SSL must be administratively disabled, and there can be no active SSH sessions.

3. The **Image Name** field is visible only when **File Type - Software** is selected. From the **Image Name** field, select one of the images from the list.
    - **image1**—Select **image1** to download image1.
    - **image2**—Select **image2** to download image2.

4. From the **Server Address Type** field, specify the format for the address you type in the TFTP Server Address field. The factory default is **IPv4**.
    - **IPv4**. Indicates the TFTP server address is an IP address in dotted-decimal format.
    - **DNS**. Indicates the TFTP server address is a hostname.

    Note: During the file transfer, the DNS name will be automatically replaced with the IP address.

5. In the **TFTP Server IP** field, specify the IP address or hostname of the TFTP server.

    The address you type must be in the format indicated by the TFTP Server Address Type. The factory default is the IPv4 address 0.0.0.0.

6. In the **Transfer File Path** field, specify the path on the TFTP server where the file is located that you want to download. The factory default is blank.

    Enter up to 160 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.

7. In the **Remote File Name** field, specify the name of the file to download from the TFTP server. You can enter up to 32 characters. A filename cannot include a space or the following symbols: '\/:*?"<>|'. The factory default is blank.

8. Select the **Start File Transfer** check box to initiate the file export.

Note: The file transfer will not begin until you click **Apply**.

9. Click the **Apply** button to begin the file transfer.

    The last row of the table displays information about the progress of the file transfer. The screen refreshes automatically until the file transfer completes or fails.

    To activate a software image that you download to the switch, see File Management on page 285.

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

HTTP File Download

Use the HTTP File Download screen to download files of various types to the switch through an HTTP session by using your web browser.

To download a file to the switch by using HTTP:

1. Select **Maintenance > Download > HTTP File Download**.
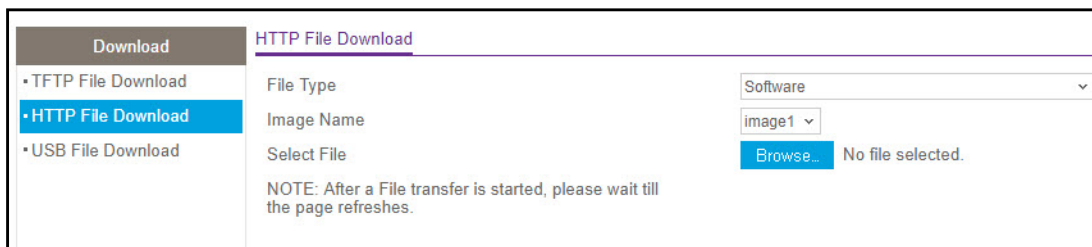
Figure 109. HTTP File Download

2. From the **File Type** list, specify the type of file to download to the switch. The factory default is **Software**.

    *   **Software**. The system software (STK) image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy; the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process.

    *   **Text Configuration**. A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for the switch to understand. The most common usage of text-based configuration is to export a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name, serial number, IP address), and download it to that device.

    *   **SSL Trusted Root Certificate PEM File**. SSL Trusted Root Certificate File (PEM Encoded).

    *   **SSL Server Certificate PEM File**. SSL Server Certificate File (PEM Encoded).

- **SSL DH Weak Encryption Parameter PEM File**. SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
- **SSL DH Strong Encryption Parameter PEM File**. SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).

Note: To download SSH key files, SSH must be administratively disabled, and there can be no active SSH sessions.

Note: To download SSL PEM files, SSL must be administratively disabled, and there can be no active SSH sessions.

3. The **Image Name** field is visible only when **File Type - Software** is selected. From the **Image Name** field, select one of the images from the list.
   - **image1**. Select **image1** to download image1.
   - **image2**. Select **image2** to download image2.

Note: Do not overwrite the active image. If you attempt to do this, the system will display a warning.

4. Next to **Select File**, click the **Browse** button to locate the file you want to download. Give the name, along with the path for the file you want to download. The factory default is blank.

5. Click the **Apply** button.

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.

Note: After the text configuration file is downloaded, the stack applies the configuration automatically.

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

USB File Download

Use the USB File Download screen to download a file to the switch from a USB device.

To access the USB File Download page, click **Maintenance** > **Download** > **USB File Download.** The following page is displayed.

Figure 110. USB File Download

To download a file to the switch from a USB device:

1. From the **File Type** list, specify the type of file to download to the switch:

    • **Software**. The STK system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy; the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process. The default is **Software**.

    • **Text Configuration**. A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for the switch to understand. The most common usage of text-based configuration is to export a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name, serial number, IP address), and download it to that device.

2. The **Image Name** field is only visible when the selected **File Type** is **Software**. If you are downloading a switch image (**Software**), use the **Image Name** list to select the software image, image1 or image2, to download to the switch.

3. In the **File Path** field, type the path for the file you want to download. You may enter up to 139 characters. The factory default is blank.

4. In the **USB File** field, specify the path and filename for the file you want to download. You may enter up to 32 characters. The default is blank.

Note: Do not overwrite the active image. If you attempt to do this, the system will display a warning.

---

5. Click the **Apply** button. The file transfer begins.

The last row of the table displays non-configurable information about the progress of the file transfer. This information is displayed only after the file transfer process starts.

File Management

The system maintains two versions of the switch software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded during subsequent switch restarts. This feature reduces switch down time when upgrading or downgrading the switch software.

A legacy software version will ignore (not load) a configuration file created that is created by a newer software version. When a configuration file created by the newer software version is discovered by the system running an older version of the software, the system displays an appropriate warning to the user.

The File Management menu contains links to the features described in the following sections.

- Copy on page 285
- Dual Image on page 285

Copy

Use the Copy screen to copy an image from one location (primary or backup) to another.

To copy an image:

1. Select **Maintenance** > **File Management** > **Copy**.
2. Next to Source Image, select image1 or image2 as the source image to copy to the destination.
3. Next to Destination Image, select the image to overwrite.
4. Next to Stack Member, select the member unit ID to copy.
5. Click the **Apply** button.

Dual Image

From the Dual Image link, you can access the following pages:

- Dual Image Configuration
- Dual Image Status on page 286

Dual Image Configuration

Use the Dual Image Configuration screen to select which image to load during the next boot cycle, configure an image description, or delete an image.

To change the image that loads during boot-up:

1. Select **Maintenance** > **File Management** > **Dual Image** > **Dual Image Configuration**.

2. From the Image Name list, select the image that is *not* the image shown in the Current-active field.

   The Current-active field displays the name of the active image.

3. From the Unit Number list, select the specific unit number or All units to configure.

4. (Optionally) In the Image Description field, specify a name for the selected image.

5. Next to Activate Image, select the check box.

6. Click the **Apply** button.

   Note: After activating an image, you must perform a system reset of the switch to run the new code. The switch continues running the image shown in the Current-active field until the switch reboots.

To delete an image:

1. From the Image Name list, select the image that is *not* the image shown in the Current-active field.

   You cannot delete the active image.

2. Next to Delete Image, select the check box.

3. Click the **Apply** button.

Dual Image Status

The Dual Image Status screen shows information about the active and backup images on the system.

To view dual image status information, select **Maintenance** > **File Management** > **Dual Image** > **Dual Image Status**

The following table describes the information available on the screen.

Table 97. Dual image status information

Field	Description
Unit	The unit number in the stack.
Image1 Ver	The version of the image1 code file.
Image2 Ver	The version of the image2 code file.
Current-active	The currently active image on this switch.
Next-active	The image to be used on the next restart of this switch.
Image1 Description	The description associated with the image1 code file.
Image2 Description	The description associated with the image2 code file.

Troubleshooting Configuration Menu

The Maintenance main navigation tab gives access to the Troubleshooting configuration menu. From this menu, you can perform basic troubleshooting functions such as pinging an IPv4 or IPv6 address to check if the switch can communicate with a particular network host and tracing an IPv4 or IPv6 route to determine the packet's path to a remote destination.

The Troubleshooting menu contains links to the features described in the following sections:

- Ping IPv4 on page 287
- Ping IPv6 on page 289
- Traceroute IPv4 on page 290
- Traceroute IPv6 on page 292
- Remote Diagnostics on page 294
- Full Memory Dump on page 295

Ping IPv4

Use the Ping screen to tell the switch to send a ping request to a specified IP address. You can use this feature to check whether the switch can communicate with a particular IP station. Once you click the **Apply** button, the switch will send a specified number of ping requests and the results will be displayed.

If a reply to the ping is not received, you will see:

```
Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec
```

If a reply to the ping is received, you will see:

```
Received response for Seq Num 0 Rtt xyz usec
Received response for Seq Num 1 Rtt abc usec
Received response for Seq Num 2 Rtt def usec
Tx = Count, Rx = Count Min/Max/Avg RTT = xyz/abc/def msec.
```

To send a ping to an IPv4 address:

1. Click **Maintenance** > **Troubleshooting** > **Ping IPv4**.

Figure 111. Ping IPv4

2. In the **IP Address/Host Name** field, specify the IP address or Hostname of the station you want the switch to ping. The initial value is blank. The IP Address or Hostname you enter is not retained across a power cycle.

3. Optionally, configure the following settings:

    •   In the **Count** field, specify the number of pings to send. The default value is 3. The range is 1 to 15. The Count you enter is not retained across a power cycle.

    •   In the **Interval** field, specify the number of seconds between pings sent. The default value is 3 seconds. The range is 1 to 60. The Interval you enter is not retained across a power cycle.

    •   In the **Size** field, specify the datagram size of the ping (ICMP) packet to send. The default value is 0 bytes. The range is 0 to 65507. The Size you enter is not retained across a power cycle.

4. In the **Source** field, select the source type from which the ping is sent, which is one of the following:

    •   **None**. The source is the IP address of the default outgoing interface. If source is not required, select None as the source option.

    •   **IP Address**. The source is an IP address that you specify. If you select this option, the IP Address field appears. Specify the source IP address of the ping in the IP address field.

    •   **Interface**. The ping is sent from a specified interface to use when sending the Echo request packets. If you select this source option, the Interface field is shown. Use the menu to select the interface from which to send the ping.

Note: Values configured in the fields above are not saved to the switch. As a result, refreshing the page sets these fields to the default values.

---

5. Click **Apply** to send the ping to the specified address. The switch sends the number of pings specified in the **Count** field, and the results are displayed below the configurable data in the **Results** area.

- If the ping is successful, you see "Reply From IP/Host: icmp_seq = 0. time = xx usec. Tx = x, Rx = x Min/Max/Avg RTT = x/x/x msec."

- If a reply to the ping is not received, you will see "Reply From IP/Host: Destination Unreachable. Tx = x, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec."

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

Ping IPv6

Use the Ping IPv6 screen 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. Once you click the **Apply** button, the switch sends three pings, and the results will be displayed below the configurable data. The output will be:

```
Send count=3, Receive count=n from (IPv6 Address). Average round trip
time = n ms.
```

To send a ping to an IPv6 address:

1. Select **Maintenance** > **Troubleshooting** > **Ping IPv6**.

Figure 112. Ping IPv6

2. In the **Ping** field, select one of the following from the list:
- Global—Ping a global IPv6 address or host.

- Link Local—Ping a link-local IPv6 address or host over the specified interface. This field is shown when Interface is selected as the ping option. Select the interface from which to send the ping.

3. In the **IPv6 Address/Hostname** field, specify the IPv6 address or Hostname of the station you want the switch to ping. The initial value is blank. The IPv6 Address or Hostname you enter is not retained across a power cycle. The format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. The maximum number of characters is 255.

4. Use **Count** to enter the number of echo requests you want to send. The range is 1 to 15. The default value is 3.

5. In the **Interval** field, specify the number of seconds between pings sent. The range is 1 to 60. The default value is 3.

6. In the **Datagram Size** field, specify the datagram size of the ping packet. The valid range is 0 to 13000. The default value is 0 bytes.

7. Enter the **Source** IP address or interface to use when sending the echo request packets. If source is not required, select None as the source option. Possible values are:

   - None—The source address of the ping packet would be the address of the default outgoing interface.

   - IPv6 Address—The source IPv6 address to use when sending the Echo request packets. This field is shown when **IPv6 Address** is selected as the source option.

   - Interface—The ping is sent from a specified interface. This field is shown when **Interface** is selected as the source option. Use the menu to select the interface from which to send the ping.

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

   The switch sends the number of pings specified in the Count field, and the results are displayed below the configurable data in the Result area:

   - If the ping is successful, the output is "Send count=3, Receive count = *n* from (IPv6 Address).Average round trip time = *n* ms".

   - If a reply to the ping is not received, the following displays: "Reply From IP/Host: Destination Unreachable. Tx = x, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec."

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

Traceroute IPv4

Use this screen to tell the switch to send a Traceroute request to a specified IP address or Hostname. You can use this traceroute utility to discover the paths that an IPv4 packet takes 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, you will see:

```
1 x.y.z.w 9869 usec 9775 usec 10584 usec
2 0.0.0.0 0 usec * 0 usec * 0 usec *
3 0.0.0.0 0 usec * 0 usec * 0 usec *
Hop Count = w Last TTL = z Test attempt = x Test Success = y.
```

To configure the traceroute settings and send probe packets to discover the route to an IPv4 address or host on the network:

1. Select **Maintenance** > **Troubleshooting** > **Traceroute IPv4**.

Figure 113. Traceroute IPv4

2. Use **IP Address/Hostname** to enter the IP address or Hostname of the station you want the switch to discover a path. The default value is blank. The IP Address or Hostname you enter is not retained across a power cycle.

3. Enter the number of **Probes Per Hop**, the number of times each hop should be probed. The default value is 3. The range is 1 to 10. The Probes per Hop you enter is not retained across a power cycle.

4. Enter the **Maximum TTL**, the maximum time-to-live for a packet in the number of hops 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.

5. Enter the **Initial TTL** the initial time-to-live for a packet in the number of hops. The default value is 1. The range is 1 to 255.The InitTTL you enter is not retained across a power cycle.

6. 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.

7. **Interval (secs)** - Enter the number of seconds between probes. The default value is 3. The range is 1 to 60. The Interval you enter is not retained across a power cycle.

8. Enter the UDP Destination **Port** in the probe packets. The default value is 33434. The range is 1- 65535. The port you enter is not retained across a power cycle.

9. 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.

10. Enter the **Source** IP address or interface to use when sending the echo request packets. If source is not required, select **None** as the source option. Possible values are:
    • **None**. The source is the IP address of the default outgoing interface.

- **IP Address**. The source is an IP address that you specify using when sending the Echo request packets. This field is shown when **IP Address** is selected as the source option.

- **Interface**. The interface to use when sending the Echo request packets. This field is shown when **Interface** is selected as the source option.

Note: Values configured in the fields above are not saved to the switch. As a result, refreshing the page sets these fields to the default values.

11. Click Apply to sends a traceroute request to the specified IP address or hostname. The results are displayed below the configurable data in the TraceRoute Results area.

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

Traceroute IPv6
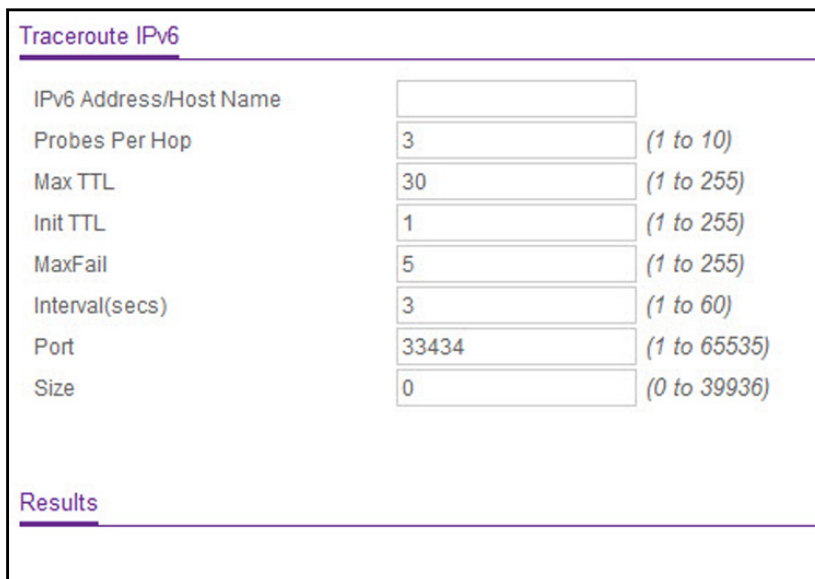
Use this screen to tell the switch to send a TraceRoute request to a specified IPv6 address or Hostname. You can use this to discover the paths that an IPv6 packet takes to a remote destination. Once you click the **Apply** button, the switch will send a traceroute and the results will be displayed below the configurable data.

If a reply to the traceroute is received, you will see:

```
1 a:b:c:d:e:f:g 9869 usec 9775 usec 10584 usec
2 0:0:0:0:0:0:0:0 0 usec * 0 usec * 0 usec *
Hop Count = w Last TTL = z Test attempt = x Test Success = y.
```

To trace a route to an IPv6 address or host:

1. Select **Maintenance** > **Troubleshooting** > **Traceroute IPv6**.

Figure 114. Traceroute IPv6

2. Use **IPv6 Address/Hostname** to enter the IPv6 address or Hostname of the station to which the switch should find a path. The initial value is blank. The IPv6 Address or Hostname you enter is not retained across a power cycle.

3. Enter the **Probes Per Hop**. Specify the number of times each hop should be probed. The default value is 3. The range is 1 to 10.

4. Enter the **Maximum TTL** maximum time-to-live for a packet in number of hops 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.

5. Enter the **Initial TTL** initial time-to-live for a packet in number of hops. The default value is 1. The range is 1 to 255. The InitTTL you enter is not retained across a power cycle.

6. 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.

7. **Interval (secs)** - Enter the number of seconds between probes. The default value is 3. The range is 1 to 60. The Interval you enter is not retained across a power cycle.

8. Enter the UDP Destination **Port** in the probe packets. The default value is 33434. The range is 1- 65535. The port you enter is not retained across a power cycle.

9. 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.

   • **Source**. Select the source type from which the packet is sent:

     - **None**. The source is the IP address of the default outgoing interface.

     - **IP address**. The source is an IP address that you specify. If you select this option, the IP Address field appears. Specify the source IP address of the probe packet in the IP address field.

     - **Interface**. The probe packet is sent from a specified interface. If you select this option, the Interface field appears. Use the menu to select the interface from which to send the probe packet.

   Note: Values configured in the fields above are not saved to the switch. As a result, refreshing the page sets these fields to the default values.

10. Click Apply to send a traceroute request to the specified IPv6 address or hostname. The results are displayed below the configurable data in the TraceRoute Results area.

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

Troubleshooting Chart

The following table lists symptoms, causes, and solutions of possible problems.

Table 98. Troubleshooting chart

Symptom	Cause	Solution
Power LED is off.	No power is received.	Check the power cord connections for the switch at the switch and the connected AC power source.
Link/ACT LED is off when a cable connects the port to a valid device.	Port connection is not working.	• Check the crimp on the connectors, and make sure that the plug is correctly inserted and locked into the port at both the switch and the connecting device. • Ensure that all cables are used correctly and comply with the Ethernet specifications. • Check for a defective adapter card, cable, or port by testing them in an alternate environment where all products are functioning.
File transfer is slow, or performance degradation is a problem.	Half- or full-duplex setting on the switch and the connected device are not the same.	Make sure that the attached device is configured to autonegotiate.
A segment or device is not recognized as part of the network.	One or more devices are not connected correctly, or cabling does not meet Ethernet guidelines.	Verify that the cabling is correct. Ensure that all connectors are securely positioned in the required ports. Equipment could have been accidentally disconnected.
Link/ACT LED is flashing continuously on all connected ports, and the network is disabled.	A network loop (redundant path) has been created.	Break the loop by ensuring that there is only one path from any networked device to any other networked device.

Remote Diagnostics

Use the Remote Diagnostics page to enable or disable the debug telnet server option to access the switch remotely to perform diagnostics services. By default, telnet server is Disabled. Debug telnet can only be accessed when the option is enabled for the purposes of collecting more information.

To enable remote diagnostics:

1. Select **Maintenance > Troubleshooting > Remote Diagnostics**.

   The Remote Diagnostics page displays.

2. Select the **Enable** radio button.

3. Click the **Apply** button.

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

Full Memory Dump

Use this screen to tell the switch to do a full memory dump to help with troubleshooting.

To display the Full Memory Dump screen, click **Maintenance** > **Troubleshooting** > **Full Memory Dump**.

Figure 115. Full Memory Dump

1. Specify the **Protocol** used to store the coredump file. Possible values are:

   a. **None**—Disable coredump.

   b. **USB**—Set USB protocol.

2. Specify the **File Path** to store the coredump file. The file path must consist of -, _, / and alphanumeric characters. Up to 64 characters can be used. The factory default is ./..

3. In the **File Name** field, specify the coredump filename. Up to 15 characters can be used. The filename must consists of -, _ and alphanumeric characters. The factory default is **core**.

4. Select the **Hostname** option to append a hostname to the coredump filename.

5. Select the **Time-stamp** option to append a time-stamp to the coredump filename.

6. Select the **Switch Register Dump** to dump the switch-chip-register in case of an exception.

7. If you specified USB as the protocol, the **Write Core Test** option appears. Select the **Write Core Test** option and press **Apply** to test the core dump setup. In this case, the **File Name** value will be used as the destination filename.

8. If you specified USB as the protocol, the **Write Core** option appears. Select the **Write Core** option and press **Apply** to create a core dump and store it in the previously configured external server. Execution of this procedure causes a reload of the device.

9. Select the **Save Current Settings** option to save the current configuration settings of the system.

10. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

8

Monitoring the System

Use the features available from the Monitoring navigation tab to view a variety of information about the switch and its ports and to configure how the switch monitors events. The Monitoring tab contains configuration menus described in the following sections.

Ports

The screens available from the Ports menu contain a variety of information about the number and type of traffic transmitted from and received on the switch. From the Ports menu, you can access links to the features described following sections:

- Switch Statistics
- Port Statistics on page 300
- Port Detailed Statistics on page 301
- EAP Statistics on page 307
- Cable Test on page 308

Switch Statistics

The Switch Statistics screen displays detailed statistical information about the traffic the switch handles.

To view the switch statistics, select **Monitoring** > **Ports** > **Switch Statistics**.

The following table describes the switch statistics displayed on the screen.

Table 99. Switch statistics

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

Table 99. Switch statistics (continued)

Field	Description
Unicast Packets Transmitted	The total number of packets that higher level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded, even though no errors had been detected, in order to prevent their being delivered to a higher layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries in Use	The number of learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

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

- Click the **Clear** button to clear all the statistics counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.
- Click **Update** to update the page with the latest information on the switch.

Port Statistics

The Port Statistics screen displays a summary of per-port traffic statistics on the switch.

To access the port summary screen:

1. Select **Monitoring** > **Ports** > **Port Statistics**.
2. Select whether to display physical interfaces, link aggregation groups (LAGs), or both by clicking one of the following links above the table heading:
   - **1** (or the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAGS**. Only link aggregation groups are displayed.
   - **All**. Both physical interfaces and link aggregation groups are displayed.

   To locate an interface quickly, type the interface number (for example, g1) in the Go To Interface field at the top or bottom of the table and click the **Go** button.

The following table describes the per-port statistics displayed on the screen.

Table 100. Port statistics

Field	Description
Interface	Lists the ports on the system.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that have been transmitted by this port to its segment.
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.
Link Down Events	The total number of link down events on a physical port.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

To reset the counters for all interfaces on the switch:

1. Select the check box in the heading of the table.
2. Click the **Clear** button.

To reset the counters for a specific interface:

1. Select the check box next to the interface for which you want to clear the counters.

    You can also type the interface number (for example, g7) in the Go To Interface field at the top or bottom of the table and click the **Go** button.

2. Click the **Clear** button.

Port Detailed Statistics

The Port Detailed Statistics screen displays a variety of per-port traffic statistics.

To view the detailed port statistics:

1. Select **Monitoring** > **Ports** > **Port Detailed Statistics**.

2. From the Interface list, select the interface with the statistics to view.

3. From the MST list, select the MST ID associated with the interface (if available).

The following table describes the detailed port information displayed on the screen.

Table 101. Detailed Interface Statistics

Field	Description
ifIndex	This field indicates the ifIndex of the interface table entry associated with this port on an adapter.
Port Type	For most ports this field is blank. Otherwise the possible values are: • Mirrored**.** Indicates that the port has been configured as a monitoring port and is the source port in a port mirroring session. For additional information about port monitoring and probe ports, see Mirroring on page 315. • Probe**.** Indicates that the port has been configured as a monitoring port and is the destination port in a port mirroring session. For additional information about port monitoring and probe ports, see Mirroring on page 315. • Port Channel. Indicates that the port has been configured as a member of a port-channel, which is also known as a Link Aggregation Group (LAG).
Port Channel ID	If the port is a member of a port channel, the port channel's interface ID and name are shown. Otherwise, Disable is shown.
Port Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
STP Mode	The Spanning Tree Protocol (STP) Administrative Mode for the port or LAG. The possible values for this field are: • Enable**.** STP is administratively enabled on this port. • Disable**.** STP is administratively disabled on this port.

Table 101. Detailed Interface Statistics (continued)

Field	Description
STP State	The port's current state Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port it will place that port into the broken state. The other five states are defined in IEEE 802.1D: • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Admin Mode	The port control administration state: • Enable. The port can participate in the network (default). • Disable. The port is administratively down and does not participate in the network.
Flow Control Mode	Indicates whether flow control is enabled or disabled for the port. This field is not valid for LAG interfaces.
LACP Mode	The Link Aggregation Control Protocol administration state, which is one of the following: • Enable. The port is allowed to participate in a port channel (LAG), which is the default mode. • Disable. The port cannot participate in a port channel (LAG).
Physical Mode	Indicates the port speed and duplex mode. In auto-negotiation mode, the duplex mode and speed are set from the auto-negotiation process.
Physical Status	Indicates the port speed and duplex mode status.
Link Status	Indicates whether the link is up or down.
Link Trap	Indicates whether or not the switch sends a trap when link status changes. • Enable. The system sends a trap when the link status changes. • Disable. The system does not send a trap when the link status changes.
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Table 101. Detailed Interface Statistics (continued)

Field	Description
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX > 1519-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Received 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Received 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
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.

Table 101. Detailed Interface Statistics (continued)

Field	Description
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 chosen to be discarded, even though no errors had been detected, in order to prevent their being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Total Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). This definition of jabber is different than the definition in IEEE 802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
Rx FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Total Received Packets Not Forwarded	A count of valid frames received which were discarded (i.e., filtered) by the forwarding process.
Local Traffic Frames	The total number of frames dropped in the forwarding process because the destination address was located off of this port.
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.

Table 101. Detailed Interface Statistics (continued)

Field	Description
Total Packets Transmitted (Octets)	The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Transmitted 65-127 Octets	The total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 128-255 Octets	The total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 256-511 Octets	The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 512-1023 Octets	The total number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 1024-1518 Octets	The total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted > 1518 Octets	The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. This counter has a max increment rate of 815 counts per sec at 10 Mb/s.
Maximum Frame Size	The maximum ethernet frame size the interface supports or is configured, including ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.
Total Packets Transmitted Successfully	The number of frames that have been transmitted by this port to its segment.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Total Transmit Errors	The sum of Single, Multiple, and Excessive Collisions.

Table 101. Detailed Interface Statistics (continued)

Field	Description
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Dropped Transmit Frames	Number of transmit frames discarded at the selected port.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.
802.3x Pause Frames Transmitted	A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
GVRP PDUs Received	The count of GVRP PDUs received in the GARP layer.
GVRP PDUs Transmitted	The count of GVRP PDUs transmitted from the GARP layer.
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

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

- Click the **Clear** button to clear all the counters. This resets all statistics for this port to the default values.
- Click **Update** to update the page with the latest information on the switch.

EAP Statistics

Use the EAP Statistics screen to display information about EAP packets received on a specific port.

To display the EAP statistics screen, select **Monitoring** > **Ports** > **EAP Statistics**.

The following table describes the EAP statistics displayed on the screen.

Table 102. EAP statistics

Field	Description
Ports	The interface which is polled for statistics.
Frames Received	The number of valid EAPOL frames received on the port.
Frames Transmitted	The number of EAPOL frames transmitted through the port.
Start Frames Received	The number of EAPOL Start frames received on the port.
Logoff Frames Received	The number of EAPOL Log off frames that have been received on the port.
Last Frame Version	The protocol version number attached to the most recently received EAPOL frame.
Last Frame Source	The source MAC Address attached to the most recently received EAPOL frame.
Invalid Frames Received	The number of unrecognized EAPOL frames received on this port.
Length Error Frames Received	The number of EAPOL frames with an invalid Packet Body Length received on this port.
Response/ID Frames Received	The number of EAP Respond ID frames that have been received on the port.
Response Frames Received	The number of valid EAP Response frames received on the port.
Request/ID Frames Transmitted	The number of EAP Requested ID frames transmitted through the port.
Request Frames Transmitted	The number of EAP Request frames transmitted through the port.

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. 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.

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

Cable Test

Use the Cable Test screen to display information about the cables connected to switch ports.

To perform the cable test:

1. Select **Monitoring** > **Ports** > **Cable Test**.
2. Select the check box next to each port on which to run the cable test.
3. Click the **Apply** button**.**

   The cable test is run on all selected ports.

   The cable test can take up to 2 seconds to complete. If the port has an active link then the link is not taken down and the cable status is always Normal. The command returns a cable length estimate if this feature is supported by the PHY for the current link speed. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter then the cable status can be Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded.

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

Table 103. Cable information

Field	Description
Port	Specifies the port that has the connected cable.
Cable Status	The cable status. • 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 can in fact be working. • Untested. The cable has not been tested yet. • 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 displayed only if the cable status is Normal.
Failure Location	The estimated distance in meters from the end of the cable to the failure location. The failure location is displayed only if the cable status is Open or Short.

Logs

The switch can generate messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored locally and can be forwarded to one or more centralized points of collection for monitoring purposes or long term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

The Logs menu contains links to the features described in the following sections.

Memory Logs

The Memory Log stores messages in memory based upon the settings for message component and severity. Use the Memory Log screen to set the administrative status and behavior of logs in the system buffer. These log messages are cleared when the switch reboots.

To configure the memory log settings:

1. Select **Monitoring** > **Logs** > **Memory Log**.
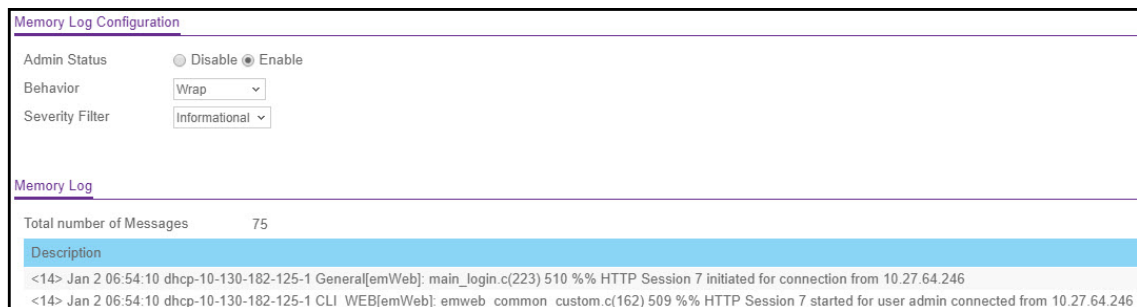
Figure 116. Memory Log

2. Next to **Admin Status**, select one of the following radio buttons:
    - **Enable**. Enable system logging.
    - **Disable**. Prevent the system from logging messages.

3. From the **Behavior** list, specify the behavior of the log when it is full.
    - **Wrap**. When the buffer is full, the oldest log messages are deleted as the system logs new messages.

- **Stop on Ful**l. When the buffer is full, the system stops logging new messages and preserves all existing log messages.

4. From the Severity Filter list, select the severity option. A log records messages equal to, or above, a configured severity threshold. Severity options are:

- Emergency (0): System is unusable.
- Alert (1): Action must be taken immediately.
- Critical (2): Critical conditions.
- Error (3): Error conditions.
- Warning (4): Warning conditions.
- Notice (5): Normal but significant conditions.
- Informational (6): Informational messages.
- Debug (7): Debug-level messages.

5. Click the **Apply** button.

The Memory Log table displays on the Memory Log screen.

The Total Number of messages displays the number of messages the system has logged in memory. Only the 200 most recent entries are displayed on the screen.

The rest of the screen displays the Memory Log messages. The format of the log message is the same for messages that are displayed for the message log, persistent log, or console log. Messages logged to a collector or relay through syslog have the same format as well.

The following example shows the standard format for a log message:

```
<14> Mar 24 05:34:05 10.131.12.183-1 UNKN[2176789276]:
main_login.c(179) 3855 %% HTTP Session 19 initiated for user admin
connected from 10.27.64.122
```

The number contained in the angle brackets represents the message priority, which is derived from the following values:

Priority = (facility value × 8) + severity level.

The facility value is usually one, which means it is a user-level message. Therefore, to determine the severity level of the message, subtract eight from the number in the angle brackets. The example log message has a severity level of 6 (informational). For more information about the severity of a log message, see Server Log on page 312.

The message was generated on March 24 at 5:34:05 a.m. by the switch with an IP address of 10.131.12.183. The component that generated the message is unknown, but it came from line 179 of the main_login.c file. This is the 3,855[th] message logged since the switch was last booted. The message indicates that the administrator logged on to the HTTP management interface from a host with an IP address of 10.27.64.122.

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

- Click the **Clear** button to clear the messages out of the buffered log in the memory.
- Click the **Refresh** button to refresh the page with the latest information on the switch.

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

FLASH Log

The FLASH log stores log messages in persistent storage, which means that the log messages can be retained across a switch reboot. The FLASH log can display the current operational and startup log messages, or it can display up to 64 messages that were logged prior to the last reboot. Only the messages that meet the configured severity level are logged to FLASH memory.

Use the FLASH Log screen to enable or disable persistent logging, set the severity filter of persistent log messages, and view log messages stored in FLASH for the current boot cycle or for the previous boot cycle.

To enable persistent logging and configure the severity level:

1. Select **Monitoring** > **Logs** > **FLASH Log**.
2. Next to Admin Status, select one of the following radio buttons:
   - **Enable**. Enable logging messages to persistent logging.
   - **Disable**. Prevent the system from logging messages in persistent storage.
3. From the Severity Filter field, specify the type of log messages to record.

   A log records messages equal to or above a configured severity threshold. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert (1). The severity can be one of the following levels:

   - **Emergency** (0). The highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
   - **Alert** (1). The second-highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down. Action must be taken immediately.
   - **Critical** (2). The third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
   - **Error** (3). A device error has occurred, such as if a port is offline.
   - **Warning** (4). The lowest level of a device warning.
   - **Notice** (5). Normal but significant conditions. Provides the network administrators with device information.
   - **Informational** (6). Provides device information.
   - **Debug** (7). Provides detailed information about the log. Debugging should be entered only by qualified support personnel.

4. Click the **Apply** button.

The rest of the screen displays the number of persistent messages the system has logged and the persistent log messages.

To view log messages stored in persistent storage:

1. Select **Monitoring** > **Logs** > **FLASH Log**.

2. Next to Logs to be Displayed, select the log messages to view:

    •   **Current Logs**. View the messages logged to persistent storage during the current boot cycle.

    •   **Previous Logs**. View the messages logged to persistent storage during the previous boot cycle. The screen displays up to 64 messages logged to persistent storage during the previous boot cycle. The persistent log file from the previous boot cycle stores the following messages:

        -   Up to 32 startup messages, which are messages that occurred immediately after the previous boot cycle completed (system startup).

        -   Up to 32 operational messages, which are messages that occurred immediately preceding the last boot.

3. Total Number of Messages. Total number of persistent log messages stored on the switch. The maximum number of persistent log messages displayed on the switch is 64.

4. Description: <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry

    The above example indicates a user-level message (1) with severity 7 (debug) on a system that is not stacked and generated by component MSTP running in thread id 2110 on Aug 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged. Messages logged to a collector or relay via syslog have an identical format to the above message.

Server Log

Use the Server Log screen to allow the switch to send log messages to the remote logging hosts configured on the system.

To configure local log server settings:

1. Select **Monitoring** > **Logs** > **Server Log.**

2. Next to Admin Status, select one of the following:

    •   **Enable**. Send log messages to all configured hosts (syslog collectors or relays) using the values configured for each host.

    •   **Disable**. Stop logging to all syslog hosts. Disable means no messages will be sent to any collector/relay.

3. In the Local UDP Port field, specify the port on the switch from which syslog messages are sent.

4. Click the **Apply** button.

    The Server Log Configuration area displays the following information:

    •   The Messages Received field shows the number of messages received by the log process. This includes messages that are dropped or ignored.

- The Messages Relayed field shows the number of messages forwarded by the syslog function to a syslog host. Messages forwarded to multiple hosts are counted once for each host.
- The Messages Ignored field shows the number of messages that were ignored.

To add a remote syslog host (log server):

1. Specify the following settings in the following list.
   - **IP Address Type**. Specify the IP Address Type of Host. It can be one of the following:
     - IPv4
     - IPv6
     - DNS
   - **Host Address**. Specify the hostname of the host configured for syslog.
   - **Port**. Specify the port on the host to which syslog messages are sent. The default port is 514.
   - **Severity Filter**. Use the menu to select the severity of the logs to send to the logging host. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert (1). The severity can be one of the following levels:
     - **Emergency** (0). The highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert** (1). The second-highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down.
     - **Critical** (2). The third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error** (3). A device error has occurred, such as if a port is offline.
     - **Warning** (4). The lowest level of a device warning.
     - **Notice** (5). Provides the network administrators with device information.
     - **Informational** (6). Provides device information.
     - **Debug** (7). Provides detailed information about the log. Debugging should be entered only by qualified support personnel.
2. Click the **Add** button.

   The Status field in the Server Configuration table shows whether the remote logging host is currently active.

To delete an existing host:

1. Select the check box next to the host to remove.
2. Click the **Delete** button.

To modify the settings for an existing host:

1. Select the check box next to the host to modify.
2. Change the desired information.
3. Click the **Apply** button.

Trap Logs

Use the Trap Logs screen to view information about the SNMP traps generated on the switch.

To view trap log information, select **Monitoring** > **Logs** > **Trap Logs**. The Trap Logs screen displays.

The following table describes the Trap Log information displayed on the screen.

Table 104. Trap log statistics

Field	Description
Number of Traps Since Last Reset	The number of traps that have occurred since the switch last reboot.
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries will overwrite the oldest entries.
Number of Traps Since Log Last Viewed	The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (such as terminal interface display, web display, or upload file from switch) will cause this counter to be cleared to 0.

The screen also displays information about the traps that were sent.

Table 105. Trap log information

Field	Description
Log	The sequence number of this trap.
System Up Time	The time at which this trap occurred, expressed in days, hours, minutes, and seconds since the last reboot of the switch.
Trap	Information identifying the trap.

Event Logs

Use the Event Logs screen to display the event log, which is used to hold error messages for catastrophic events. After the event is logged and the updated log is saved in flash memory, the switch will be reset. The log can hold at least 2,000 entries and is erased when an attempt is made to add an entry after it is full. The event log is preserved across system resets.

To view the event logs, select **Monitoring** > **Logs** > **Event Logs**.

The following table describes the event log information displayed on the screen.

Table 106. Event log information

Field	Description
Entry	The number of the entry within the event log. The most recent entry is first.
Type	Specifies the type of entry.
Filename	The switch source code filename identifying the code that detected the event.
Line	The line number within the source file of the code that detected the event.
Task ID	The OS-assigned ID of the task reporting the event.
Code	The event code passed to the event log handler by the code reporting the event.
Time	The time the event occurred, measured from the previous reset.

Mirroring

The Port Mirroring screen allows you to view and configure port mirroring on the system.

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.

Use the Port Mirroring screen to define port mirroring sessions.

To configure port mirroring:

1. Select **Monitoring** > **Mirroring** > **Port Mirroring**.

Figure 117. Port Mirroring

2. In the Global Configuration section of the screen, click the option to enable (**True**) or disable (**False**) the **Admin Mode** for the current session. When Admin Mode is enabled, any traffic entering or leaving the source ports of the current session is copied (mirrored) onto the corresponding destination port. The default mode is disabled (False).

3. In the **Destination Port** list, select the destination port to which port traffic is be copied. The default value is **None**.

4. In the Source Interface Configuration section of the screen, select the source port or ports.

    You can configure multiple ports and LAGs as source ports. The CPU port can also be configured as a source port. When the CPU is a source port, traffic received or sent by the CPU is mirrored to the probe port.

    a. Display the ports or LAGs to configure as source ports.

    To display physical interfaces, LAGs, or both, click one of the following links above the table heading:

    •   **1**. Only physical interfaces are displayed. This is the default setting.

    •   **LAGS**. Only link aggregation groups are displayed.

    •   **CPU**. The CPU port is displayed.

    •   **All**. Both physical interfaces and link aggregation groups are displayed.

    b. Select the check box next to each physical port or LAG to configure as the mirrored source.

5. From the **Direction** list, specify the direction of the traffic to be mirrored from the configured mirrored port(s). If the value is not configured, it will be shown as **None**. The default value is **None**.

   - **None**. The value is not configured.
   - **Tx and Rx**. Monitors both transmitted and received packets on the selected ports.
   - **Tx only**. Monitors transmitted packets only on the selected ports.
   - **Rx only**. Monitors received packets only on the selected ports.

6. Click the **Apply** button to send the updated configuration to the switch. Configuration changes take effect immediately.

   If the port is configured as a source port, the Status value is Mirrored.

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

8. The **Status** column is a nonconfigurable field and indicates the interface state.

To delete a mirrored port:

1. Select the check box next to the mirrored port.
2. Click the **Delete** button.

A

Configuration Examples

This appendix contains information about:

Virtual Local Area Network Configuration Example

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). For traffic to flow between different VLANs, it must go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of workstations, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

VLANs have a number of advantages:

- It is easy to do network segmentation. Users that communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.

- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.

- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.

- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID tag number. Each port has a default VLAN ID setting that is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed in the Port PVID Configuration screen. See Port VLAN ID Configuration on page 142.

- When a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID setting. The packet proceeds to the VLAN specified by its VLAN ID tag number.

- If the port through which the packet entered does not have membership with the VLAN specified by the VLAN ID tag, the packet is dropped.

- If the port is a member of the VLAN specified by the packet's VLAN ID, the packet can be sent to other ports with the same VLAN ID.

- Packets leaving the switch are either tagged or untagged, depending on the setting for that port's VLAN membership properties. A U for a given port means that packets leaving the switch from that port are untagged. Inversely, a T for a given port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

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 create the following VLANs:
   - A VLAN with VLAN ID 10.
   - A VLAN with VLAN ID 20.

Figure 118. VLAN Configuration Example

For more information about how to perform this step, see Basic VLAN Configuration on page 140.

2. In the VLAN Membership screen, 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).
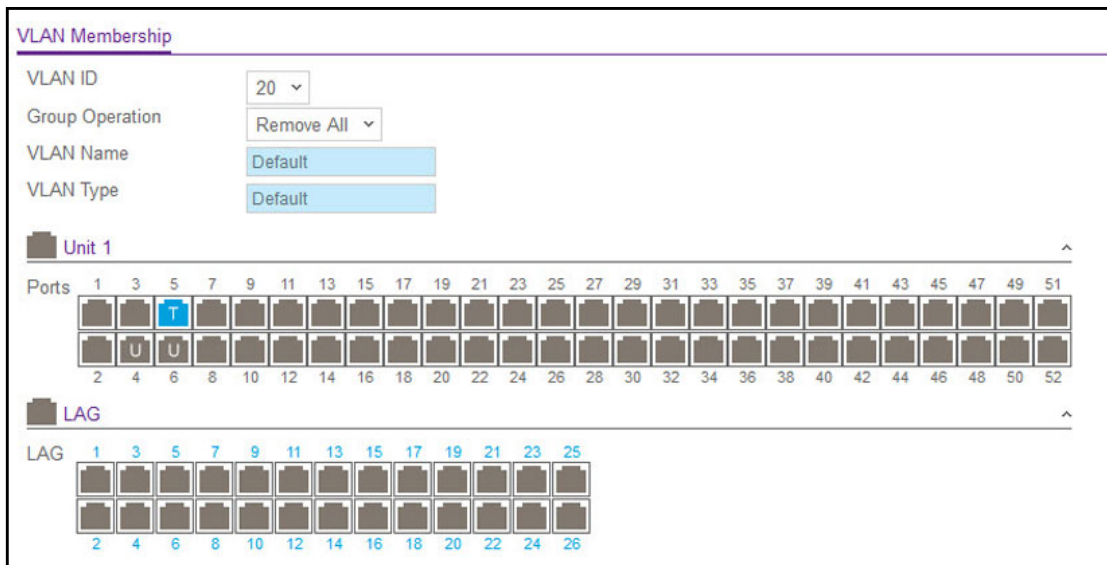
Figure 119. VLAN Membership

For more information about how to perform this step, see VLAN Membership Configuration on page 140.

3. In the Port PVID Configuration screen, 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

For more information about how to perform this step, see Port VLAN ID Configuration on page 142.

With the VLAN configuration that you set up, the following situations produce results as described:

- If an untagged packet enters port 1, the switch tags it with VLAN ID 10. The packet has access to port 2 and port 3. The outgoing packet is stripped of its tag to leave port 2 as an untagged packet. For port 3, the outgoing packet leaves as a tagged packet with VLAN ID 10.

- If a tagged packet with VLAN ID 10 enters port 3, the packet has access to port 1 and port 2. If the packet leaves port 1 or port 2, it is stripped of its tag to leave the switch as an untagged packet.

- If an untagged packet enters port 4, the switch tags it with VLAN ID 20. The packet has access to port 5 and port 6. The outgoing packet is stripped of its tag to become an untagged packet as it leaves port 6. For port 5, the outgoing packet leaves as a tagged packet with VLAN ID 20.

Access Control Lists

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and 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.

To filter traffic by using an ACL:

1. Create an access list.

2. Configure and add rules to the access list.

   A defined ACL 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.

3. Apply the access list to an interface in the inbound direction.

The switch allows ACLs to be bound to physical ports and LAGs.The switch software supports MAC ACLs and IP ACLs.

MAC ACL Configuration Example

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.

2. For more information about how to perform this step, see <u>MAC ACL on page 258</u>.

   By default, this ACL will be bound on the inbound direction, which means the switch will examine traffic as it enters the port.

3. From the MAC Rules screen, create a rule for the Sales_ACL with the following settings:
   - **ID**. 1
   - **Action**. Permit
   - **Assign Queue**. 0
   - **Match Every**. False

- **CoS**. 0
- **Destination MAC**. 01:02:1A:BC:DE:EF
- **Destination MAC Mask**. 00:00:00:00:FF:FF
- **Source MAC**. 02:02:1A:BC:DE:EF
- **Source MAC Mask**. 00:00:00:00:FF:FF
- **VLAN ID**. 2

Figure 120. MAC ACL

For more information about how to perform this step, see MAC Rules on page 259.

4. From the MAC Binding Configuration screen, assign the Sales_ACL to Ethernet ports 6, 7, and 8.

Figure 121. MAC Binding Configuration

For more information about how to perform this step, see MAC Binding Configuration on page 261

The ACL named Sales_ACL looks for Ethernet frames with destination and source MAC addresses and MAC masks defined in the rule. Also, the frame must be tagged with VLAN ID 2, which is the Sales department VLAN. The CoS value of the frame must be 0, which is the default value for Ethernet frames. Frames that match this criteria are permitted on interfaces 6, 7, and 8 and are assigned to the hardware egress queue 0, which is the default queue. All other traffic is explicitly denied on these interfaces. To allow additional traffic to enter these

ports, you must add a new *permit* rule with the desired match criteria and bind the rule to interfaces 6, 7, and 8.

Standard IP ACL Configuration Example

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.

   For more information about this step, see IP ACL on page 262.

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 more information about this step, see IP Rules on page 263.

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 Ethernet ports 2, 3, and 4, and assign a sequence number of 1.

   For more information about this step, see IP Binding Configuration on page 271.

   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.

The IP ACL in this example matches all packets with the source IP address and subnet mask of the Finance department's network and deny it on the Ethernet interfaces 2, 3, and 4 of the switch. The second rule permits all non-Finance traffic on the ports. The second rule is required because there is an explicit *deny all* rule as the lowest priority rule.

Differentiated Services

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 can be delayed, sent sporadically, or dropped. For typical Internet applications, such as e-mail and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS-capable. If one node is unable to meet the necessary timing requirements, this creates a deficiency in the network path and the performance of the entire packet flow is compromised.

There are two basic types of QoS:

- **Integrated Services**. Network resources are apportioned based on request and are reserved (resource reservation) according to network management policy (RSVP, for example).
- **Differentiated Services**. Network resources are apportioned based on traffic classification and priority, giving preferential treatment to data with strict timing requirements.

The switch supports DiffServ.

The DiffServ feature contains a number of conceptual QoS building blocks you can use to construct a differentiated service network. Use these same blocks in different ways to build other types of QoS architectures.

There are 3 key QoS building blocks needed to configure DiffServ:

- Class
- Policy
- Service (i.e., the assignment of a policy to a directional interface)

Class

You can classify incoming packets at layers 2, 3, and 4 by inspecting the following information for a packet:

- Source/destination MAC address
- EtherType
- Class of Service (802.1p priority) value (first/only VLAN tag)
- VLAN ID range (first/only VLAN tag)

- IP Service Type octet (also known as: ToS bits, Precedence value, DSCP value)
- Layer 4 protocol (such as TCP or UDP)
- Layer 4 source/destination ports
- Source/destination IP address

From a DiffServ point of view, there are two types of classes:

- DiffServ traffic classes
- DiffServ service levels/forwarding classes

DiffServ Traffic Classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multifield (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

You can combine these classifiers with logical AND or OR operations to build complex MF-classifiers (by specifying a class type of *all* or *any*, respectively). That is, within a single class, multiple match criteria are grouped together as an AND expression or a sequential OR expression, depending on the defined class type. Only classes of the same type can be nested; class nesting does not allow for the negation (i.e., *exclude* option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a given DSCP value, on the egress interface. These service levels are defined by configuring BA classes for each.

Creating Policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, there are two types of policies:

- **Traffic Conditioning Policy**. A policy applied to a DiffServ traffic class
- **Service Provisioning Policy**. A policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

Traffic Conditioning Policy

- **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.

- **Mark 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.

- **Mark CoS (802.1p)**. Sets the three-bit priority field in the first/only 802.1p header to a specified value when packets are transmitted for the traffic class. An 802.1p header is inserted if it does not already exist. This is useful for assigning a layer 2 priority level based on a DiffServ forwarding class (i.e., DSCP or IP Precedence value) definition to convey some QoS characteristics to downstream switches which do not routinely look at the DSCP value in the IP header.

- **Policy**. 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, 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. For more information, see Service Statistics on page 225.

- **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.

DiffServ Configuration Example

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 step, see Class Configuration on page 218.

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 step, see Class Configuration on page 218.

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 step, see Policy Configuration on page 222.

6. Click the **Add** button to add the new policy.
7. Click the Policy1 hyperlink to view the Policy Class Configuration screen for this policy.
8. Configure the Policy attributes as follows:
   - **Assign Queu**e. 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 step, see Policy Configuration on page 222.

9. From the Service Configuration screen, select the check box next to interfaces g7 and g8 to attach the policy to these interfaces,

For more information about this step, see <u>Service Configuration on page 225</u>.

10. Click the **Apply** button.

All UDP packet flows destined to the 192.12.2.0 network with an IP source address from the 192.12.1.0 network that have a Layer 4 Source port of 4567 and Destination port of 4568 from this switch on ports 7 and 8 are assigned to hardware queue 3.

On this network, traffic from streaming applications uses UDP port 4567 as the source and 4568 as the destination. This real-time traffic is time sensitive, so it is assigned to a high-priority hardware queue. By default, data traffic uses hardware queue 0, which is designated as a best-effort queue.

Also the *confirmed action* on this flow is to send the packets with a committed rate of 1,000,000 Kbps and burst size of 128 KB. Packets that violate the committed rate and burst size are dropped.

802.1X Configuration Example

Local Area Networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments, it can be desirable to restrict access to the services offered by the LAN to those users and devices that are permitted to use those services.

Port-based network access control makes use of the physical characteristics of LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics and of preventing access to that port in cases in which the authentication and authorization process fails. In this context, a port is a single point of attachment to the LAN, such as ports of MAC bridges and associations between stations or access points in IEEE 802.11 Wireless LANs.

The IEEE 802.11 standard describes an architectural framework within which authentication and consequent actions take place. It also establishes the requirements for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

The switch supports a guest VLAN, which allows unauthenticated users to have limited access to the network resources.

Note: You can use QoS features to provide rate limiting on the guest VLAN to limit the network resources the guest VLAN provides.

Another 802.1X feature is the ability to configure a port to Enable/Disable EAPoL packet forwarding support.You can disable or enable the forwarding of EAPoL when 802.1X is disabled on the device.

The ports of an 802.1X authenticator switch provide the means in which it can offer services to other systems reachable via the LAN. Port-based network access control allows the operation of a switch's ports to be controlled in order to ensure that access to its services is only permitted by systems that are authorized to do so.

Port access control provides a means of preventing unauthorized access by supplicants to the services offered by a system. Control over the access to a switch and the LAN to which it is connected can be desirable in order to restrict access to publicly accessible bridge ports or to restrict access to departmental LANs.

Access control is achieved by enforcing authentication of supplicants that are attached to an authenticator's controlled ports. The result of the authentication process determines whether the supplicant is authorized to access services on that controlled port.

A Port Access Entity (PAE) is able to adopt one of two distinct roles within an access control interaction:

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

Additionally, there exists a third role:

- **Authentication server**. Performs the authentication function necessary to check the credentials of the Supplicant on behalf of the Authenticator.

All three roles are required in order to complete an authentication exchange.

The switch supports 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.
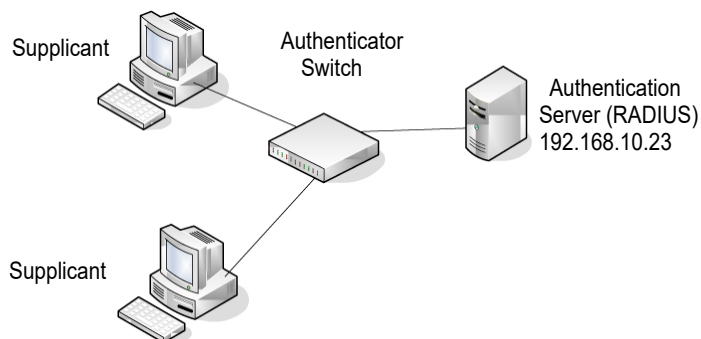
Figure 122. 802.1x Configuration Example

This example shows how to configure the switch so that 802.1X-based authentication is required on the ports in a corporate conference room (g1–g8). These ports are available to visitors and need to be authenticated before granting access to the network. The

authentication is handled by an external RADIUS server. When the visitor is successfully authenticated, traffic is automatically assigned to the guest VLAN. This example assumes that a VLAN has been configured with a VLAN ID of 150 and VLAN Name of Guest.

1. From the Port Authentication screen, select ports g1 through g8.

2. From the Port Control list, select Unauthorized.

   The Port Control setting for all other ports where authentication is not needed should Authorized. When the Port Control setting is Authorized, the port is unconditionally put in a force-Authorized state and does not require any authentication. When the Port Control setting is Auto, the authenticator PAE sets the controlled port mode.

3. In the Guest VLAN field for ports g1–g8, enter 150 to assign these ports to the guest VLAN.

   You can configure additional settings to control access to the network through the ports. See Port Security Interface Configuration on page 252 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.

   For more information about this step, see Port Security Configuration on page 251.

6. Click the **Apply** button.

   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.

7. 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 about this step, see RADIUS Configuration on page 229.

8. Click the **Add** button.

9. From the Authentication List screen, configure the default List to use RADIUS as the first authentication method.

   For more information about this step, see Authentication List Configuration on page 235.

This example enables 802.1X-based port security on the switch and prompts the hosts connected on ports g1–g8 for an 802.1X-based authentication. The switch passes the authentication information to the configured RADIUS server.

MSTP

Spanning Tree Protocol (STP) runs on bridged networks to help eliminate loops. If a bridge loop occurs, the network can become flooded with traffic. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree, with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the Forwarding state).

The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notification. These features are represented by the parameters *pointtopoint* and *edgeport*. MSTP is compatible to both RSTP and STP. It behaves appropriately to STP and RSTP bridges.

A MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provides simple and full connectivity for frames assigned to any given VLAN throughout a Bridged LAN comprising arbitrarily interconnected networking devices, each operating MSTP, STP or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MSTP Bridges. These Regions and the other Bridges and LANs are connected into a single Common Spanning Tree (CST). [IEEE DRAFT P802.1s/D13]

MSTP connects all Bridges and LANs with a single Common and Internal Spanning Tree (CIST). The CIST supports the automatic determination of each MST region, choosing its maximum possible extent. The connectivity calculated for the CIST provides the CST for interconnecting these Regions, and an Internal Spanning Tree (IST) within each Region. MSTP ensures that frames with a given VLAN ID are assigned to one and only one of the MSTIs or the IST within the Region, that the assignment is consistent among all the networking devices in the Region and that the stable connectivity of each MSTI and IST at the boundary of the Region matches that of the CST. The stable active topology of the Bridged LAN with respect to frames consistently classified as belonging to any given VLAN thus simply and fully connects all LANs and networking devices throughout the network, though frames belonging to different VLANs can take different paths within any Region, per IEEE DRAFT P802.1s/D13.

All bridges, whether they use STP, RSTP or MSTP, send information in configuration messages via Bridge Protocol Data Units (BPDUs) to assign port roles that determine each port's participation in a fully and simply connected active topology based on one or more spanning trees. The information communicated is known as the spanning tree priority vector. The BPDU structure for each of these different protocols is different. A MSTP bridge will transmit the appropriate BPDU depending on the received type of BPDU from a particular port.

An MST Region comprises of one or more MSTP Bridges with the same MST Configuration Identifier, using the same MSTIs, and which have no Bridges attached that cannot receive and transmit MSTP BPDUs. The MST Configuration Identifier has the following components:

- Configuration Identifier Format Selector
- Configuration Name
- Configuration Revision Level
- Configuration Digest: 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID to MSTID mapping)

As there are Multiple Instances of Spanning Tree, there is a MSTP state maintained on a per-port, per-instance basis (or on a per port per VLAN basis: as any VLAN can be in one and only one MSTI or CIST). For example, port A can be forwarding for instance 1 while discarding for instance 2. The port states have changed since IEEE 802.1D specification.

To support multiple spanning trees, a MSTP bridge has to be configured with an unambiguous assignment of VLAN IDs (VIDs) to spanning trees. This is achieved by:

1. Ensuring that the allocation of VIDs to FIDs is unambiguous.
2. Ensuring that each FID supported by the Bridge is allocated to exactly one Spanning Tree Instance.

The combination of VID to FID and then FID to MSTI allocation defines a mapping of VIDs to spanning tree instances, represented by the MST Configuration Table.

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

An instance can occur that has no VIDs allocated to it, but every VLAN must be allocated to one of the other instances of spanning tree.

The portion of the active topology of the network that connects any two bridges in the same MST Region traverses only MST bridges and LANs in that region, and never Bridges of any kind outside the Region, in other words connectivity within the region is independent of external connectivity.

MSTP Configuration Example

This example shows how to create an MSTP instance on the switch. The example network has three different switches that serve different locations in the network. In this example, ports g1–g5 are connected to host stations, so those links are not subject to network loops. Ports g6–g8 are connected across switches 1, 2, and 3.
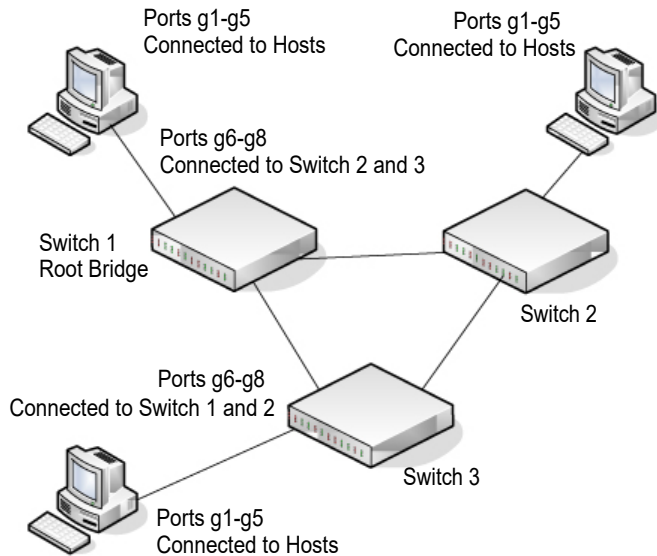
Figure 123. MSTP Configuration Example

Perform the following procedures on each switch to configure MSTP:

1. Use the VLAN Configuration screen to create VLANs 300 and 500.

   For more information about this step, see, Basic VLAN Configuration on page 140.

2. Use the VLAN Membership screen to include ports g1–g8 as tagged (T) or untagged (U) members of VLAN 300 and VLAN 500.

   For more information about this step, see VLAN Membership Configuration on page 140.

3. From the STP Configuration screen, enable the Spanning Tree State option.

   For more information about this step, see STP Configuration on page 153.

   Use the default values for the rest of the STP configuration settings. By default, the STP Operation Mode is MSTP and the Configuration Name is the switch MAC address.

4. From the CST Configuration screen, set the Bridge Priority value for each of the three switches to force Switch 1 to be the root bridge:

   • **Switch 1**. 4096
   • **Switch 2**. 12288
   • **Switch 3**. 20480

Note: Bridge priority values are multiples of 4096.

If you do not specify a root bridge and all switches have the same Bridge Priority value, the switch with the lowest MAC address is elected as the root bridge (see CST Configuration on page 154).

5. From the CST Port Configuration screen, select ports g1–g8 and select Enable from the STP Status list.

   For more information about this step, see CST Port Configuration on page 155.

6. Click the **Apply** button.

7. Select ports g1–g5 (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 about this step, see MST Configuration on page 158.

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 g1, g2, and g3) and in the HR department (ports g4 and g5). Switches 1 and 2 also have hosts in the Sales and Human Resources departments. The hosts connected from Switch 2 use VLAN 500, MST instance 2 to communicate with the hosts on Switch 3 directly. Likewise, hosts of Switch 1 use VLAN 300, MST instance 1 to communicate with the hosts on Switch 3 directly.

The hosts use different instances of MSTP to effectively use the links across the switch. The same concept can be extended to other switches and more instances of MSTP.

VLAN Routing Interface Configuration Example

VLANs divide broadcast domains in a LAN environment. Whenever hosts in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed between them. This is known as inter-VLAN routing. On the switch, it is accomplished by creating Layer 3 interfaces (switch virtual interfaces (SVI)).

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

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required. A port can be either a VLAN port or a router port, but not both. However, a VLAN port can be part of a VLAN that is itself a router port.

Complete these steps to configure a switch to perform interVLAN routing.

1. Use the IP Configuration screen to enable routing on the switch.

    For more information about this step, see).

2. Determine the IP addresses you want to assign to the VLAN interface on the switch.

    For the switch to be able to route between the VLANs, the VLAN interfaces must be configured with an IP address. When the switch receives a packet destined for another subnet/VLAN, the switch looks at the routing table to determine where to forward the packet. The packet is then passed to the VLAN interface of the destination. It is then sent to the port where the end device is attached.

3. Use the VLAN Routing Wizard screen to create a routing VLAN, configure the IP address and subnet mask, and to add the member ports.

    In the following figure, VLAN 300 is created with IP address 10.1.2.1 and subnet mask 255.255.255.0, with ports 9, 10, and 11 as untagged members.

Figure 124. VLAN Routing Wizard

The following figure shows the VLAN Routing screen with the configured VLAN routing interface.

Figure 125. VLAN Routing Configuration

Smart M4300/S3300 Firmware Upgrade Procedure

This section describes the firmware upgrade procedures in the following typical scenarios:

- Bringing Up M4300 and S3300 to Form Mixed Stacking on page 338
- Regular Image Upgrade After Mixed Stacking is Formed with 6.6.4 Image on page 340
- Converting the M4300 Units Back Into Fully Managed M4300 Mode on page 340

Bringing Up M4300 and S3300 to Form Mixed Stacking

Because there is no hardware change in either M4300 or in S3300 products, the mixed stacking capability is purely software controlled. In order to support mixed stacking between M4300 and S3300, the software prerequisites are as follows:

- M4300 labeled image 12.0.2.17 (or newer version)
- M4300 labeled image 6.6.4.x (with typical filename `m4300v6.6.4.x.stk`)
- S3300 labeled image 6.6.4.x (with typical filename `S3300v6.6.4.x.stk`)

There are two separate images, one for S3300 and another for M4300, as part of the 6.6.4.x release.

Note: M4300 and S3300 should have the *exact same* version number in order for them to mix stack successfully. For example, they both should be loaded with the 6.6.4.1 version of the respective images. If one device loads 6.6.4.1, and the other device loads 6.6.4.2, the mix stack would report Code Mismatch and would not be operational.

Steps to Follow for M4300

1. Download the 12.0.2.17 (or newer version) image into a M4300-12X12F, or into a M4300-24X, or into a homogeneous or heterogeneous stack of them

   Note: This 12.0.2.17 image can also be downloaded into other M4300 models and that will not cause any issues. However, the 12.0.2.17 image will make sure that the 6.6.4.x image can be downloaded *only* on M4300-12X12F and M4300-24X, and not in any other M4300 platforms.

2. Activate the 12.0.2.17 image and reload the unit or stack with it.

   Note: This stack can be any one of the M4300 models, but this procedure example uses M4300-12X12F and M4300-24X for the steps below.

3. When the 12.0.2.17 image is running, download the 6.6.4.x image into this unit/stack.

   Note: The 6.6.4.x image can be downloaded in the usual way via the Web UI (and also through CLI). This image can be downloaded as the Active or as the Backup image. If the image is downloaded as the Backup image, activate this image via Web UI (or via CLI).

4. Reload the switch to come up with the 6.6.4.x image.

   Note: At this stage, all previous configurations from 12.0.2.x will be lost, and the switch will come up with a default configuration, similar to the default configuration of S3300.

5. Now that the switch is running the 6.6.4.x image, configure a maximum of four ports (any four from the eight available ports listed below) into Stacking mode and reload the switch:
   • M4300-24X: ports 17–24
   • M4300-12X12F: ports 9–12 and ports 21–24

When M4300 is running with the 6.6.4.x image, configuration setting via service port and console port will no longer be available. Smart Control Center (SCC) can be used to discover the Smart M4300 and do some basic settings, same as that can be done on the S3300.

M4300 has a default Management IP of 192.168.0.239 if it cannot get an IP address from an available DHCP server.

Steps to Follow for S3300

1. Download the 6.6.4.x image directly into the S3300 unit as the stack from the running 6.6.0.x or 6.6.1.x image.

   Note: The 6.6.4.x image can be downloaded in the usual way using the Web UI. This image can be downloaded as the Active or as the Backup image. If the image is downloaded as the Backup image, activate this image using the Web UI.

   Note: The 6.6.4.x release *will* accept configuration from the 6.6.0 or 6.6.1 release. Thus configuration from those previous releases will be accepted on 6.6.4.x.

2. Once the switch is running with 6.6.4.x, configure (if not done already) a maximum of four uplink 10G ports (the last four) into stacking mode and reload the switch.

Forming Mixed Stacking

Now that both M4300 and S3300 units are running with the *exact same* 6.6.4.x code, they can be connected together to form mixed stacking via the stacking ports on M4300 and S3300.

Regular Image Upgrade After Mixed Stacking is Formed with 6.6.4 Image

After the mixed stacking is formed using the steps in <u>Bringing Up M4300 and S3300 to Form Mixed Stacking on page 338</u>, the mixed stack can now be upgraded to a newer 6.6.4 image. Use the following steps to do that:

1. Download a new S3300 6.6.4 image (such as, a 6.6.4.2 image when the stack is running with 6.6.4.1) through the Web UI.

   This will update the S3300 units in the mix stack with the new 6.6.4 image (for example, 6.6.4.2), but will not download this image into the M4300 units.

2. Download a new M4300 6.6.4 image (for example, 6.6.4.2) through the Web UI.

   This will update the M4300 units with the new 6.6.4 image but will not download this into the S3300 units.

   Note: Both <u>Step 1</u> and <u>Step 2</u> are required to be performed since there are two images for each 6.6.4 release. This can be done irrespective of whether M4300 or S3300 is the stack master.

3. After both the 6.6.4 images are downloaded into the respective units, activate the new image and reload the stack.

   Note: The new 6.6.4 image can be downloaded into either Active or Backup image. In case both the 6.6.4 images are downloaded into backup, activate them via the Web UI (using the **Maintenance > File Management > Dual Image > Dual Image Configuration** option in the Web UI).

   The stack should come up with the new 6.6.4 image (such as, 6.6.4.2).

Converting the M4300 Units Back Into Fully Managed M4300 Mode

The two M4300 units that are part of mixed stacking with S3300 can be brought back to regular M4300 mode (in Fully Managed form with a 12.0.2 image). To do that, follow the steps below:

1. Disconnect the M4300 units from the mixed stack such that they either become standalone, or form a homogeneous stack among themselves.

2. Connect the network port to the master unit, if it's not already connected.

3. Download any released 12.0.2 image via the Web UI and activate it.

   Note: The 12.0.2 image can be loaded as either the Active or the Backup image.

4. Reload the unit with the 12.0.2 image.

   M4300 units should come up with the 12.0.2 image, and their Service Port becomes active. The CLI also appears on the console.

   Note: The existing configuration from 6.6.4 mixed stacking gets migrated to the 12.0.2 release (with unsupported configuration being discarded, and that generates logs into the memory log buffer for each of those failed/non-migrated configurations).

B

Hardware Specifications and Default Values

This appendix contains the following sections.

Switch Specifications

The switch conforms to the TCP/IP, UDP, HTTP, ICMP, TFTP, DHCP, IEEE 802.1D, IEEE 802.1p, and IEEE 802.1Q standards.

Table 107. S3300 Switch Specifications and Performance

Feature	Value
S3300-28X	24 10/100/1000Mbps 2 10G/1G SFP+ ports 2 10G/1G/100M RJ45 ports
S3300-28X-PoE+	24 POE+ 10/100/1000Mbps 2 10G/1G SFP+ ports 2 10G/1G/100M RJ45 ports
S3300-52X	48 10/100/1000Mbps 2 10G/1G SFP+ ports 2 10G/1G/100M RJ45 ports
S3300-52X-PoE+	48 PoE+ 10/100/1000Mbps 2 10G/1G SFP+ ports 2 10G/1G/100M RJ45 ports
Flash memory size	64 MB Flash SPI
SRAM size and type	256 MB DDR3 SDRAM
Switching capacity	Non-Blocking Full WireSpeed on all packet sizes
Forwarding method	Store and Forward
Packet forwarding rate	10M:14,880 pps 100M:148,810 pps 1G:1,488,000 pps 10G:14,880,000 pps
MAC addresses	16K

Table 108. M4300 Switch Specifications

Feature	Value
M4300-12X12F (XSM4324S)	A stackable, fully-managed L2+ Gigabit switch.
	24-port Gigabit Ethernet Layer 2 switch.
	12 10G Copper ports.
	12 10G Fiber ports.
	These are the existing M4300 series switches that have been reconfigured to act as S3300 switches. The capabilities of the switches match the S3300 capabilities.

M4300-24X (XSM4324CS)

A stackable, fully-managed L2+ Gigabit switch.

24-port 10GBaseT with 4 shared SFP+.

These are the existing M4300 series switches that have been reconfigured to act as S3300 switches. The capabilities of the switches match the S3300 capabilities.

Switch Features and Defaults

The tables in this section provide information about the switch features and default values.

Table 109. Feature Default Values and Default State

Feature Name/Parameter	Default
DHCP L2 Relay	
Global	
Admin Mode	Disabled
VLAN	
Admin Mode	Disabled
Circuit ID Mode	Disabled
Interface	
Admin Mode	Disabled
82 Option Trust Mode	Disabled
Stacking	
Global	
Switch Priority	Unassigned
Stack Sample Mode	Cumulative
Stack Port	

Table 109. Feature Default Values and Default State (continued)

Feature Name/Parameter	Default
Configured Stack Mode	Ethernet
Stack Firmware Synchronization	
Stack Firmware Auto Upgrade	Disabled
Traps	Enabled
Allow Downgrade	Enabled
PoE	
Global	
System Usage Threshold	95%
Power Management Mode	Dynamic
Traps	Enabled
Interface	
Admin Mode	Enabled
Port Priority	Low
Power Mode	802.3at
Power Limit Type	User
Power Limit (mW)	30000 (mW)
Detection Type	IEEE 802
Timer Schedule	None
Virtual LAN (IEEE 802.1Q	
Default VLANs	1 (Default), 4089 (Auto-Video) **Note:** 1. All ports member of default VLAN 2. No ports member of Auto-Video VLAN
PVID	1
Acceptable Frame Types	Admit All
Ingress Filtering	Disabled
Port Priority	0
Jumbo Frames	
Maximum Frame Size	1518

Table 109. Feature Default Values and Default State (continued)

Feature Name/Parameter	Default
Flow Control	
Admin Mode	Disabled
802.1X	
Port Based Authentication State	Disabled
VLAN Assignment Mode	Disabled
Dynamic VLAN Creation Mode	Disabled
EAPOL Flood Mode	Disabled
Port Control	Auto
Guest VLAN ID	0
Guest VLAN Period	90
Unauthenticated VLAN ID	0
Periodic Reauthentication	Disabled
Reauthentication Period	3600
Quiet Period	60
Resending EAP	30
Max EAP Requests	2
Supplicant Timeout	30
Server Timeout	30
STP/RSTP/MSTP	
Global	
Spanning Tree State	Enabled
STP Operation Mode	RSTP
Configuration Name	<MAC address>
Configuration Revision Level	0
Forward BPDU while STP Disabled	Disabled
CST Bridge Priority	32768
CST Bridge Max Age	20
CST Bridge Hello Time	2
CST Bridge Forward Delay	15

346

Table 109. Feature Default Values and Default State (continued)

Feature Name/Parameter	Default
CST Spanning Tree Max Hops	20
MST Default Instance ID	0
MST Instance 0 Priority	32768
MST Instance 0 VLAN IDs	1,2,3
PV(R)STP UplinkFast Rate	150
Interface	
CST STP Status	Enabled
CST Auto Edge	Enabled
CST Fast Link	Disabled
CST BDPU Forwarding	Disabled
CST Path Cost	0
CST Priority	128
CST External Path Cost	0
GARP	
Interface	
Join Timer	20 (centiseconds)
Leave Timer	60 (centiseconds)
Leave All Timer	1000 (centiseconds)
GVRP	
Global	
GVRP Mode	Disabled
Interface	
Port GVRP Mode	Disabled
Link Aggregation	
Lag Name	ch<n> where n is 1 to 26
Description	" "
Admin Mode	Enabled
STP Mode	Enabled
Link Trap	Enabled

Table 109. Feature Default Values and Default State (continued)

Feature Name/Parameter	Default
LAG Type	Static
Local Link Discovery Protocol (LLDP)	
Global	
TLV Advertised Interval	30
Hold Multiplier	4
Reinitializing Delay	2
Transmit Delay	5
Fast Start Duration	3
Interface	
Admin Status	Tx and Rx
Management IP Address	Auto Advertise
Notification	Disabled
Optional TLVs	Enabled
DHCP Snooping	
Global	
Admin Mode	Disabled
MAC Address Validation	Enabled
Interface	
Trust Mode	Disabled
Logging Invalid Packets	Disabled
Rate Limit	N/A
Burst Interval	N/A
Persistent Configuration	
Store	Local
Write Delay	300
Audio/Video Bridging (AVB)	
802.1AS	
Global	
802.1AS Status	Disabled

Table 109. Feature Default Values and Default State (continued)

Feature Name/Parameter	Default
Local Clock Priority 1	246
Local Clock Priority 2	248
Interface	
Admin Mode	Enabled
Pdelay Threshold (copper)	2500
Pdelay Threshold (fiber)	8000
Allowed Lost Responses	3
Initial Sync Interval	−3
Initial Pdelay Interval	0
Initial Announce Interval	0
SyncRx Timeout	3
Announce Rx Timeout	3
MRP	
Global	
MVRP Mode	Disabled
MMRP Mode	Disabled
MSRP Mode	Disabled
MSRP talker Pruning	Disabled
Periodic State Machine (MVRP Mode)	Disabled
MSRP Max Fan In Ports	12
MSRP Boundary Propagation	Disabled
802.1Qav Class A EAV Priority	3
802.1Qav Class A EAV Remap Priority	1
802.1Qav Class B EAV Priority	2
802.1Qav Class B EAV Remap Priority	1
Interface	
MVRP Mode	Enabled
MMRP Mode	Disabled
MSRP Mode	Enabled

Table 109. Feature Default Values and Default State (continued)

Feature Name/Parameter	Default
Join Timer	20
Leave Timer	300
Leave All Timer	2000
MSRP SR Class PVID	2
802.1Qav Class A MSRP Delta Bandwidth (percent)	75
802.1Qav Class B MSRP Delta Bandwidth (percent)	0
IP Routing	
Admin Mode	Disabled
Time-To-Live	64
Maximum Next Hops	1
ARP/ARP Aging	
Age Time (seconds)	1200
Response Time (seconds)	10
Retries	10
Cache Size	512
Dynamic Review	Enabled
Router Discovery Protocol	
Advertise Mode	Disabled
Advertise Address	224.0.0.1
Maximum Advertise Interval	600
Minimum Advertise Interval	450
Advertise Lifetime	1800
Preference Level	0
Differentiated Services	
Admin Mode	Disabled
Class of Service (CoS)	
Global	
Trust Mode	802.1p

Table 109. Feature Default Values and Default State (continued)

Feature Name/Parameter	Default
802.1p to Queue Mapping (802.1p -> Queue)	0 -> 1 1 -> 0 2 -> 0 3 -> 1 4 -> 2 5 -> 2 6 -> 3 7 -> 3
DSCP to Queue Mapping (DSCP -> Queue)	Class Selector: (CS 0) 000000 -> 1 (CS 1) 001000 -> 0 (CS 2) 010000 -> 0 (CS 3) 011000 -> 1 (CS 4) 100000 -> 2 (CS 5) 101000 -> 2 (CS 6) 110000 -> 3 (CS 7) 111000 -> 3 Assured Forwarding: (AF 11) 001010 -> 0 (AF 12) 001100 -> 0 (AF 13) 001110 -> 0 (AF 21) 010010 -> 0 (AF 22) 010100 -> 0 (AF 23) 010110 -> 0 (AF 31) 011010 -> 1 (AF 32) 011100 -> 1 (AF 33) 011110 -> 1 (AF 41) 100010 -> 1 (AF 42) 100100 -> 1 (AF 43) 100110 -> 1 Expedited Forwarding: (EF) 101110 -> 2

Table 109. Feature Default Values and Default State (continued)

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

Table 109. Feature Default Values and Default State (continued)

Feature Name/Parameter	Default
Interface	
Trust Mode	802.1p
Interface Shaping Rate	0
802.1p to Queue Mapping (802.1p –> Queue)	0 -> 1 1 -> 0 2 -> 0 3 -> 1 4 -> 2 5 -> 2 6 -> 3 7 -> 3
Queue Minimum Band Width	0
Queue Scheduler Type	Weighted
Auto-VoIP	
Protocol-based	
Admin Mode	Disabled
Prioritization Type	Traffic Class
Traffic Class	3
OUI-based	
Admin Mode	Disabled
Auto-VoIP VLAN	2
OUI-based priority	7

Table 110. Traffic control

Feature	Sets Supported	Default
Storm control	All ports	Disabled
Jumbo frame	All ports	Disabled Max = 9216 bytes

Table 111. Quality of service

Feature	Sets Supported	Default
Number of queues	7	N/A
802.1p	1	Enabled
DSCP	1	Disabled
Rate limiting	All ports	Disabled

Table 112. Security

Feature	Sets Supported	Default
802.1X	All ports	Disabled
MAC ACL	100 (shared with IP and IPv6 ACLs)	All MAC addresses allowed
IP ACL	100 (shared with MAC and IPv6 ACLs)	All IP addresses allowed
IPv6 ACL	100 (shared with IP ACL and MAC ACL)	All IP addresses allowed
Password control access	1	Idle timeout = 5 mins. Password = "password"
Management security	1 profile with 20 rules for HTTP/HTTPS/SNMP access to allow/deny an IP address/subnet	All IP addresses allowed
Port MAC lock down	All ports	Disabled

Table 113. System setup and maintenance

Feature	Sets Supported	Default
Boot code update	1	N/A
DHCP/manual IP	1	DHCP enabled/192.168.0.239
Default gateway	1	192.168.0.254
System name configuration	1	NULL
Configuration save/restore	1	N/A
Firmware upgrade	1	N/A
Restore defaults	1 (web and front-panel button)	N/A

Table 113. System setup and maintenance (continued)

Feature	Sets Supported	Default
Dual image support	1	Enabled
Factory reset	1	N/A

Table 114. System management

Feature	Sets Supported	Default
Multi-session web connections	4	Enabled
SNMPv1/V2c SNMP v3	Max 5 community entries	Enabled (read, read-write communities)
Time control	1 (Local or SNTP)	Local Time enabled
LLDP/LLDP-MED	All ports	Enabled
Logging	3 (Memory/Flash/Server)	Memory Log enabled
MIB support	1	Disabled
Smart Control Center	N/A	Enabled
Statistics	N/A	N/A

Table 115. Other features

Feature	Sets Supported	Default
Timer Schedules	100	Type — Absolute
IGMP snooping v1/v2/v3	All ports	Disabled
Configurations upload/download	1	N/A
EAPoL flooding	All ports	Disabled
BPDU flooding	All ports	Disabled
Static multicast groups	8	Disabled
Filter multicast control	1	Disabled
Number of static routes	32	N/A
Number of routed VLANs	15	N/A
Number of ARP Cache entries	512	N/A
Number of DHCP snooping bindings	8K	N/A
Number of DHCP static entries	1024	N/A

Table 115. Other features (continued)

Feature	Sets Supported	Default
MLD Snooping	N/A	N/A
Protocol and MAC-based VLAN	N/A	N/A
Dynamic ARP Inspection	N/A	Disabled
Multiple VLAN Registration (MVR)	N/A	Disabled
Multiple Registration Protocol (MRP)	N/A	Disabled
802.1AS	N/A	Disabled