


# NETGEAR®

## **XS728T ProSAFE**

**28-Port 10-Gigabit L2+ Smart Switch  
Software Administration Manual**

July 2015  
202-11492-01

350 East Plumeria Drive  
San Jose, CA 95134  
USA



## Support

Thank you for selecting NETGEAR products.

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

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

Phone (Other Countries): Check the list of phone numbers at <http://support.netgear.com/general/contact/default.aspx>.

Contact your Internet service provider for technical support.

## Compliance

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

See the regulatory compliance document before connecting the power supply.

## Trademarks

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

# Contents

## Chapter 1 Getting Started

Switch Management Interface .....	4
Connect the Switch to the Network.....	4
Discover a Switch in a Network with a DHCP Server .....	5
Switch Discovery in a Network Without a DHCP Server.....	5
Configure the Network Settings on the Administrative System .....	6
Access the Management Interface from the Web .....	8
Interface Naming Convention .....	12

## Chapter 2 System

Management .....	16
Device View .....	29
SNMP.....	29
LLDP .....	32
Services—DHCP Snooping .....	40

## Chapter 3 Switching

Ports .....	44
LAG .....	45
VLAN.....	48
Voice VLAN.....	56
Auto-VoIP Configuration .....	58
Spanning Tree Protocol.....	59
Multicast.....	67
Address Table.....	80

## Chapter 4 Routing

IP .....	84
VLAN.....	87
Routing Table .....	89
ARP .....	90
IPv6 .....	93

## Chapter 5 Quality of Service

CoS .....	102
Differentiated Services .....	105

## Chapter 6 Security

Management Security Settings .....	114
Access .....	121
Port Authentication .....	124
Traffic Control .....	129
ACL .....	134

## Chapter 7 Monitoring

Ports .....	150
Logs .....	157
Port Mirroring .....	160
System Resources Utilization .....	161

## Chapter 8 Maintenance

Reset .....	164
Upload .....	164
Download .....	167
File Management .....	170
Troubleshooting .....	171

## Chapter 9 Help

Online Help .....	178
Registration .....	178

## Appendix A Hardware Specifications and Default Values

Switch Features and Defaults .....	182
------------------------------------	-----

## Appendix B Configuration Examples

Virtual Local Area Networks (VLANs) .....	186
Access Control Lists (ACLs) .....	188
Differentiated Services (DiffServ) .....	190
802.1x .....	194
MSTP .....	197
Configure VLAN Routing with Static Route .....	201

# Getting Started

---

# 1

This manual describes how to configure and operate the XS728T ProSAFE 28-Port 10-Gigabit L2+ Smart Switch by using the web-based graphical user interface (GUI). This manual describes the software configuration procedures and explains the options available within those procedures. These switches are referred to as the NETGEAR switch throughout this document.

This chapter provides an overview of starting your NETGEAR switch and accessing the user interface. It also describes some actions that can be performed in 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>.

This chapter contains the following sections:

- *Switch Management Interface*
- *Connect the Switch to the Network*
- *Discover a Switch in a Network with a DHCP Server*
- *Switch Discovery in a Network Without a DHCP Server*
- *Configure the Network Settings on the Administrative System*
- *Access the Management Interface from the Web*
- *Interface Naming Convention*

## Switch Management Interface

The NETGEAR switch contains an embedded web server and management software for managing and monitoring switch functions. The 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 under Windows XP, Windows 2003, Windows 2008 or Windows 7 (32 bit and 64 bit) 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 was 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.

## 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. By default, the switch is also assigned a default gateway of 192.168.0.254.

To change the switch's default network, 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 5.
- **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 [Switch Discovery in a Network Without a DHCP Server](#) on page 5.
- **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-based 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 6.

## 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 automatically assigns an IP address to your switch. To discover the IP address automatically assigned to the switch, use the Smart Control Center.

➤ **To install the switch in a network with a DHCP server, use the following steps:**

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 **Discover** for the Smart Control Center to find your switch.
6. Make a note of the displayed IP address assigned by the DHCP server.

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

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

The Smart Control Center displays a login window.

The default password is **password**. Use this screen to manage your switch. For more information, see [Access the Management Interface from the Web](#) on page 8.

## Switch Discovery 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. 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 **Discover** for the Smart Control Center to find your NETGEAR switch.

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

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

The screen expands to display more fields at the bottom of the screen.

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 and type your password.

**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**.

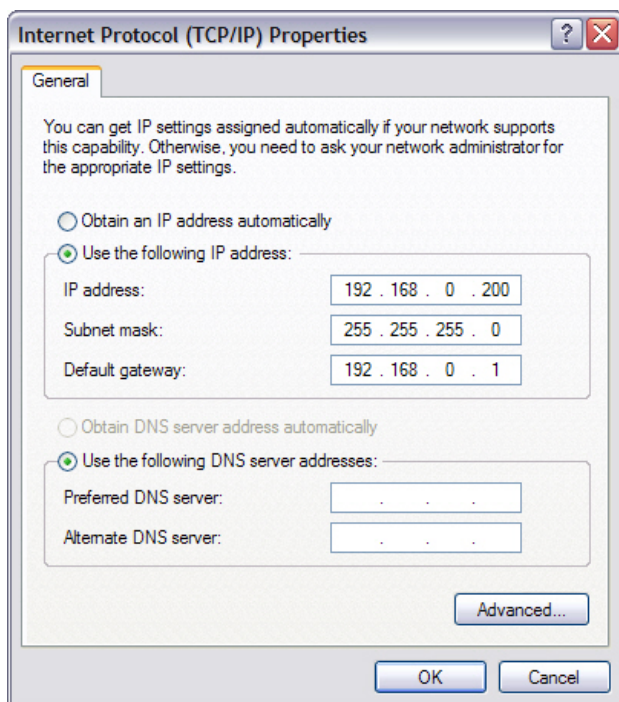
9. Click **Apply** to configure the switch with the network settings.

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 do not use the Smart Control Center to configure the switch network information, 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).

To change the IP address on an administrative system running a Windows operating system, open the Internet Protocol (TCP/IP) Properties screen that you access from each local area connection, as shown in the following screen. You need Windows Administrator privileges to change these settings.

**WARNING:**

**When you change the IP address of your administrative system, connection to the rest of the network is lost. Be sure to write down your current network address settings before you change them.**

➤ **To modify the network settings on your administrative system:**

1. On your computer, access the Windows operating system TCP/IP Properties screen.
2. 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 the switch's address but within the same subnet.

3. Click **OK**.

➤ **To configure a static address on the switch:**

1. Use a straight-through Ethernet cable to connect the Ethernet port on the administrative system directly to any port on the NETGEAR switch.
2. Open a web browser on your computer and connect to the management interface.  
For more information, see [Access the Management Interface from the Web](#) on page 8.
3. Change the network settings on the switch to match the settings on your network.  
For more information, see [IP Configuration on page 20](#).
4. Return the network configuration on your administrative system to the original settings.

## Access the Management Interface from the Web

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

- From the Smart Control Center, select the switch and click **Web Browser Access**. For more information, see the documentation for this application at <http://docs.netgear.com/scc/enu/202-10685-01/index.htm>.
- 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 NETGEAR switch 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 into the address field.

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

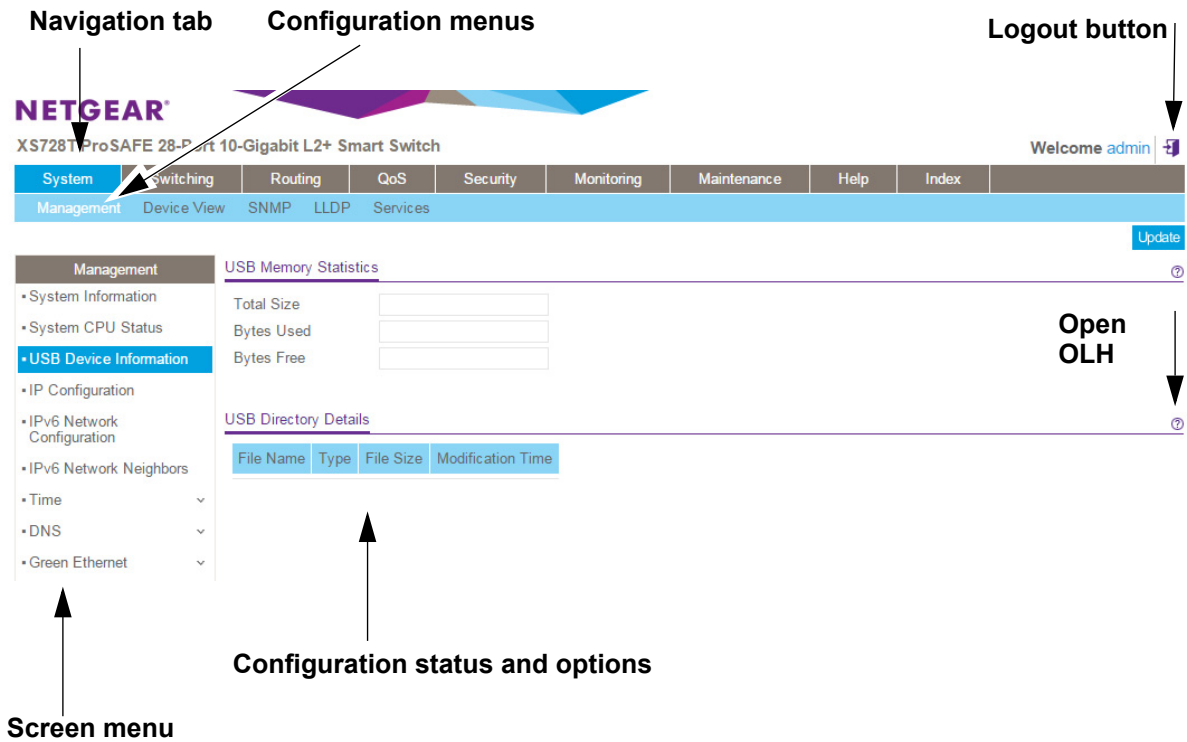
## Understand the User Interface

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

- Internet Explorer versions 9 to 11
- Firefox version 31-33
- Chrome versions 38-40
- Safari
  - On Windows OS: 5.1.7
  - On MAC OS: 8.0.2 (MAC OS version 10.10)

### ➤ To log on to the web interface:

1. Open a web browser and enter the IP address of the switch in the web browser address field.
2. The factory default password is **password**. Type the password in the field on the Login screen and click **Login**. Passwords are case-sensitive.
3. After the system authenticates you, the System Information screen displays.



## 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 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. When you click a menu item that includes multiple configuration screens, additional submenu links are displayed.

## Configuration and Status Options

The area directly below the feature links 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 enter 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	Adds a new entry in a table.
Apply	Sends the updated configuration, entered by user, to the switch.
Cancel	Resets the data on the screen to the latest value of the switch.
Clear	Clears and resets counter information.
Delete	Removes the selected entry from a table.
Update	Reloads the screen with the latest information from the device.
Logout	Ends the session.

## Device View

The Device View is a Java applet that displays the ports on the switch. See [Device View](#) on page 32.

### Link/Speed/ACT-LED Mode for Ports 1 to 24

The following describes these LEDs for ports 1 to 24.

- LED off indicates that no 1G bps/10G bps link is established on the port.
- A solid green LED indicates that a valid 10G bps link is established.
- A blinking green LED indicates that packets transmitting/receiving is occurring at 10 Gbps.
- A solid yellow LED indicates that a valid 1 Gbps link is established.
- A blinking yellow LED indicates that packets transmission/reception is occurring at 1 Gbps.

### Link/Speed/ACT-LED mode for ports SFP+ ports (25 to 28)

The following describes these LEDs for ports 25 to 28.

- LED off indicates that no SFP+ module link is established on the port.
- A solid green LED indicates that a valid 10Gbps SFP+ module link is established on the port.
- A blinking green LED indicates that packets transmission or reception is occurring on the port at 10 Gbps.
- A solid yellow LED indicates that a valid 1 Gbps SFP module link is established on the port.
- A blinking yellow LED indicates that packets transmission or reception is occurring on the port at 1 Gbps.

## 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 device is powered on and run-time code is up and running.
- A solid yellow LED indicates that system is in the boot-up stage.
- LED off indicates that power is not being supplied to the device.

### FAN Status LED

FAN status is indicated as follows:

- A solid yellow LED indicates that one or more of the fans is faulty.
- LED off indicates that all of the fans are operating normally.

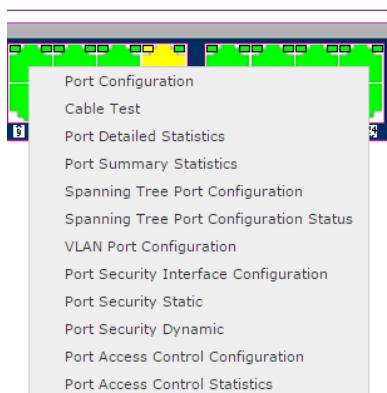
### Port Access

The following image shows the device view of the NETGEAR switch.




Click the port you want to view or configure to see a menu that displays statistics and configuration options. Click the menu option to access the screen that contains the configuration or monitoring options.

To display a menu for a port, right-click the port graphic and its menu displays:



### Help Screen Access

Every screen contains a link to the online help  , which contains information to help configure and manage 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 1, Configuration Status and Options* 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 on the configuration web screen. All characters can be used except for the following (unless specifically noted in for that feature):

\            <  
/            >|  
\*            |  
?

## Use SNMP

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 more switch functionality. 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** web screen, which displays after a successful login, displays the information you need to configure an SNMP manager to access the switch.

Any user can connect to the switch using the SNMPv3 protocol. However, for authentication and encryption, the switch only supports a single user called **admin**, which is the only profile that can be created or modified.

See *SNMP* on page 32 for more information

## Interface Naming Convention

The switch supports physical and logical interfaces. Interfaces are identified by their type and the interface number. The switches support the following types of ports:

- Ports 1–28 are 1G/10G 10 Gigabit ports.
  - Ports 1-24 are copper ports (RJ45).
  - Ports 25–28 are fiber ports (SFP+).

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 2. Naming Convention for Switch Interfaces**

Interface	Description	Example
Physical	The physical ports are numbered sequentially starting from 1.	xg1 ... xg28
Link aggregation group (LAG)	LAG interfaces are logical interfaces that are used only for bridging functions.	LAG1 ... LAG8



## 2 System

---

# 2

Use the features in the System tab to define the switch's relationship to its environment. The System tab contains links to screens described in the following sections:

- *Management*
- *Device View*
- *SNMP*
- *LLDP*
- *Services—DHCP Snooping*

## Management

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

- *System Information*
- *System CPU Status*
- *USB Device Information*
- *IP Configuration*
- *IPv6 Network Configuration*
- *IPv6 Network Neighbors*
- *Time*
- *DNS*
- *Green Ethernet*

## System Information

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

### ➤ To define system information:

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

The **Product Name** is displayed, as well as current software and boot version info.

2. Define the following fields:

- **System Name.** Enter the name you want to use to identify this switch. You can use up to 160 alphanumeric characters. The factory default is blank.
- **System Location.** Enter the location of this switch. You can use up to 160 alphanumeric characters. The factory default is blank.
- **System Contact.** Enter the contact person for this switch. You can use up to 160 alphanumeric characters. The factory default is blank.

3. Click **Apply** to apply the changes to the system.

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

Field	Description
Serial Number	The serial number of the switch.
System Object ID	The base object ID for the switch's enterprise MIB.
Date & Time	The current date and time.

Field	Description
System Up Time	Displays the number of days, hours, minutes and seconds since the last system restart.
Base MAC Address	Universally assigned network address.
IC Temp (C)	Integrated circuit temperature in Celsius values.
Fan Status for Fans 1-4	The status of fan operations.
Model Name	The model name of the switch.
Boot Version	The boot code version of the switch.
Software Version	The software version of the switch.

## System CPU Status

Use this screen to view system RAM memory information and CPU utilization.

### ➤ To enable CPU utilization:

#### 1. Select **System > Management > System CPU Status**.

The following fields are displayed:

- **Total System Memory.** Amount of total RAM memory available on the device.
- **Available Memory.** Amount of unused RAM memory on the device.

#### 2. Configure the following fields to enable or disable calculation of the CPU utilization:

- **CPU Utilization.** Select Disable or Enable. The default value is Enable.
- **Refresh Rate.** Select the number of seconds indicating how frequently CPU utilization will be computed.

The **CPU Input Rate**, which is the number of frames forwarded to CPU per second, is displayed.

The **CPU Utilization Rate**, which is the number of frames forwarded to CPU per second is displayed in a graph at the bottom of the page. The number of values displayed on the x axis is correlated to the refresh rate.

## USB Device Information

Use this screen to view the files on the external USB Memory device, connected to the device via USB port on device front panel.

Supported USB disks must:

- Comply with USB 2.0.
- Support file type of FAT32.

➤ **To view the USB directories and files:**

Select **System > Management > USB Device Information**.

The following fields are displayed:

- **Total Size.** Size of the USB memory.
- **Bytes Used.** Number of bytes used.
- **Bytes Free.** Number of bytes remaining to be used.

The following fields are displayed for each file stored in the USB.

- **File Name.** Name of file or name of directories included in the selected parent folder.
- **Type.** Type of file, which can be one of the following:
  - **Folder.** Entry in this line relates to a sub-folder within current folder being viewed.

You can click on folder name to view the contents of the sub-folder.

- **File.** Entry in line relates to a file.
- **Other.** Entry in line relates to current or parent folder path.
  - **Current path entry.** Displays full path information for current folder being displayed
  - **Parent folder path entry.** Allows you to click on this entry and return to parent folder.
- **File Size.** Size of file or folder in bytes.
- **Modification Time.** Last time file was changed.

## 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**.
2. Select the appropriate radio button in the **Current Network Configuration Protocol** field to determine how to configure the network information for the switch management interface:
  - **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.
  - **Dynamic IP Address (DHCP).** Specifies that the switch will obtain the IP address through a DHCP server.
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 0. 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 IP address assigned to the default gateway 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 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 [VLAN](#) on page 53.

---

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 must be reconnected to the port in the new management VLAN.
5. Click **Apply** to apply the changes to the system.

## 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 any of the switch's front-panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front-panel ports through which traffic is switched or routed.

To access the switch over a IPv6 network, you must initially configure the switch with IPv6 information (IPv6 prefix, prefix length, and default gateway). IPv6 can be configured using IPv6 auto configuration.

When in-band connectivity is established, IPv6 information can be changed using any of the following:

- SNMP-based management
- Web-based management

The IPv6 network interface uses the same VLAN as the IPv4 network interface.

➤ **To configure the global settings for an IPv6 Interface:**

1. Select **System > Management > IPv6 Network Configuration**.
2. In the Global Configuration section, configure the following:
  - **Admin Mode.** Enable or disable the IPv6 network interface on the switch. The default value is Enable.
  - **IPv6 Address Auto Configuration Mode.** The IPv6 address for the IPv6 network interface is automatically configured if this option is enabled. The default value is Disable.
  - **IPv6 Gateway.** Specify the gateway for the IPv6 network interface. The gateway address is in IPv6 global or link-local address format.
3. Click **Apply** to apply the changes to the system.

➤ **To add or modify IPv6 addresses on the network interface:**

1. Select **System > Management > IPv6 Network Configuration**.
2. in the IPv6 Network Interface Configuration section, configure the following:
  - **IPv6 Prefix/Prefix Length.** Select an existing IPv6 prefix and prefix length from the list, or add a new IPv6 prefix and prefix length to the list of IPv6 addresses. The address is in the global address format.
  - **EUI64.** Specify whether the IPv6 address is in EUI-64 format. The default value is False.
3. Click **Add** to add a new IPv6 address, or click **Delete** to delete a selected IPv6 address from the list of IPv6 addresses.
4. Click **Apply** to apply the changes to the system.

## IPv6 Network Neighbors

➤ **To view the IPv6 Network Interface Neighbors:**

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

Properties of each neighbor are displayed, as described below:

- **IPv6 Address.** Specifies the IPv6 address of the neighbor interface.
- **MAC Address.** Specifies the MAC address associated with the neighbor 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.** Specifies the state of the neighbor cache entry. The following are the states for dynamic entries in the IPv6 neighbor discovery cache:
  - **Reach.** No more than ReachableTime milliseconds have elapsed since confirmation was received that the forward path to the neighbor was functioning properly. When in REACH state, the device takes no special action as packets are sent.
  - **Stale.** More than ReachableTime milliseconds have elapsed since a confirmation was last received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.
  - **Delay.** More than ReachableTime milliseconds have elapsed since a confirmation was last received that the forward path was functioning properly. A packet was sent within the last DELAY\_FIRST\_PROBE\_TIME seconds. If no confirmation is received within DELAY\_FIRST\_PROBE\_TIME seconds of entering the DELAY state, the device sends a neighbor solicitation message and changes the state to PROBE.
  - **Probe.** A confirmation is actively sought by repeatedly sending neighbor solicitation messages every RetransTimer milliseconds until a confirmation is received.
- **Last Updated.** Elapsed time since the address was last confirmed as reachable.

## Time

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

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

Time sources are established by stratum. Stratum defines the accuracy of the reference clock. The higher the stratum (where 0 is the highest), the more accurate the clock. The switch is a stratum 2 device, and as such accepts stratum 1 or higher time indications.

The following is an example of stratum:

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

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

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

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

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

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

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

From the Time menu, you can access features described in the following sections:

- *SNTP Global Configuration*
- *SNTP Server Configuration*
- *Daylight Savings Time*

## SNTP Global Configuration

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

### ➤ To manually configure the time:

1. Select **System > Management > Time > SNTP Global Configuration**.
2. Next to the **Clock Source**, select **Local**.
3. In the **Date** field, enter the date in the DD-MMM-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 calculates the date and time using the CPU's clock cycle.

---

When the clock source is set to Local, the **Time Zone Offset** field is disabled.

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

### ➤ To configure the time through SNTP:

1. Next to the **Clock Source**, select **SNTP**.

When the clock source is set to **SNTP**, the **Date** and **Time** fields are disabled. The switch gets the date and time from the network.

2. In the **Time Zone Offset** list, select the Coordinated Universal Time (UTC) time zone in which the switch is located, expressed as the number of hours.
3. Use the SNTP Server Configuration screen to configure the SNTP server settings.
4. Click **Apply** to send the updated configuration to the switch.

Configuration changes take effect immediately.

The SNTP Global Status table on the SNTP Global Configuration screen displays information about the system's SNTP client.

The following table describes the SNTP Global Status fields.

Field	Description
Version	Specifies the SNTP version the client supports.
Supported Mode	Specifies the SNTP modes the client supports. Multiple modes might be supported by a client.
Last Update Time	Specifies the local date and time (UTC) the SNTP client last updated the system clock.
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.
Server Mode	Specifies the mode of the server for the last received valid packet.
Unicast Server Max Entries	Specifies the maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	Specifies the number of current valid unicast server entries configured for this client.

## 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**.
2. Enter the appropriate SNTP server information in the following fields:
  - **Server Type**. Specifies whether the address for the SNTP server is an IP address (IPv4) or host name (DNS).
  - **Address**. Enter the IP address or the host name of the SNTP server.
  - **Port**. Enter a port number on the SNTP server to which SNTP requests are sent. The valid range is 1–65535. The default is 123.
3. Click **Add**.

Repeat the previous steps to add more SNTP servers. You can configure up to 8 SNTP servers.

➤ **To change the settings for an existing SNTP server:**

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

Configuration changes take effect immediately.

➤ **To remove an SNTP server:**

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

The entry is removed, and the device is updated.

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

Field	Description
Address	Specifies all the existing server addresses.
Last Update Time	Specifies the local date and time (UTC) of the server response, according to which the system clock was updated. The update interval is 1024 seconds.

## Daylight Savings Time

Use this screen to configure Day Light Savings (DST) time on the device. Used in some countries around the world, summer time is the Configure System Information practice of temporarily advancing clocks during the summer months. Typically clocks are adjusted forward 1 or more hours near the start of spring and are adjusted backward in autumn.

➤ **To configure a new SNTP server:**

1. Select **System > Management > Time > DayLight Saving (DST) Configuration**.
2. Next to Summer Time, select one of the following options:
  - **Disable**. Disable DST.
  - **Recurring**. 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**. The system clock uses the standard recurring summer time settings used in countries in the European Union. When this field is selected, the applicable fields for start and end times for the time shift fields on the screen are automatically populated and cannot be edited.
  - **Recurring USA**. The system clock uses the standard recurring daylight saving time settings used in the United States. When this field is selected, the applicable fields for start and end times for the time shift fields on the screen are automatically populated and cannot be edited.

---

**Note:** For both US and EU recurring time ranges, add the settings of offset and zone (just like for recurring time ranges).

---

- **Non Recurring.** 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. If the selected summer time mode is Recurring or Non Recurring, set the start and end times for the time shift:
    - **Begins At.** From the appropriate lists, select the date and time on which summer time begins.
    - **Ends At.** From the appropriate lists, select the date and time on which summer time ends.
  4. In the **Offset** field, specify the number of minutes to shift the summer time from the standard time. The default time shift is 60 minutes.
  5. In the **Zone** field, specify the acronym associated with the time zone when summer time is in effect.

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

6. Click the **Apply** button.

The **DayLight Saving (DST) Status** table shows information about the DST time settings and whether the time shift for summer time is currently in effect. The **DayLight Saving (DST)** displays whether DST is enabled; **DayLight Saving (DST) in Effect** displays whether is actually in effect.

## DNS

Use the DNS screens to configure information about DNS servers used by the network and DNS client settings for the switch.

From the DNS menu, you can access features described in the following sections:

- *DNS Configuration*
- *Host Configuration*

### DNS Configuration

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**.
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. In the **DNS Default Name** field, enter a default DNS name to include in DNS queries. When the system is performing a lookup on an unqualified host name, this field is provided as the domain name. For example, if the default domain name is netgear.com and the host name to resolve is test, test.netgear.com is used in DNS resolution queries.
  4. In the **DNS Server** field, enter an IP address representing the DNS server to which the switch sends DNS queries, and click **Add**. The server appears in the DNS Server list.
    - Use standard IPv4 dot notation.
    - You can specify up to eight DNS servers.
    - DNS server precedence is set according to the creation order.
  5. In the **Preference** field, specify a preference value for the server.
  6. Click **Apply** to send the updated configuration to the switch.  
Configuration changes take effect immediately.

## Host Configuration

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**.
2. Specify the static host name to add.
  - Enter up to 158 characters.
  - Each label (separated by periods) can be up to 63 characters.
3. Specify the IP or IPv6 address to associate with the hostname.
4. Click **Add**. The entry displays in the list.

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.

Field	Description
Host	Lists the host name you assign to the specified IP address.
Type	The type of the dynamic entry.
IPv4/IPv6 Address	Lists the IP address associated with the host name.

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

## Green Ethernet

The Green Ethernet features enable the switch to reduce power consumption on a per-port basis. Each switch can support one or more of the following features:

- **Auto Power Down Mode.** Auto Power Down mode is always enabled. When the port link is down, the physical layer (PHY) automatically shuts down for a short period and wakes up to check link pulses. This mode reduces power consumption on the port when no link partner is present.
- **Short Cable Mode.** Short Cable mode is always enabled. When the cable length is less than a certain limit, the PHY goes into low-power mode.
- **Energy Efficient Ethernet (EEE) Mode.** EEE enables ports to enter a low-power mode to reduce power consumption during periods of low link utilization. EEE is defined by IEEE 802.3az. EEE enables both the send and receive sides of the link to disable some functionality for power savings when the link is lightly loaded. By default this feature is disabled globally and per interface.

From the Green Ethernet menu, you can access features described in the following sections:

- [Green Ethernet Configuration](#)
- [Green Ethernet Interface Configuration](#)
- [Green Ethernet Detail](#)
- [Green Ethernet Summary](#)

## Green Ethernet Configuration

### ➤ To configure the Green Ethernet Configuration features:

1. Select **System > Management > Green Ethernet > Green Ethernet Configuration**.
2. The Auto Power Down Mode and Short Cable Mode features are enabled and cannot be disabled.
3. Enable or disable the EEE Mode.
  - **Enable.** Enter a low-power mode and disable some functionality for power savings when the link is lightly loaded.
  - **Disable.** Provide full power to the PHY always.
4. Click **Apply** to apply the change to the system.  
Configuration changes take effect immediately.

## Green Ethernet Interface Configuration

Using the Green Ethernet Interface Configuration feature allows for proper port configuration and the ability to enable or disable EEE Mode on specific ports.

### ➤ To configure the Green Ethernet Interface feature:

1. Select **System > Management > Green Ethernet > Green Ethernet Interface Configuration**.
2. Select the following interface settings for the physical port:
  - **Go To Interface.** Enter a port identifier (appears in the Port column) and click **Go**. The table entry corresponding to the specified port is selected.

- **Port.** Selects the interface for which data is displayed or configured.
  - **EEE Mode.** Determines whether Energy Efficient Ethernet (EEE) mode is enabled for the port.
3. Click **Apply** to apply the change to the system.  
Configuration changes take effect immediately.

## Green Ethernet Detail

Use this screen to display or configure Green Ethernet details per interface.

### ➤ To configure the Green Ethernet Detail feature:

1. Select **System > Management > Green Ethernet > Green Ethernet Detail**.
2. View or configure the Local Device Information:
  - **Interface.** The interface to be displayed or configured.
  - **Energy Detect Admin Mode.** Only **Enable** is supported.
  - **Operational Status.** Displays the Energy Detect operational status, either Active or Inactive.
  - **Reason.** Displays the reason for operational status - Active or Inactive.
  - **Short Reach Admin Mode.** Only **Enable** is supported.
  - **Operational Status.** Displays the Short Reach operational status of the port, either Active or Inactive.
  - **Reason.** Displays the reason why the port is either Active or Inactive.
  - **EEE Admin Mode.** Select **Enable** or **Disable**.
  - **Tw\_sys\_tx (uSec).** Displays the amount of time the Tw\_sys\_tx has been present on the port.
  - **Tw\_sys\_tx Echo (uSec).** Displays the amount of time the Tw\_sys\_tx Echo has been present on the port.
  - **Tw\_sys\_rx (uSec).** Displays the amount of time the Tw\_sys\_rx has been present on the port.
  - **Tw\_sys\_rx Echo (uSec).** Displays the amount of time the Tw\_sys\_rx Echo has been present on the port.
3. View the Remote Device Information:
  - **Interface.** If local interfaces are enabled to receive LLDP data, this feature allows you to select the remote device and retrieve port information.
  - **Remote ID.** Displays the remote port identifier.
  - **Remote Tw\_sys\_tx (uSec).** Displays the amount of time the Remote Tw\_sys\_tx has been present on the port.
  - **Remote Tw\_sys\_tx Echo (uSec).** Displays the amount of time the Remote Tw\_sys\_tx Echo has been present on the port.

- **Remote Tw\_sys\_rx (uSec)**. Displays the amount of time the Remote Tw\_sys\_rx has been present on the port.
- **Remote Tw\_sys\_rx Echo (uSec)**. Displays the amount of time the Remote Tw\_sys\_rx Echo has been present on the port.

## Green Ethernet Summary

This screen summarizes the Green Ethernet Summary settings and status per interface.

### ➤ To access the Green Ethernet Summary screen:

1. Select **System > Management > Green Ethernet > Green Ethernet Summary**.
2. In the Green Mode Statistics Summary section, view the following:
  - **Cumulative Energy Saving (Watts\*Hours)**. Displays the cumulative energy savings on the local device.
3. In the Green Ethernet Interface Summary section, view the following:
  - **Interface. Lists** the local interfaces on the device.
  - **Energy Detect Admin Mode**. Displays the Energy Detect Admin mode for each of the local interfaces (always Enabled).
  - **Energy Detect Operational Status**. Displays the operational status of the Energy Detect mode for each of the local interfaces (Active or Inactive).
  - **Short Reach Admin Mode**. Displays the Short Reach Admin Mode for each of the local interfaces (always Enabled).
  - **Short Reach Operational Status**. Displays the operational status of the Short Reach Admin mode for each of the local interfaces (Active or Inactive).
  - **EEE Admin Mode**. Displays the EEE Admin mode for each of the local interfaces (Enable or Disable).

## 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**.

## SNMP

From SNMP menu under the System tab, you can configure SNMP settings for SNMP v1/v2 and SNMPv3.

SNMP features are described in the following sections:

- *SNMP v1/v2*

- [Trap Flags](#)
- [SNMP Supported MIBs](#)
- [SNMP v3 User Configuration](#)

## SNMP v1/v2

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

### Community Configuration

By default, two SNMP Communities exist:

- **Private.** Read/Write privileges and status set to **Enable**.
- **Public.** Read-only privileges and status set to **Enable**.

These communities are well-known. To change the defaults or to add other communities, use the Community Configuration screen. Only the communities that you define using this screen have access to the switch using the SNMPv1 and SNMPv2c protocols. Only communities with read/write access can be used to change the configuration using SNMP.

#### ➤ To add a new SNMP community:

1. Select **System > SNMP > SNMP v1/v2 > Community Configuration**.
2. To add a new SNMP community, enter community information in the available fields described below.
  - **Management Station IP.** Specify the IP address of the management station. 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 value (Management Station IP or Management Station IP Mask) is 0.0.0.0, access is allowed from any IP address. Otherwise, bitwise AND operations are performed between every client's address and the mask, and between the management station IP address and the mask. If the values are equal, access is allowed. For example, if the management station IP and mask parameters are 192.168.1.0/255.255.255.0, any client whose address is 192.168.1.0 through 192.168.1.255 (inclusive) is allowed access. To allow access from only one station, use a Mask value of 255.255.255.255, and use that machine's IP address for as the client address.
  - **Management Station IP Mask.** Specify the subnet mask to associate with the management station IP address.
  - **Community String.** Specify a community name. A valid entry is a case-sensitive string of up to 16 characters.
  - **Access Mode.** Specify the access level for this community by selecting Read/Write or Read Only.
  - **Status.** Specify the status of this community by selecting Enable or Disable from the pull down menu. If you select Enable, the Community Name must be unique among

all valid Community Names or the set request is rejected. If you select Disable, the Community Name becomes invalid.

3. Click **Add**.  
Configuration changes take effect immediately.

## Trap Configuration

This screen displays an entry for every active Trap Receiver.

### ➤ To configure SNMP trap settings:

Select **System > SNMP > SNMP v1/v2 > Trap Configuration**.

### ➤ To add a host that receives SNMP traps:

1. Enter trap configuration information in the following fields:
  - **Recipients IP**. The address in x.x.x.x format to receive SNMP traps from this device.
  - **Version**. The trap version used by the receiver.
    - **SNMP v1**. Uses SNMP v1 to send traps to the receiver.
    - **SNMP v2**. Uses SNMP v2 to send traps to the receiver.
  - **Community String**. The community string for the SNMP trap packet sent to the trap manager. This community string can be up to 16 characters and is case-sensitive.
2. Click **Add**.  
Configuration changes take effect immediately.

### ➤ To modify an existing SNMP recipient:

1. Select the check box next to the recipient, and change the desired fields.
2. Click **Apply**.  
Configuration changes take effect immediately.

## 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 encounters 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**.
2. From the **All** field, globally enable or disable activation of all traps by selecting the corresponding button.  
The factory default is **Enable**.
3. From the **Authentication** field, enable or disable activation of authentication failure traps by selecting the corresponding button.

The factory default is **Enable**.

4. Click **Apply**.

Configuration changes take effect immediately.

## SNMP Supported MIBs

The screen allows you to view a list of the supported MIBs.

➤ **To display the Supported MIBS screen:**

Select **System > SNMP > SNMP v1/v2 > Supported MIBS**.

## SNMP v3 User Configuration

This is the configuration for SNMP v3.

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.

➤ **To configure SNMPv3 settings for the user account:**

1. Select **System > SNMP > SNMP v3 > User Configuration**.
2. Next to Authentication Protocol, select the SNMPv3 Authentication Protocol setting for the selected user account. The following are the valid authentication protocols:
  - **None**. No authentication is performed
  - **MD5** or **SHA**. The user login password is used as SNMPv3 authentication password, and you must therefore specify a password. The password must be eight characters in length.
3. Next to **Encryption Protocol**, select whether to encrypt SNMPv3 packets transmitted by the switch.
  - **None**. Do not encrypt the contents of SNMPv3 packets transmitted from the switch.
  - **DES**. Encrypt SNMPv3 packets using the DES encryption protocol.
4. If you selected DES for the **Encryption Protocol**, enter the SNMPv3 encryption key in the **Encryption Key** field. Otherwise, this field is ignored. Valid keys are 0–15 characters long.
5. Click **Apply**.  
Configuration changes take effect immediately.

## LLDP

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

From the LLDP menu, you can access the features described in the following sections:

- *LLDP Configuration*
- *LLDP Port Settings*
- *LLDP-MED Network Policy*
- *LLDP-MED Port Settings*
- *Local Information*
- *Neighbors Information*

LLDP is a one-way protocol; there are no request-response sequences. Stations advertise information by implementing the transmit function, and stations implementing the receive function receive and process information. The transmit and receive functions can be enabled or disabled separately per port. By default, both the transmit and receive functions 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:

- Autodiscovery 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 number and asset number).

## LLDP Configuration

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

### ➤ To configure global LLDP settings:

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

---

**Note:** You can also access the LLDP Configuration screen by selecting **System > LLDP > Advanced > LLDP Configuration**.

---

2. Configure the following LLDP settings:
  - **TLV Advertised Interval.** Specify the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32768 seconds.
  - **Hold Multiplier.** Specify multiplier on the transmit interval to assign to Time-to-Live (TTL). The default is 4, and the range is 2–10.

- **Reinitializing Delay.** Specify the delay before a reinitialization. The default is 2 seconds, and the range is 1–10 seconds.
  - **Transmit Delay.** Specify the interval for the transmission of notifications. The default is 5 seconds, and the range is 2–3600 seconds.
3. To change the LLDP-MED properties in the **Fast Start Duration** field, specify the number of LLDP packets sent when the LLDP-MED Fast Start mechanism is initialized.

This occurs when a new endpoint device links with the LLDP-MED network connectivity device. The default value is 3, and the range is from 1–10.

4. Click **Apply**.

Configuration changes take effect immediately.

## LLDP Port Settings

Use the LLDP Port Settings screen to specify LLDP parameters that are applied to a specific interface.

### ➤ To configure LLDP port settings:

1. Select **System > LLDP > Advanced > LLDP Port Settings**.
2. Select the check box next to one or more ports.
3. Specify the following LLDP port settings:
  - **Interface.** Specifies the port affected by these parameters.
  - **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 & Rx.** Enable both transmitting and receiving LLDP PDUs on the selected ports. This value is the default value.
    - **Disabled.** Do not transmit or receive LLDP PDUs on the selected ports.
  - **Management IP Address.** Select whether to advertise the management IP address from the interface. The possible 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.
  - **Notification.** When notifications are enabled, LLDP interacts with the trap manager to notify subscribers of remote data change statistics. The default is Disabled.
  - **Optional TLVs.** Enable or disable the transmission of optional type-length value (TLV) information from the interface. The optional 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 16. For information about how to configure the port description, see *Ports* on page 48.
4. Click **Apply** to apply the new settings to the system.

## LLDP-MED Network Policy

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

➤ **To view LLDP-MED information:**

1. Select **System > LLDP > Advanced > LLDP-MED Network Policy**.
2. From the **Interface** menu, select the interface for which you want to view information.

The following LLDP-MED network policy information displays:

- **Network Policy Number.** The policy number.
- **Application.** The media application type associated with the policy. Only the Voice application type is supported. The application type that is received on the interface has the VLAN ID, priority, DSCP, *tagged* bit status, and *unknown* bit status. This information is displayed only if a network policy TLV has been transmitted.
- **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.

## 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**.
2. From the **Port** list, select the port to configure.
3. From the **LLDP-MED Status** list, enable or disable the LLDP-MED mode for the selected interface. Default is enable.
4. From the **Notification** list, select Enable or Disable to specify whether the port must send a topology change notification if a device is connected or removed. Default is enable.
5. From the **Transmit Optional TLVs** list, select Enable or Disable to specify whether the port must transmit optional type length values (TLVs) in the LLDP PDU frames. Default is enable.

If enabled, the following LLDP-MED TLVs are transmitted:

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

6. Click **Apply** to apply the new settings to the system. Configuration changes take effect immediately.

## Local Information

Use the LLDP Local Information screen to view the data that each port advertises through LLDP.

➤ **To display the LLDP Local Device Information screen:**

1. Select **System > LLDP > Advanced > Local Information**.

The following table describes the device information displayed:

Field	Description
Chassis ID Subtype	Type of chassis ID (for example, MAC address).
Chassis ID	Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device appears
System Name	Name of device.
System Description	Description of the device (in alpha-numeric format).
System Capabilities	Primary functions of the device, such as bridge, WLAN AP, or router.

The following table describes the LLDP local information that displays for each port.

Field	Description
Interface	The interface with the information to display.
Port ID Subtype	Identifies the type of data displayed in the Port ID field.
Port ID	Identifies the port ID according to the Port ID subtype setting.
Port Description	Identifies the user-defined description of the port. For information about how to configure the port description, see <a href="#">Ports</a> on page 48.
Advertisement	Displays the advertisement status of the port.

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

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

Field	Description
<b>Managed Address</b>	
Address SubType	Displays the type of address the management interface uses, such as an IPv4 address.
Address	Displays the address used to manage the device.

Field	Description
Interface SubType	Displays the port subtype.
Interface Number	Displays the number that identifies the port.
<b>MAC/PHY Details</b>	
Auto-Negotiation Supported	Specifies whether the interface supports port-speed autonegotiation. Possible values are True and False.
Auto-Negotiation Enabled	Displays the port speed autonegotiation support status. The possible values are True (enabled) and False (disabled).
Auto Negotiation Advertised Capabilities	Displays the port speed autonegotiation capabilities such as 1000BASE-T half-duplex mode or 100BASE-TX full-duplex mode.
Operational MAU Type	Displays 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.
<b>MED Details</b>	
Capabilities Supported	Displays the MED capabilities enabled on the port.
Current Capabilities	Displays the TLVs advertised by the port.
Device Class	Network Connectivity indicates that the device is a network connectivity device.
<b>Network Policies</b>	
Application Type	Specifies the media application type associated with the policy.
VLAN ID	Specifies the VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	Specifies the priority associated with the policy.
DSCP	Specifies 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 display the LLDP Neighbors Information screen:**

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

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

Field	Description
MSAP Entry	Displays the Media Service Access Point (MSAP) entry number for the remote device.
Local Port	Displays the interface on the local system that received LLDP information from a remote system.
Chassis ID SubType	Identifies the type of data displayed in the Chassis ID field on the remote system.
Chassis ID	Identifies the remote 802 LAN device's chassis.
Port ID SubType	Identifies the type of data displayed in the remote system's <b>Port ID</b> field.
Port ID	Identifies the port ID according to the Port ID subtype setting.
System Name	Identifies 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 more information about the remote device, click the link in the **MSAP Entry** column.

The following table describes the information that displays for a selected port:

Field	Description
<b>Port Details</b>	
Local Port	Displays the interface on the local system that received LLDP information from a remote system.
MSAP Entry	Displays the Media Service Access Point (MSAP) entry number for the remote device.
<b>Basic Details</b>	
Chassis ID Subtype	Identifies the type of data displayed in the Chassis ID field on the remote system.
Chassis ID	Identifies the remote 802 LAN device's chassis.
Port ID Subtype	Identifies the type of data displayed in the remote system's Port ID field.
Port ID	Identifies the physical address of the port on the remote system from which the data was sent.
Port Description	Identifies the user-defined description of the port.
System Name	Identifies the system name associated with the remote device.
System Description	Specifies the description of the selected port associated with the remote system.
System Capabilities	Specifies the system capabilities of the remote system.
<b>Managed Addresses</b>	

## XS728T ProSAFE 28-Port 10-Gigabit L2+ Smart Switch

Field	Description
Address SubType	Specifies the type of the management address.
Address	Specifies the advertised management address of the remote system.
Interface SubType	Specifies the port subtype.
Interface Number	Identifies the port on the remote device that sent the information.
<b>MAC/PHY Details</b>	
Auto-Negotiation Supported	Specifies whether the remote device supports port-speed auto negotiation. Possible values are True and False.
Auto-Negotiation Enabled	Displays the port speed auto negotiation support status. Possible values are True and False.
Auto Negotiation Advertised Capabilities	Displays the port speed auto negotiation capabilities.
Operational MAU Type	Displays 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.
<b>MED Details</b>	
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: <ul style="list-style-type: none"> <li>• Endpoint Class 1. Indicates a generic endpoint class, offering basic LLDP services.</li> <li>• Endpoint Class 2. Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features.</li> <li>• 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.</li> </ul>
PoE Device Type	Port PoE type; for example, powered.
PoE Power Source	Port power source.
PoE Power Priority	Port power priority.
PoE Power Value	Port power value.
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.
Manufacturer Name	The manufacturer name advertised by the remote device.
Model Name	The model name advertised by the remote device.

Field	Description
Asset ID	The asset ID advertised by the remote device.
<b>Location Information</b>	
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	Specifies unknown location information for the remote device.
<b>Network Policies</b>	
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.
<b>LLDP Unknown TLVs</b>	
Type	The unknown TLV type field.
Value	The unknown TLV value field.

## Services—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 each of the local untrusted interfaces of a switch.

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.

From the Services menu, you can access features described in the following sections:

- [DHCP Snooping Global Configuration](#)
- [DHCP Snooping Interface Configuration](#)

- *DHCP Snooping Binding Configuration*
- *DHCP Snooping Persistent Configuration*

## DHCP Snooping Global Configuration

### ➤ To configure DHCP snooping global settings:

1. Select **System > Services > DHCP Snooping > Global Configuration**.
2. Next to **DHCP Snooping Mode**, select **Enable** or **Disable** to turn the DHCP snooping feature on or off. The factory default is disabled.
3. Next to **MAC Address Validation**, select **Enable** or **Disable** to turn on or off the MAC address validation feature. MAC address validation is enabled by default.
4. Enter the VLAN in the **VLAN ID** field to enable the DHCP snooping mode.
5. Select **Enable** or **Disable** from the **DHCP Snooping Mode** list to enable or disable the DHCP snooping feature for entered VLAN. The factory default is disabled.
6. Click **Apply** to apply the change to the system.  
Configuration changes take effect immediately.

## DHCP Snooping 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**.
2. In the **Go To Interface** field, enter the interface name and click **Go**.  
The entry corresponding to the specified interface is selected.
3. To configure DHCP snooping interface settings, click **PORTS**, **LAGS**, or **All**.
4. Select the check box next to the port or LAG to configure.  
  
You can select multiple ports and LAGs to apply the same setting to the selected interfaces. To apply the same settings to all interfaces, select the check box in the heading row.
5. Select the **Trust Mode** for the selected ports or LAGs.  
  
If you select **Enable**, DHCP snooping application considers the port as trusted. The factory default is disabled.
6. Click **Apply** to apply the change to the system.  
Configuration changes take effect immediately.

## DHCP Snooping Binding Configuration

➤ **To configure DHCP binding settings:**

1. Select **System > Services > DHCP Snooping > Binding Configuration**.
2. In the Static Binding Configuration section, in the **Interface** list, select the interface for which to add a binding to the DHCP snooping database.
3. In the **MAC Address** field, specify the MAC address for the binding to be added.  
This MAC address is the key to the binding database.
4. In the **VLAN ID** list, select the VLAN from the list for the binding rule.  
The valid range of the VLAN ID is 1–4093.
5. In the **IP Address** field, specify a valid IP address for the binding rule.
6. Click **Add** to add the DHCP snooping binding entry to the database.  
Configuration changes take effect immediately.

Click **Delete** to delete selected DHCP snooping binding static entries from the database, or **Clear** to delete all DHCP snooping binding entries from the database.

The following table describes the information that displays for DHCP Snooping Dynamic Binding Configuration:

Field	Description
Interface	Displays information about the interface to which a binding entry in the DHCP snooping database.
MAC Address	The MAC address for the binding entry in the binding database.
VLAN ID	The VLAN for the binding entry in the binding database. The valid range of the VLAN ID is 1–4093.
IP Address	The IP address for the binding entry in the binding database.
Lease Time	The remaining lease time for the dynamic binding entries.

## DHCP Snooping Persistent Configuration

➤ **To configure DHCP snooping persistent settings:**

1. Select **System > Services > DHCP Snooping > Persistent Configuration**.
2. Next to the Local Store, select **Enable** or **Disable** to determine if the binding table is stored locally. Factory default is disabled
3. Click **Apply** to apply the change to the system.  
Configuration changes take effect immediately.

# Switching

---

# 3

Use the features you access from the Switching tab to define Layer 2 features. The Switching tab contains links to features described in the following sections:

- *Ports*
- *LAG*
- *VLAN*
- *Voice VLAN*
- *Auto-VoIP Configuration*
- *Spanning Tree Protocol*
- *Multicast*
- *Address Table*

## 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. From the Ports menu, you can access the features described in the following sections:

- *Global Configuration*
- *Port Configuration*

### Global Configuration

IEEE 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This action can lead to high-priority and network control traffic loss. When IEEE 802.3x flow control is enabled, lower-speed switches can communicate with higher-speed switches by requesting that the higher-speed switch refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

➤ **To configure global configuration settings:**

1. Select **Switching > Ports > Global Configuration**.
2. Next to **Global Flow Control (IEEE 802.3x) Mode**, enable or disable IEEE 802.3x flow control on the system. The default is Disable.
  - **Enable**. The switch sends pause packets if the port buffers become full.
  - **Disable**. The switch does not send pause packets if the port buffers become full.
3. Click **Apply** to apply the changes to the system.

### Port Configuration

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

➤ **To configure port settings:**

1. Select **Switching > Ports > Port Configuration**.
2. Select the interface for which you want to configure settings.
  - To configure settings for a physical port, click **PORTS**.
  - To configure settings for a link aggregation group (LAG), click **LAGS**.
  - To configure settings for both physical ports and LAGs, click **All**.
3. Select the check box next to the port or LAG to configure.

You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

4. 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.
  - **Port Type.** This field is blank for most ports. Otherwise, the possible values are:
    - **Mirrored.** Indicates that the port is a source mirroring port.
    - **Probe.** Indicates that the port is a destination mirroring port.
    - **LAG.** Indicates that the port is a member of a link aggregation trunk. For more information, see [LAG](#) on page 45.
  - **Admin Mode.** Select the menu the port control administration state, which can be one of the following:
    - **Enable.** The port can participate in the network (default).
    - **Disable.** The port is administratively down and does not participate in the network.
  - **Port Speed.** Select the port's speed and duplex mode. If you select Auto, the auto negotiation process sets the duplex mode and speed. The port advertises both 10 Gbps full duplex as well as 1Gbps full duplex. Otherwise, your selection determines the port's duplex mode and transmission rate. The default is Auto.
  - **Physical Status.** Indicates the actual port's speed and duplex mode.
  - **Link Status.** Indicates whether the link is up or down.
  - **MAC Address.** Displays the physical address of the specified interface.
  - **ifIndex.** The ifIndex of the interface table entry associated with this port. If the interface field is set to All, this field is blank.
5. Click **Apply** to apply the changes to the system.

## LAG

Link aggregation groups (LAGs), which are also known as port channels, allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. You assign the LAG VLAN membership after you create a LAG. The LAG by default becomes a member of the management VLAN.

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

Static LAGs are supported. When a port is added to a LAG as a static member, it does not transmit or receive LAGPDUs. This switch supports eight LAGs.

From the LAGs menu, you can access features described in the following sections:

- [LAG Configuration](#)
- [LAG Membership](#)
- [LACP Configuration](#)
- [LACP Port Configuration](#)

## LAG Configuration

Use the LAG Configuration screen to group one or more full-duplex Ethernet links to aggregate 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**.
2. Select the check box next to the LAG to configure.

You can select multiple LAGs to apply the same settings 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:
  - **Description.** Specify the description string to be attached to a LAG. It can be up to 64 characters in length.
  - **LAG ID.** Displays the number assigned to the LAG. This field is read-only.
  - **Admin Mode.** Select **Enable** or **Disable** from the list. When the LAG (port channel) is disabled, no traffic flows and LAGPDUs are dropped, but the links that form the LAG (port channel) are not released. The default is Enable.
  - **STP Mode.** Select **Enable** or **Disable** from the list to specify the Spanning Tree Protocol administrative mode associated with the LAG.
  - **LAG Type.** Specifies whether the LAG is configured as a static or LACP port. When the LAG is static, it does not transmit or process received LAGPDUs. For example the member ports do not transmit LAGPDUs and all the LAGPDUs it might receive are dropped. The default is Static.
  - **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 static or LACP port channel.
  - **LAG State.** Indicates whether the link is up or down.
4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

## LAG Membership

Use the LAG Membership screen to select two or more full-duplex Ethernet links to aggregate 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 create a LAG:

1. Select **Switching > LAG > Basic > LAG Membership**.
2. From the **LAG ID** field, select the LAG to configure.  
The **LAG Name** field, shows the name assigned to the LAG. The values are ch1, ch2, ..., and ch8.

3. Click **Current members** to display the list of ports currently members of that LAG. These ports are also designated on the display of ports by a check mark.
4. Click the box, representing each required port to include the port in the LAG.

The following screen shows an example of how to configure LAG1 with ports xg1, xg2, xg3, xg6 and xg7 as members.

LAG Membership

LAG ID: LAG1

LAG Name: ch1

Current members

Port

Port	1	3	5	7	9	11	13	15	17	19	21	23	25	27
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	2	4	6	8	10	12	14	16	18	20	22	24	26	28

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

## LACP Configuration

### ➤ 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 to 65535. The default value is 32768.

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

## LACP Port Configuration

### ➤ To configure LACP port priority settings:

1. Select **Switching > LAG > Advanced > LACP Port Configuration**.
2. Select the check box next to the port to configure. You can select multiple ports to apply the same settings to all selected ports.
3. Configure the **LACP Priority** value for the selected port. The valid range is 0–255. The default value is 128.
4. Configure the administrative **LACP Timeout** value.
  - **Long**. Specifies a long time-out value. This is the default setting.

- **Short.** Specifies a short time-out value.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

## VLAN

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. 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 are 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 might 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.

From the VLAN menu, you can access the features described in the following sections:

- [VLAN Configuration](#)
- [VLAN Membership](#)
- [VLAN Status](#)
- [Port PVID Configuration](#)
- [MAC Based VLAN Group Configuration](#)
- [MAC Based VLAN Group Membership](#)
- [Protocol Based VLAN Group Configuration](#)
- [Protocol Based VLAN Group Membership](#)
- [GARP Switch Configuration](#)
- [GARP Port Configuration](#)

## VLAN Configuration

Use the VLAN Configuration screen to define VLAN groups stored in the VLAN membership table. The switch supports up to 512 VLANs. VLAN 1 is created by default, and by default all ports are untagged members.

Ports in the default VLAN can be tagged.

### ➤ To configure VLANs:

1. Select **Switching > VLAN > Basic > VLAN Configuration**.

2. To add a VLAN, configure the VLAN ID and name and click **Add**.

You have the following options:

- **VLAN ID.** Specify the VLAN identifier for the new VLAN. You can enter data in this field only when you are creating a VLAN. The range of the VLAN ID is 2–4093.
  - **VLAN Name.** Use this optional field to specify a name for the VLAN. It can be up to 32 alphanumeric characters long, including blanks. The default is blank.
  - **VLAN Type.** This field identifies the type of the VLAN you are configuring. You cannot change the type of the default VLAN (VLAN ID = 1) because the type is always Default. When you create a VLAN on this screen, its type is always Static.
3. To modify settings for a VLAN, select the check box next to the **VLAN ID**, change the desired information, and click **Apply**.

Configuration changes take effect immediately.

➤ **To reset VLAN settings on the switch to the defaults:**

1. Select the **Reset Configuration** check box
2. Click **OK** in the pop-up message to confirm the operation.

If the Management VLAN is set to a non-default VLAN (VLAN 1), it is automatically set to 1 after you reset the VLAN configuration.

## VLAN Membership

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:**

1. Select **Switching > VLAN > Advanced > VLAN Membership**.
2. From the **VLAN ID** list, select the VLAN to which you want to add ports.

The **VLAN Name** and **VLAN Type** are displayed.

The Port block displays the physical ports in the VLAN and whether they are currently members of the selected VLAN, As well as if they are one of the following:

- **Tagged.** Frames transmitted from this port and VLAN are tagged with specified VLAN ID.
- **Untagged.** Frames transmitted from this port and VLAN are untagged. By default, all ports are untagged members of VLAN 1.

A blank square means that the port is not a member of the VLAN.

The LAG block displays the LAGs on the switch.

3. To select the ports or LAGs to add to the VLAN, click the square belonging to each port or LAG. Each port is added as Untagged or Tagged according to the number of clicks.
4. To configure the same VLAN membership settings for all ports and LAGs, select an identical configuration for all the ports from the Group Operations list.

The possible values are:

- **Tag All.** All frames transmitted for this VLAN are tagged. All the ports are included in the VLAN.
  - **Untag All.** All frames transmitted from this VLAN are untagged. All the ports are included in the VLAN.
  - **Remove All.** Exclude all ports from the selected VLAN.
5. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

## VLAN Status

Use this screen to display the VLANs on the device and their member ports.

➤ **To view current VLAN status and membership:**

Select **Switching > VLAN > Advanced > VLAN Status**

The following table describes the fields displayed:.

Field	Description
VLAN ID	The VLAN identifier (VID) of the VLAN. The range of the VLAN ID is (1 to 4093)
VLAN Name	Name of VLAN. VLAN ID 1 is always named Default.
VLAN Type	The following values are possible: <ul style="list-style-type: none"> <li>• Static. A VLAN an administrator has configured.</li> <li>• Dynamic. The VLAN that is created by GVRP registration initially has a type of Dynamic (GVRP).</li> </ul>
Routing Interface	The routing interface presents IPv4 and IPv6 addresses, if defined on the VLAN interfaces.
Member Ports	The ports that are included in the VLAN.

## Port PVID Configuration

The Port PVID Configuration screen lets you assign a port VLAN ID (PVID) and define VLAN membership (tagged/untagged) to an interface.

A PVID has the following requirements:

- All ports must have a defined PVID.
- If no other value is specified, the default VLAN PVID is used.

➤ **To configure PVID and VLAN Membership information:**

1. Select **Switching > VLAN > Advanced > Port PVID Configuration**.
2. Select the check box next to the interfaces to configure.

You can select multiple interfaces to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

- To configure PVID settings for a physical port, click **PORTS**.
  - To configure PVID settings for a link aggregation group (LAG), click **LAGS**.
  - To configure PVID settings for both physical ports and LAGs, click **All**.
3. Configure the **PVID** to assign to untagged or priority tagged frames received on this port.
  4. Enter the VLAN IDs in which the port is a member in the **VLAN Member** field. Multiple ports can be entered, separated by commas or hyphens.
  5. Enter the tagged VLAN IDs in which the port is a member in the **VLAN Tag** field. Multiple ports can be entered, separated by commas or hyphens. For tagged membership you must enter the relevant VLAN ID in both this field and the VLAN membership field.
  6. In the **Acceptable Frame Types** list, specify how you want the port to handle untagged and priority tagged frames.

Whichever you select, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard. The default is Admit All.

- **VLAN Only**. The port discards any untagged or priority tagged frames it receives.
  - **Admit All**. Untagged and priority tagged frames received on the port are accepted and assigned the value of the Port VLAN ID for this port.
7. In the **Ingress Filtering** list, specify how you want the port to handle tagged frames. You have the following options:
    - **Enable**. A tagged frame is discarded if this port 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 IEEE 802.1Q VLAN standard. The default is Enable.
  8. In the **Port Priority** field, specify the default 802.1p priority assigned to untagged packets arriving at the port. Possible values are 0–7.
  9. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

## MAC Based VLAN Group Configuration

MAC-based VLAN can be used to define filtering criteria for untagged packets. By default, if you do not configure MAC-based VLAN settings on a port, untagged packets will be assigned to the port PVID. The MAC-based VLAN feature enables incoming untagged packets to be classified per port, to a defined VLAN ID based on the source MAC address of the packet.

A MAC-to-MAC-based VLAN Group ID mapping is defined by configuring an entry in the MAC-to-MAC-based VLAN Group ID table. An entry is specified via a source MAC address, prefix mask and the desired MAC-based VLAN Group ID. Then, for each port, a specific MAC-based VLAN Group ID can be mapped to a specific VLAN. MAC-based VLAN Group ID to VLAN ID mappings are unique for each port.

When untagged or priority-tagged packets arrive on a certain port, the source MAC address of the packet is looked up. If a matching MAC-based VLAN Group ID to VLAN ID mapping entry is found, the packet is classified to the corresponding VLAN ID. If the packet is already priority tagged, it will maintain this value, otherwise the priority will be set to zero. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues, otherwise the packet is dropped. This implies that the user is allowed to configure a MAC address mapping to a VLAN that has not been created on the system, however the packet will be forwarded only if the VLAN was configured on the port.

➤ **To create a new MAC Based VLAN Group:**

1. Click **Switching > VLAN > Advanced > MAC Based VLAN Group Configuration**.
2. Enter a **MAC Address** which will be bound to a MAC-based VLAN ID Group.
3. Enter a value in the **Prefix Mask** (allowed values 9-48).
4. Add a **Group ID** to identify the group.
5. Click **Add**. Configuration changes take place immediately.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. If you make any changes to an entry on this page, make the required changes and then click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

The following table displays the fields in the MAC Based VLAN Mapping block:

Field	Description
Group ID	Number of the protocol group.
VLAN ID	VLAN member of group
Ports	The ports that are included in the VLAN due to MAC-based VLAN operation.

---

**Note:** The per port association of the MAC-based VLAN Group to VLAN ID is done in the *MAC Based VLAN Group Membership* on page 52.

---

## MAC Based VLAN Group Membership

➤ **To configure the MAC-based VLAN group membership:**

1. Click **Switching > VLAN > Advanced > MAC Based VLAN Group Membership**.
2. Select the **MAC-based VLAN Group ID** for which you want to display or configure data in the **Group ID** drop-down menu.
3. Select a single VLAN from the **VLAN ID** menu. This is the VLAN to which you want to associate the specified group ID for the selected ports.

4. **Port Block.** Add selected ports to this MAC Based VLAN Group and select VLAN ID, by clicking on the ports.
5. **LAG Block.** Add selected LAGs to this MAC Based VLAN Group and selected VLAN ID, by clicking on the ports.

---

**Note:** Classification of MAC-based VLAN Group ID to VLAN ID is a per port configuration.

---



---

**Note:** If the associated VLAN is not configured on the port, the classified packet will be dropped.

---

If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

## 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 protocol-based VLAN on a port, untagged packets will be assigned to port PVID. You can override this behavior by defining protocol based VLANs. 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 specific VLAN ID, according to protocol-based VLAN for a specific protocol, untagged frames received on that port for that protocol will be assigned the protocol based VLAN ID. Untagged frames received on the port for other protocols will be assigned the Port VLAN ID, either the default PVID (1) or a PVID you have specifically assigned to the port using the Port VLAN Configuration screen.

You define a protocol-based VLAN by creating a group, associated to a certain protocol. Per each port, each group has a one-to-one relationship with a certain defined VLAN ID.

### ➤ To create a new Protocol Based VLAN Group:

1. Click **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration**.
2. Enter a number used to identify the group created by the user in the **Group ID** field. Group IDs should be assigned when a group is created by the user.
3. Use **Protocol** to select the protocols you want to be associated with the group. There are three configurable protocols: IP, IPX, ARP.
  - **IP.** IP is a network layer protocol that provides a connectionless service for the delivery of data.
  - **ARP.** Address Resolution Protocol (ARP) is a low-level protocol that dynamically maps network layer addresses to physical medium access control (MAC) addresses
  - **IPX.** The Internetwork Packet Exchange (IPX) is a connectionless datagram Network-layer protocol that forwards data over a network.

In addition, you can manually enter a protocol ID, either in Hex or decimal format. Display of protocol ID is always in Hex format.

4. Click **Add**. The group is created.

---

**Note:** The per port association of Protocol Based VLAN Group to VLAN ID is done in the *Protocol Based VLAN Group Membership* on page 54.

---

The following table displays the fields in the Protocol Based VLAN Mapping block:

Field	Description
Group ID	Number of the protocol group.
VLAN ID	VLAN member of group
Ports	The ports that are included in the VLAN, due to Protocol Based VLAN operation.

5. To remove the Protocol Based VLAN group identified by the value in the **Group ID** field, click **Delete**.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

If you make any changes to an entry on this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

## Protocol Based VLAN Group Membership

➤ **To configure the protocol-based VLAN group membership and VLAN association:**

1. Click **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership**.
2. Select the protocol-based VLAN Group ID for which you want to display or configure data in the **Group ID** drop-down menu.
3. Select a single VLAN from the **VLAN ID** drop-down menu. This is the VLAN to which you want to associate the specified group ID for the selected ports.
4. **Port Block.** Add selected ports to this protocol-based VLAN group and selected VLAN ID, by clicking on the ports.
5. **LAG Block.** Add selected LAGs to this protocol-based VLAN group and selected VLAN ID, by clicking on the ports.

---

**Note:** Classification of protocol-based VLAN Group ID to VLAN ID is a per port configuration.

---

---

**Note:** If the associated VLAN is not configured on port, a classified packet will be dropped.

---

If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

## 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 enable GARP on the switch:**

1. Click **Switching > VLAN > Advanced > GARP Switch Configuration**.
2. Use **GVRP Mode** to choose the GARP VLAN Registration Protocol administrative mode for the switch by selecting **Enable** or **Disable** from the radio button. The default is Disable.

## GARP Port Configuration

➤ **To configure GARP on ports:**

1. Click **Switching > VLAN > Advanced > GARP Port Configuration**.
2. Use **Interface** to select the physical interface for which data is to be displayed or configured.
3. Use **GVRP State** to choose the GARP VLAN Registration Protocol administrative mode for the port by selecting enable or disable from the drop-down list. If you select disable, the protocol will not be active and the Join Time, Leave Time and Leave All Time will have no effect. The default is Disable.
4. Use **Join Timer** to specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN in centiseconds. Enter a number between 10 and 100 (0.1 to 1.0 seconds). The default is 20 centiseconds (0.2 seconds). An instance of this timer exists for each GARP participant for each port.

5. Use **Leave Timer** to specify the time to wait after receiving an unregister request for a VLAN before deleting the associated entry, in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 20 and 600 (0.2 to 6.0 seconds). The default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.
6. Use **Leave All Timer** to control how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5\*LeaveAllTime. The timer is specified in centiseconds. Enter a number between 200 and 6000 (2 to 60 seconds). The default is 1000 centiseconds (10 seconds). An instance of this timer exists for each GARP participant for each port.

---

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

---

## 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.

The following are two operational modes for IP phones:

- IP phones are configured with VLAN mode enabled, ensuring that the phone uses tagged packets for all communications.
- IP phones are configured with VLAN mode disabled, ensuring that the phone uses untagged packets for all communications. The phone uses untagged packets while retrieving the initial IP address through DHCP. The phone eventually uses the voice VLAN and commences sending tagged packets.

From the Voice VLAN menu, you can access the features described in the following sections:

- *Properties*
- *Port Setting*
- *OUI*

## Properties

- **To configure Voice VLAN:**

---

**Note:** The management VLAN (by default VLAN 1) cannot be configured as the voice VLAN.

---

1. Select **Switching > Voice VLAN > Basic > Properties**.
2. Next to **Voice VLAN Status**, enable or disable (default) voice VLAN on the switch.  
If the switch does not handle traffic from IP phones, the status should be disabled.
3. From the **Voice VLAN ID** list, select the VLAN ID to use for voice traffic.
4. In the **Class of Service** list, select the CoS tag value to be reassigned for packets received on the voice VLAN when Remark CoS is enabled. The default value is 6.
5. In the **Remark CoS** list, specify whether to enable or disable (default) Class of Service remarks on the selected port.
6. In the **Voice VLAN Aging Time** field, specify the amount of time after the last IP phone's OUI is aged out for a specific port.  
The port ages out after the bridge and voice aging time.
7. Click **Apply** to send the updated configuration to the switch.  
Configuration changes take effect immediately.

## Port Setting

### ➤ To configure Voice VLAN port settings:

1. Select **Switching > Voice VLAN > Advanced > Port Setting**.
  2. Select the check box next to the port to configure.  
You can select multiple check boxes to apply the same setting to all selected ports.
- Or**
3. In **Go To Interface**.  
Enter the port to be configured and click **Go**.
  4. From the **Voice VLAN Mode** list, specify whether to enable or disable voice VLAN on the selected port.
  5. Click **Apply** to send the updated configuration to the switch.

---

**Note:** The Membership field displays whether the current operational status of the voice VLAN on the interface is active or not active.

---

## OUI

The Organizational Unique Identifier (OUI) identifies the IP phone manufacturer. The switch comes preconfigured with the following OUIs:

- **00:01:E3**. SIEMENS
- **00:03:6B**. CISCO1

- **00:04:0D**. AVAYA1
- **00:12:43**. CISCO2
- **00:1B:4F**. AVAYA2
- **00:60:B9**. NITSUKO
- **00:D0:1E**. PINTEL
- **00:E0:75**. VERILINK
- **00:E0:BB**. 3COM

You can select an existing OUI or add a new OUI and description to identify the IP phones on the network.

➤ **To configure OUI settings:**

1. Select **Switching > Voice VLAN > Advanced > OUI**.
2. To modify the OUI prefix list, you have the following options:
  - Add an OUI prefix to the list. Enter the VOIP OUI prefix in the **Telephony OUI(s)** field, provide a **Description** of the prefix, and click **Add**. The OUI prefix must be in the format AA:BB:CC.
  - Delete an OUI prefix from the list. Select the check box next to the OUI prefix and click **Delete**.
  - Modify information for an entry in the OUI list. Select the check box next to the OUI prefix, update the OUI prefix or description and click **Apply**.
3. Click **RESTORE DEFAULTS** to restore the list to the preconfigured OUIs.

## Auto-VoIP Configuration

Auto-VoIP automatically makes sure that time-sensitive voice traffic is given priority over data traffic on ports that have this feature enabled. Auto-VoIP checks for packets carrying the following VoIP protocols:

- Session Initiation Protocol (SIP)
- H.323 (Prioritize only signaling packets)
- Skinny Call Control Protocol (SCCP)

All three protocols are checked during the signaling, call identification stage. Once the VoIP call is established, only the SIP and SCCP protocols are checked. This feature supports up to 48 bidirectional VoIP calls.

VoIP frames that are received on ports that have the Auto-VoIP feature enabled are assigned to queue 6.

Auto-VoIP and QoS CoS/DiffServ mode features can co-exist and be activated at the same time. If both features are active at the same time on the same port, the manual QoS assignment might override the VoIP QoS assignment.

To configure the Auto-VoIP parameters, use the Auto-VoIP configuration screen. The Interface column specifies all the configurable Auto-VoIP interfaces. The Traffic Class displays the traffic class on which the received VoIP frames are marked.

➤ **To enable Auto-VoIP:**

1. Select **Switching > Auto-VoIP**.
1. To configure Auto-VoIP interface settings for a physical port or a LAG port, click **PORT**, **LAGS**, or **All**.  
Or:
2. Enter the interface name in the **Go To Interface** field and click **Go**.  
The entry corresponding to the specified port is selected.
3. Select **Enable** or **Disable** from the **Auto-VoIP Mode** drop-down list, as the Auto-VoIP administrative mode for the interface.  
**Traffic Class** is pre configured and cannot be changed.
4. Click **Apply** to send the updated configuration to 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 62.

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 point-to-point and edgeport. MSTP is compatible with both RSTP and STP, and can be configured to operate entirely as an RSTP bridge or an STP bridge.

---

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

---

The STP link contains links to features 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 Switch 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. Next to **STP Operation Mode**, specify the Force Protocol Version parameter for the switch.

The following options are:

- **STP (Spanning Tree Protocol)**. IEEE 802.1D
  - **RSTP (Rapid Spanning Tree Protocol)**. IEEE 802.1w. This is the default mode.
  - **MSTP (Multiple Spanning Tree Protocol)**. IEEE 802.1s
4. Specify the configuration name and revision level (relevant when in MSTP mode).
    - **Configuration Name**. Name used to identify the configuration currently being used. It can be up to 32 alphanumeric characters. By default it is the switch MAC address.
    - **Configuration Revision Level**. Number used to identify the configuration currently being used. The valid range is 0–65535. The default value is 0.
  5. Next to **Forward BPDU while STP Disabled**, select Enable or Disable.

The **Forward BPDU while STP Disabled** field specifies whether spanning tree BPDUs should be forwarded or not (default) while spanning-tree is disabled on the switch.

6. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

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

Field	Description
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time in seconds since the topology of the CST last changed.
Topology Change Count	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.
Max Age (sec)	Specifies the bridge maximum age for CST. The value must be less than or equal to $(2 \times \text{bridge forward delay}) - 1$ and greater than or equal to $2 \times (\text{bridge hello time} + 1)$ .
Forward Delay (sec)	Derived value of the root port bridge forward delay parameter.
Hold Time (sec)	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

To configure Common Spanning Tree (CST) and Internal Spanning Tree on the switch, use the CST Configuration screen.

➤ **To configure CST settings:**

1. Select **Switching > STP > Advanced > CST Configuration**.
2. Specify values for CST in the following fields:
  - **Bridge Priority.** Specify the bridge priority value for the Common and Internal Spanning Tree (CST). 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.
  - **Bridge Max Age (Sec).** 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 value must be less than or equal to  $(2 * \text{bridge forward delay}) - 1$  and greater than or equal to  $2 * (\text{bridge hello time} + 1)$ . The valid range is 6–40, and the default value is 20.

- **Bridge Hello Time (Sec).** Specifies 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 (Sec).** 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 valid range is 4–30 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 1–40. The default value is 20.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

The following table describes the MSTP Status information displayed on the CST Configuration screen:

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.

➤ **To configure CST port settings:**

1. Select **Switching > STP > Advanced > CST Port Configuration**.
2. To configure CST settings for an interface, click **PORTS**, **LAGS**, or **All**.
3. Select the check box next to the port or LAG to configure.
 

You can select multiple ports and LAGs to apply the same settings to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
4. Configure the CST values for the selected ports or LAGs:
  - **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 Auto, Enable, or Disable. The default is Auto, which specifies that the software waits for 3 seconds (with no BPDUs received on the interface) before putting the interface into the PortFast mode.

- **BPDU Forwarding.** Specifies whether spanning tree BPDUs should be forwarded while spanning-tree is disabled on the switch. Select **Enable** or **Disable**.
  - **Port State.** The forwarding state of this port. This field is read-only.
  - **Path Cost.** Set the Path Cost to a new value for the specified port in the Common and Internal Spanning Tree. The valid range is 1–200000000.
  - **Priority.** The priority for a particular port within the CST. The port priority is set in multiples of 16.
  - **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 value is fixed at 2 seconds.
5. Click **Apply** to send the updated configuration to the switch.  
Configuration changes take place immediately.

## CST Port Status

To display Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch, use the CST Port Status screen.

➤ **To display the CST Port Status screen:**

1. Select **Switching > STP > Advanced > CST Port Status**.
2. To view CST settings for an interface, click **PORTS**, **LAGS**, or **All**.

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

Field	Description
Interface	Select a physical or port channel interface to configure. The port is associated with the VLANs 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 can be one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
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.
Edge Port	Indicates whether the port is active as an edge port. Possible values are True and False.

Field	Description
Point-to-point MAC	Derived value of the point-to-point status.
CST Regional Root	Displays the bridge priority and base MAC address of the CST regional root.
CST Path Cost	Displays the path cost to the CST tree regional root.
Port Forwarding State	Displays the forwarding state of this port.

## Rapid STP

Use the Rapid STP screen to view information about Rapid Spanning Tree (RSTP) port status.

➤ **To display the Rapid STP screen:**

Select **Switching > STP > Advanced > RSTP**.

The following table describes the Rapid STP Status information displayed on the screen..

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 can be one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
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 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. To add an MST instance, configure the MST values and click **Add**:
  - **MST ID**. Specify the ID of the MST to create. The valid range is 1–15.
  - **Priority**. Specify 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. The default priority is 32768. The valid range is 0–61440.
  - **VLAN ID**. The list contains all VLANs configured on the switch. Select a VLAN to associate with the MST instance.
3. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

➤ **To modify an MST instance:**

1. Select the check box next to the instance to configure and update the values.  
You can select multiple check boxes to apply the same setting to all selected MTS instances.
2. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

To delete an MST instance, select the check box next to the instance and click **Delete**.

The following table describes the information displayed on the screen for each configured MST instance..

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	Displays 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	Displays 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 and False.
Designated Root	Displays the bridge identifier of the root bridge for the selected MST instance, which is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Displays 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.

## 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.

➤ **To configure MST port settings:**

1. Select **Switching > STP > Advanced > MST Port Configuration**.

---

**Note:** To restart the STP migration process (force re-negotiation with neighboring switches on selected interfaces) select one or more interface(s) and press the **Activate Protocol Migration** button.

---

2. Select the MST instance to be configured from the **Select MST** field.
3. To view CST settings for an interface, click **PORTS**, **LAGS**, or **All**.
4. Select the check box next to the port or LAG to configure.

You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

5. Configure the MST values for the selected ports or LAGs:
  - **Port Priority.** The priority for a particular port within the selected MST instance. The port priority is set in multiples of 16. The valid range is 0–240.
  - **Port Path Cost.** Set the path cost to a new value for the specified port in the selected MST instance. The valid range is 0–200000000. If you enter 0, the device recalculates the path cost.
6. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

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

Field	Description
Auto Calculated Port Path Cost	Displays that the path cost is not automatically calculated (Disabled). Path cost is recalculated based on the link speed of the port if the configured value for <b>Port Path Cost</b> is 0.
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 Mode	Spanning Tree Protocol Administrative Mode associated with the port or port channel. Possible values are Enable and 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: <ul style="list-style-type: none"> <li>• <b>Disabled.</b> STP is disabled on the port. The port forwards traffic while learning MAC addresses.</li> <li>• <b>Blocking.</b> The port is blocked and cannot be used to forward traffic or learn MAC addresses.</li> <li>• <b>Listening.</b> The port is in the listening mode. The port cannot forward traffic or learn MAC addresses.</li> <li>• <b>Learning.</b> The port is in the learning mode. The port cannot forward traffic, however, it can learn new MAC addresses.</li> <li>• <b>Forwarding.</b> The port is in the forwarding mode. The port can forward traffic and learn new MAC addresses</li> </ul>
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
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.

Field	Description
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 page to view information about the number of bridge protocol data units (BPDUs) transmitted and received on each port.

To display the Spanning Tree Statistics page:

1. Click **Switching** > **STP** > **Advanced** > **STP Statistics**.

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

Field	Description
Interface	Select a physical or port channel interface to view its statistics.
STP BPDUs Received	Number of STP + RSTP + MSTP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP + RSTP + MSTP BPDUs transmitted from the selected port.

2. Click **Update** to update the screen with the latest STP statistics information.

## Multicast

Multicast IP traffic is traffic that is destined to a host group. The class D addresses identify the host groups for IPv4 multicast, which range from 224.0.0.0 to 239.255.255.255. The prefix ff00::/8 identifies the host groups for IPv6 multicast.

From the Multicast menu, you can access features described in the following sections:

- *MFDB*
- *Auto-Video Configuration*
- *IGMP Snooping*
- *IGMP Snooping Querier*
- *MLD Snooping*
- *Static Multicast Address*

## MFDB

The switch uses the Layer 2 Multicast Forwarding Database (MFDB) to make forwarding decisions for packets that arrive with a multicast destination MAC address. By limiting multicast transmissions only to certain ports in the switch, traffic is prevented from going to unnecessary parts of the network.

When a packet with a destination multicast MAC address is received on the switch, this address is combined with the VLAN ID, and a search is performed in the Layer 2 MFDB. If no match is found, the packet is either flooded to all ports in the VLAN or discarded, depending on the switch configuration. If a match is found, the packet is forwarded only to the ports that are members of that multicast group per the specific VLAN ID.

From the MFBD link, you can access the following screens:

- [MFDB Table](#)
- [MFDB Statistics](#)

### MFDB Table

The 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 view the MFDB Table screen:

1. Select **Switching > Multicast > MFDB > MFDB Table**.
2. In the **Search by MAC Address** field, enter the MAC address whose MFDB table entry you want to display.

Enter six 2-digit hexadecimal numbers separated by colons. For example, 01:01:23:43:45:67.

3. Click **Go**.

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

The MFDB Table screen displays the following:

- **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.** The component that is responsible for this entry in the MFDB. Possible values are IGMP Snooping, Static Filtering, and MLD Snooping.
- **Type.** The type of the entry. Static entries 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 (Fit:) for the selected address.

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

## MFDB Statistics

To access the MFDB Statistics screen, click **Switching > Multicast > MFDB > MFDB Statistics**.

The MFDB Statistics screen displays the following:

- **Max MFDB Table Entries.** The maximum number of entries that the MFDB table can hold.
- **Current Entries.** The current number of entries in the MFDB table.

## Auto-Video Configuration

If the switch supports devices or applications running multicast traffic, the Auto-Video feature simplifies IGMP snooping querier configuration, such as video surveillance cameras.

### ➤ To configure Auto-Video:

1. Select **Switching > Multicast > Auto-Video Configuration**.
2. Globally enable or disable the Auto-Video administrative mode for the switch by selecting **Enable** or **Disable** next to the Auto-Video Status radio button.
3. Select the VLAN ID of the auto-video VLAN in the **Auto-Video VLAN** field.
4. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

## 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. Class D IP addresses identify host groups, 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 action 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

few 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 that the multicast packet is flooded. The problem of wasting bandwidth is even worse when the LAN segment is not shared, for example in full-duplex links.

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

From the IGMP Snooping link, you can access features described in the following sections:

- [IGMP Snooping Configuration](#)
- [IGMP Snooping Table](#)
- [IGMP Snooping VLAN Configuration](#)

## IGMP Snooping Configuration

Use the IGMP Snooping Configuration screen to configure the parameters for IGMP snooping.

### ➤ To configure IGMP Snooping:

1. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Configuration**.
2. Next to IGMP Snooping Status, 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 **Block Unknown Multicast Addresses**.
  - **Enable**. Packets with unknown multicast MAC addresses in the destination field are dropped.
  - **Disable**. Packets with unknown destination multicast MAC addresses are flooded to all interfaces in VLAN.
4. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

The following table displays information about the global IGMP snooping status.

Field	Description
VLAN IDs Enabled For IGMP Snooping	Displays VLAN IDs enabled for IGMP snooping. For more information about how to enable VLANs for IGMP snooping, see <a href="#">IGMP Snooping VLAN Configuration</a> on page 71.
VLAN IDs Enabled For IGMP Snooping Querier	Displays VLAN IDs enabled for IGMP snooping querier.

## IGMP Snooping Table

- To view all of the entries in the Multicast Forwarding Database that were created for IGMP snooping:

- Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Table**.

The following table describes the fields in the IGMP Snooping Table..

Field	Description
MAC Address	A multicast MAC address for which the switch has forwarding and filtering information. The format is six 2-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 field displays the type of the entry. Static entries 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 (Fit) 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. Select the VLAN ID 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 mode 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.** The value for group membership interval of IGMP snooping for the specified VLAN ID. This value is calculated as follows: **(Query Interval \* 2) + Maximum Response Time**.
  - **Maximum Response Time.** Enter the amount of time in seconds that a switch waits after sending a query on the VLAN because it did not receive a report for a particular

group in that interface. The valid range is 5–20 seconds. The default value is 10. This value must be less than the Host Timeout value.

- **MRouter Timeout.** 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. This value is calculated as follows: **Query Interval** \* 2.
- **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 30–1800 seconds. The default is 125 seconds.

3. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

To disable IGMP snooping on a VLAN and remove it from the list, select the check box next to the VLAN ID and click **Delete**.

## 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 stops forwarding multicast transmissions to the port where the end device is located.

The screens you access from the IGMP Snooping Querier link enable you to configure and display information about IGMP snooping queriers on the network and, separately, on VLANs.

The IGMP Snooping Querier feature contains links to features described in the following sections:

- [Querier Configuration](#)
- [Querier VLAN Configuration](#)
- [Querier VLAN Status](#)

### 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. Click **Switching** > **Multicast** > **IGMP Snooping Querier** > **Querier Configuration**.
2. Next to the **Querier Admin Mode**, enable or disable the administrative mode for IGMP snooping querier. The default setting is Disable.
3. In the **Snooping Querier Address** field, specify the IP address to be used as the source address in periodic IGMP queries (if there no querier address is specified for a VLAN).

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. Only version 2 is supported.
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 in the range of 30–1800 seconds. The default value is 125.

The **Querier Expiry Interval** specifies the time interval in seconds after which the last querier information is removed. The Query Expiry Interval is a read-only parameter calculated as:  $2 * \text{Query Interval} + 5$ , so by default the value is:  $2*125+5 = 255$ .

6. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

In the VLAN IDs Enabled for IGMP Snooping Querier block, the VLANs that are enabled for IGMP snooping querier are displayed.

## Querier VLAN Configuration

Use this screen to configure IGMP queriers for use with VLANs on the network.

### ➤ To configure Querier VLAN settings:

1. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration**.
2. To create a VLAN ID for IGMP Snooping, select **New Entry** from the VLAN ID list and complete the following fields:
  - **VLAN ID**. New Entry is selected.
  - **VLAN ID**. Specifies the VLAN ID for which the IGMP snooping querier is to be enabled.
  - **Querier Election Participate Mode**. Enable or disable querier participate mode.
    - **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.
  - **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 **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

To disable Snooping Querier on a VLAN, select the VLAN ID and click **Delete**.

## Querier VLAN Status

- **To view the operational state and other information for IGMP snooping queriers for VLANs on the network:**

Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status**.

The following table describes the information available on the Querier VLAN Status screen.

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: <ul style="list-style-type: none"> <li>• <b>Enabled.</b> The snooping switch is the querier in the VLAN. The snooping switch sends out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode.</li> <li>• <b>Disabled.</b> 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.</li> </ul>
Operational Version	Displays the IGMP protocol version of the operational querier.
Operational Max Response Time	Displays the maximum response time 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 sub protocol 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.

The MLD snooping link contains features described in the following sections:

- [Configuration](#)
- [MLD VLAN Configuration](#)
- [Multicast Router VLAN Configuration](#)
- [Querier Configuration](#)
- [Querier VLAN Configuration](#)

## 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. Next to **MLD Snooping Admin Mode**, enable or disable the administrative mode for MLD Snooping for the switch.

The default is disabled.

The VLAN IDs Enabled For MLD Snooping section displays VLAN IDs enabled for MLD snooping.

3. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

## 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, select a VLAN ID from a drop down menu listing all VLANs configured on the switch.
3. In the **Admin Mode** field, enable MLD Snooping for the specified VLAN ID.
4. In the **Fast Leave Admin Mode** field, enable or disable the MLD Snooping Fast Leave mode for the specified VLAN ID.
5. In the **Group Membership Interval** field, enter the value for the group membership interval of MLD Snooping for the specified VLAN ID.

The valid range is 4-3620 seconds. The default value is 260.

6. In the **Maximum Response Time** field, set the value for maximum response time of MLD snooping for the specified VLAN ID. The Maximum Response Time value must be less than Group Membership Interval value.

The valid range is 1–20 seconds. The default value is 10.

7. The **Multicast Router Expiry Time** field is a calculated field, displaying the value for multicast router expiry time of MLD snooping for the specified VLAN ID. Multicast Router Expiry Time is calculated as **Group Membership Interval field value - Maximum Response Time field value**.

8. Click **Add** to enable MLD Snooping on the specified VLAN.

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

### 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. As is not the case in the previous release of the system firmware, snooping dynamic learning mode (snooping interface mode or snooping VLAN mode) does not need not to be enabled on the interface. The dynamic learning mode is applicable only for dynamically learned multicast router information (queries from an attached true querier).

#### ➤ To configure the Multicast Router VLAN:

1. Select **Switching > Multicast > MLD Snooping > Multicast Router VLAN Configuration**.
2. In the **Interface** field, select the interface ID.  
The entry corresponding to the specified interface is selected.
3. In the **VLAN ID** field, enter the VLAN ID for which the multicast router mode is to be enabled or disabled.
4. In the **Multicast Router** field, enable or disable multicast router on the selected interface.
5. Click **Apply** to send the updated configuration to the switch.  
Configuration changes take place immediately.

### Querier Configuration

Use this page 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. Click **Switching > Multicast > MLD Snooping > Querier Configuration**.
2. From the **Querier Admin Mode** field, enable or disable the administrative mode for MLD Snooping Querier.
3. In the **Snooping 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 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 30–1800 seconds. The default value is 125.
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 is calculated as  $2 * \text{Query Interval} + 5$ . The default value is 255.

VLAN IDs enabled for MLD Snooping Querier are displayed.

7. Click **Apply** to apply the new settings 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.

## Querier VLAN Configuration

### ➤ To configure MLD queriers for use with VLANs on the network:

1. Click **Switching > Multicast > MLD Snooping > Querier VLAN Configuration**.
2. Enter a **VLAN ID** to specify the VLAN ID on which MLD Snooping Querier is administratively enabled. This VLAN must exist in the VLAN database.
3. Select **Enable** or **Disable** in the **Querier Election Participate Mode** field. The MLD Snooping Querier participate in election mode. When this mode is disabled, up on seeing other querier of same version in the VLAN, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where the least IP address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
4. Enter the **Querier VLAN Address** that specifies the source address in periodic MLD queries sent on the specified VLAN

The following table describes the information available on the Querier VLAN Status page.

Field	Description
Operational State	Specifies the operational state of the IGMP Snooping Querier on a VLAN: <ul style="list-style-type: none"> <li>• <b>Enabled.</b> 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.</li> <li>• <b>Disabled.</b> 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.</li> </ul>
Operational Version	Displays the MLD protocol version of the operational querier.
Last Querier Address	Displays the IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	Displays the MLD protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	Displays the maximum response time to be used in the queries that are sent by the snooping querier.

5. Click **Add** to add a Querier on the specified VLAN.
6. Click **Delete** to delete a Querier on the specified VLAN.

7. Click **Apply** to apply the new settings 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.

## Static Multicast Address

The Static Multicast Address link feature contains features described in the following sections:

- *Multicast Group Configuration*
- *Multicast Group Membership*
- *Multicast Forward All*

### Multicast Group Configuration

The Multicast Group Configuration screen contains fields for creating, deleting, and modifying multicast service groups. The Multicast Group Configuration table contains up to 512 multicast service groups.

#### ➤ To add a multicast group:

1. Select **Switching > Multicast > Static Multicast Address > Multicast Group Configuration**.
2. Select the VLAN ID.
  - **VLAN ID**. Displays the VLAN ID.
  - **VLAN Name**. Displays the user-defined VLAN name.
3. In the **Multicast Address** field, enter the multicast group MAC Address associated with the VLAN.
  - **Type**. Indicates the VLAN ID status in relation to the multicast group.
    - **Static**. Attaches the VLAN ID to the multicast group as static member.
    - **Dynamic**. Dynamically joins the VLAN ID to the multicast group.
4. Click **Apply** to send the updated configuration to the switch.  
Configuration changes take place immediately.

### Multicast Group Membership

The multicast Group Membership screen displays the ports and LAGs attached to the selected VLAN and the multicast service group. The Port and LAG tables also reflect the manner in which the port or LAGs joined the multicast group.

#### ➤ To configure the multicast group membership:

1. Select **Switching > Multicast > Static Multicast Address > Multicast Group Membership**.
2. Select the VLAN for which you want to configure multicast group settings.

- To configure the multicast group for a physical port, click **PORTS**.
  - To configure the multicast group for a link aggregation group (LAG), click **LAGS**.
  - To configure the multicast group for both physical ports and LAGs, click **All**.
3. Select the check box next to the interfaces to configure.

You can select multiple interfaces to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

Or:

4. Select the interface in the **Go To Interface** field and click **Go**. The entry corresponding to the specified interface will be selected.
5. Select the **Interface Status** of the interfaces. The possible values are:
- **Static**. Attaches the interface to the multicast group as a static member.
  - **Forbidden**. Specifies that this interface is forbidden from joining this group on this VLAN.
  - **Excluded**. Indicates that the interface is not currently a static member of this multicast group on this VLAN.

---

**Note:** If an interface was added to the Multicast group as a result of IGMP/MLD snooping, its status is Dynamic. This status cannot be selected manually.

---

6. Click **Apply** to send the updated configuration to the switch.

## Multicast Forward All

After IGMP snooping is enabled, multicast packets are forwarded only to the appropriate port and VLANs. The Multicast Forward All screen enables configuring ports or LAGS to forward all multicast traffic, even if IGMP or static configuration did not determine them as members of specific multicast groups.

### ➤ To configure the Multicast Forward All feature:

1. Select **Switching > Multicast > Static Multicast Address > Multicast Forward All**.
2. Select the **VLAN ID** for which you want to configure multicast forward all settings.
  - To configure multicast forward all settings for a physical port, click **PORTS**.
  - To configure the multicast forward all settings for a link aggregation group (LAG), click **LAGS**.
  - To configure the multicast forward all settings for both physical ports and LAGs, click **All**.
3. Select the check box next to the interfaces to configure.

You can select multiple interfaces to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

Or:

Select the interface in the **Go To Interface** field and click **Go**. The entry corresponding to the specified interface will be selected.

4. Select the **Interface Status** of the interfaces. The possible values are:
  - **Static**. The port receives all multicast streams.
  - **Forbidden**. Interfaces cannot receive any multicast streams, even if IGMP/MLD snooping designated the interface to join a multicast group.
  - **Excluded**. The interface is currently not a forward all interface.
5. Click **Apply** to send the updated configuration to the switch.

## Address Table

The Address Table contains information about unicast entries for which the switch has forwarding or filtering information. The transparent bridging function uses this information in determining how to propagate a received frame. Use the search function of the Address Table screen to display information about the entries in the table.

From the Address Table link, you can access features described in the following sections:

- [Address Table](#)
- [Dynamic Address](#)
- [Static MAC Address](#)

### ➤ To search for an entry in the MAC Address Table:

1. Select **Switching > Address Table > Basic > Address Table**.
2. In the **Search By** field, select whether to search for MAC addresses by MAC address, VLAN ID, or interface.
  - **MAC Address**: Select MAC Address and enter a 6-byte hexadecimal MAC address in 2-digit groups separated by colons, then click **Go**. If the address exists, that entry is displayed. An exact match is required.
  - **VLAN ID**: Select VLAN ID and enter the VLAN ID, for example, 100. Then click **Go**. If any entries with that VLAN ID exist they are displayed.
  - **Interface**: Select Interface, enter the interface ID in xg1, xg2... format, then, click **Go**. If any entries learned on that interface exist, they are displayed.

Click **Clear** to clear dynamic MAC addresses in the table.

The following table describes the information available for each entry in the address table..

Field	Description
VLAN ID	Specifies the VLAN ID on which the MAC address has forwarding or filtering information.
MAC Address	A unicast MAC address for which the switch has forwarding or filtering information. The format is a 6-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: <ul style="list-style-type: none"> <li>• <b>Static</b>. The entry was added when a static MAC filter was defined.</li> <li>• <b>Learned</b>. The entry was learned by observing the source MAC addresses of incoming traffic, and is currently in use.</li> </ul>

## Dynamic Address

Use the Dynamic Address 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 setting:

1. Select **Switching > Address Table > Advanced > Dynamic Address**.
2. Specify the number of seconds the forwarding database should wait before deleting a learned entry that has not been updated in the **Address Aging Timeout** field.

You can enter any number of seconds from 10 through 630. The default is 300.

3. Click **Apply** to send the updated configuration to the switch.
4. Click **Cancel** to reset the data to the latest value of the switch.

## Static MAC Address

Use the Static MAC Address Configuration page to configure and view static MAC addresses on an interface.

### ➤ To configure a static MAC address:

1. Select **Switching > Address Table > Advanced > Static MAC Address**.
2. Select the **VLAN ID** corresponding to the MAC address to add.
3. Specify the **MAC address** to add.
4. Specify the **Interface** associated with the MAC address.
5. Click **Add**.

To delete a static MAC address, select the check box next to the entry and click **Delete**.

To modify the settings for a static MAC address, select the check box next to the entry, update the desired values, and click **Apply**.

Click **Update** to reload the page and display the latest MAC address learned on a specific VLAN.

The switch supports IP routing. Use the menus under the Routing tab to manage routing on the system. This chapter contains the following sections:

- *IP*
- *VLAN*
- *Routing Table*
- *ARP*
- *IPv6*

## IP

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, the switch searches the host table for a matching destination IP address. If an entry is found, the packet is routed to the host. If there is not a matching entry, the switch performs a longest prefix match on the destination IP address. If an entry is found, the packet is routed to the next hop. If there is no match, the packet is routed to the next hop specified in the default route. If there is no default route configured, the packet is passed to the software to be handled appropriately.

The routing table can have entries added either statically by the administrator or dynamically by a routing protocol. The host table can have entries added either statically by the administrator or dynamically using ARP.

From the IP link, you can access features described in the following sections:

- [IP Configuration](#)
- [IP Statistics](#)

## IP Configuration

### ➤ To configure routing parameters for the switch:

1. Select **Routing > IP > IP Configuration**.
2. Next to **Routing Mode**, select **Enable** or **Disable**.

If you select **Disable**, the switch will not perform routing.

You must enable routing for the switch before you can route through any of the interfaces. The default value is router mode.

3. Enter the value for **IPv4 MTU** (longest packet that can be received).

The following table describes the fields displayed in this page:

	Description
Default Time to Live	The default value is 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 value set for this field is 64.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a compile-time constant. The value set for this field is 1.

4. Click **Apply** to send the updated configuration to the switch.

## IP Statistics

The statistics reported on the IP Statistics page are as specified in RFC 1213.

➤ **To display the page:**

1. Click **Routing > IP > 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.

Field	Description
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this 'no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully re-assembled.
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
IcmlnMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmlnErrors.
IcmlnErrors	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
IcmlnDestUnreachs	The number of ICMP Destination Unreachable messages received.
IcmlnTimeExcds	The number of ICMP Time Exceeded messages received.
IcmlnParmProbs	The number of ICMP Parameter Problem messages received.
IcmlnSrcQuenchs	The number of ICMP Source Quench messages received.
IcmlnRedirects	The number of ICMP Redirect messages received.
IcmlnEchos	The number of ICMP Echo (request) messages received.
IcmlnEchoReps	The number of ICMP Echo Reply messages received.
IcmlnTimestamps	The number of ICMP Timestamp (request) messages received.

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

2. Click **Update** to update the page with the most current data.

## VLAN

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 can also be used when a VLAN spans multiple physical networks, or when more segmentation or security is required. This section shows how to configure XS728T software to support VLAN routing.

From the VLAN link, you can access features described in the following sections:

- [VLAN Routing Wizard](#)
- [VLAN Routing](#)

## VLAN Routing Wizard

The VLAN Routing Wizard allows you to create 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.
- Add selected LAGs 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 settings:

1. Select **Routing > VLAN > VLAN Routing Wizard**.
2. In the **VLAN ID** field specify a VLAN ID.

This VLAN identifier (VID) associated with this VLAN is created if it does not exist. The valid range is 1–4093.

3. In the **IP Address** field, specify the IP address of the VLAN interface.
4. In the **Network Mask** field, specify the subnet mask of the VLAN interface.
5. Select the operation mode for ports and LAGs.

The Port and LAG blocks each display selectable physical ports and LAGs (if any). Selected interfaces are added to the routing VLAN. Each interface can be configured to operate in one of three modes:

- **T (Tagged)**. Select the interfaces on which all frames transmitted for this VLAN are tagged. The interfaces that are selected are included in the VLAN.
  - **U (Untagged)**. Select the interfaces on which all frames transmitted for this VLAN are untagged. The interfaces that are selected are included in the VLAN.
  - **Blank (Autodetect)**. Select the interfaces that might be dynamically registered in this VLAN using GVRP. This selection has the effect of excluding an interface from the selected VLAN.
6. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

## VLAN Routing

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 settings:**

1. Select **Routing > VLAN > VLAN Routing**.
2. In the **VLAN** list, Select the existing VLAN you want to configure for VLAN Routing.  
The **MAC Address** field displays the MAC Address associated with the VLAN Routing Interface.
3. In the **IP Address** field, enter an IP Address of the VLAN Routing Interface.
4. In the **Subnet Mask** field, Enter a subnet mask for the VLAN Routing Interface.
5. Click **Add** to add the VLAN Routing Interface specified in the **VLAN ID** field to the switch configuration.
6. Click **Apply** to send the updated configuration to the switch.  
Configuration changes take place immediately.

## Routing Table

From the **Routing Table** screen, you can configure static and default routes and view the routes that the NETGEAR switch has already learned.

➤ **To configure routes:**

1. Select **Routing > Routing Table**.
2. In the **Route Type** field, specify whether the route is to be a default route or a static route.  
When you create a default route, all you need to specify is the next hop IP address.
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, indicate the portion of the IP address that identifies the attached network.
5. In the **Next Hop IP Address** field, specify 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 you create a route, the next hop IP must be on the same network as the routing interface. Valid next hop IP addresses can be seen on the Route Table screen.
6. In the **Preference** field, specify a preference value for the configured next hop.

Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, the user controls whether a static route is more or less preferred. The preference is an integer value from 1 to 255. You can specify the preference value (sometimes called “administrative distance”) of an individual static route.

7. Click **Add** to add the routing entry to the switch configuration.

To delete a route, select the check box next to the route and click **Delete**.

The Learned Routes table provides information about the routes the switch already has in its routing table.

The following fields are displayed:

**Table 4-1.**

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 field 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 the following: <ul style="list-style-type: none"> <li>• Local</li> <li>• Static</li> </ul>
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 value for the configured next hop.

## ARP

The Address Resolution Protocol (ARP) associates a Layer 2 MAC address with a Layer 3 IPv4 address. The switch software features both dynamic and manual ARP configuration. With manual ARP configuration, you can statically add entries to 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. Learning is achieved by broadcasting an ARP request packet, to which the intended recipient responds with a unicast 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 its 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 NETGEAR switches support 1024 ARP entries. These entries include 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 might have disappeared from the network altogether (that is, 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 an ageout interval, specified through configuration.

From the ARP menu, you can access features described in the following sections:

- [ARP Cache](#)
- [ARP Entry Configuration](#)
- [Global ARP Configuration](#)
- [ARP Entry Management](#)

## ARP Cache

➤ **To view entries in the ARP table, a table of the remote connections most recently seen by this switch.**

1. Select **Routing > ARP > Basic > ARP Cache**.

The following ARP cache fields display:

- **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 attached device.
- **Type.** The type of the ARP entry. The 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 learned by the router.

2. Click **Update** to update the page with the most current data.

## ARP Entry Configuration

### ➤ To add a static entry to the ARP table:

1. Select **Routing > ARP > Advanced > ARP Create**.
2. In the **IP Address** field, specify the IP address that you want to add.

It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.

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 **Add** to add the static entry to the switch configuration.

To delete a static entry from the ARP cache, select **Delete**.

Entries for the switch are displayed in the Routing VLANs ARP Cache Table. This table contains both static and dynamic addresses. Static addresses are manually configured and do not age out. The device creates dynamic addresses from the ARP packets it receives. Dynamic addresses age out after a configured time

## Global ARP Configuration

Use the Global ARP Configuration screen to display and change the configuration parameters of the ARP table.

### ➤ To configure the global ARP settings:

1. Select **Routing > ARP > Advanced > Global ARP Configuration**.
2. In the **Age Time** field, enter the value you want the switch to use for the ARP entry ageout time.

You must enter an integer value, which represents the number of seconds it takes for an ARP entry to age out. The valid range is 15 – 21,600 seconds. The default value is 1200 seconds.

3. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

## ARP Entry Management

Use this screen to remove entries from the ARP Table.

### ➤ To remove entries from the ARP table:

1. Select **Routing > ARP > Advanced > ARP Entry Management**.

2. In the **Remove From Table** field, select the ARP entries to remove.

The following are ARP entries then can be removed:

- **All Dynamic Entries.** Remove the dynamic entries from the ARP table.
  - **All Static Entries.** Remove the static entries from the ARP table.
  - **All Entries.** Remove all static and dynamic entries from the ARP table.
  - **Specific Entry.** Remove a specific ARP entry from the ARP table. If you select Specific Entry in the Remove from Table list, you can enter the IP address of an entry to remove from the ARP table.
  - **None.** Select if you do not want to delete any entry from the ARP Table.
3. Click **Apply** to send the updated configuration to the switch.

Configuration changes take place immediately.

## IPv6

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

- [Global Configuration](#)
- [Route Table](#)
- [VLAN Configuration](#)
- [IPv6 Addresses](#)
- [Prefix Configuration](#)
- [IPv6 Interface Statistics](#)
- [Neighbor Table](#)

### Global Configuration

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

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

#### ➤ Configure IPv6 Global Configuration.

1. In the **IPv6 Unicast Routing** field, select the option to globally Enable or Disable IPv6 unicast routing. The default setting is Disable.
2. In the **IPv6 Hop Limit** field, enter a value for the unicast hop count used in IPv6 packets originated by the node. Valid values for hops are 1 to 255, inclusive. The default is 64.
3. In the **ICMPv6 Rate Limit Error Interval** field, specify the interval for sending “burst size” ICMPv6 error packets. This value controls the ICMPv6 error packets. The default Rate Limit is 100 packets per second, meaning that the burst interval is 1000 mseconds. To disable

ICMP Rate Limiting, set this field to 0. The valid Rate Interval must be in the range 0 to 2147483647 micro seconds.

4. In the **ICMPv6 Rate Limit Burst Size** field, specify the number of ICMP error packets allowed per burst interval. This value controls the ICMP error packets. Default burst size is 100 packets. Valid Burst Size must be in the range of 1 to 200.
5. In the **IPv6 MTU** field, specify in bytes the maximum Transmitted packet size for IPv6 routing. This must be in the range of 1280 to 9000. The default setting is 1500 bytes.
6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

## Route Table

The Route table contains all the IPv6 routes, static and non-static that exist on the device.

### ➤ To add a static IPv6 route to the Route Table:

1. Click **Routing > IPv6 > Basic > Route Table**.
2. Enter the following fields for the route:
  - **IPv6 Prefix**. Enter the network prefix.
  - **Prefix Length**. Enter the network length.
  - **Next Hop IPv6 Address Type**. Select either **Link Local** or **Global**.
  - **Next Hop IPv6 Address**. Enter the next hop IPv6 address for the route.
  - **Interface**. Enter the outgoing IPv6 routing VLAN Interface to use when forwarding traffic to the destination.
  - **Preference**. Enter the route preference of this route.
3. Select the IPv6 Route Table to display.
4. In the **Routes Displayed** list, select from the following:
  - **All Routes**. Shows all best active IPv6 routes.
  - **All Static Routes**. Shows the static routes configured by the users.

The fields described above are displayed for the routes. In addition, the following fields are described:

- **Protocol**. How route was created. The following options are available:
    - **Static**. Manually defined.
    - **ND (Neighbor Discovery)**. Discovered by ND protocol.
    - **Connected**. Route was derived from a manually-configured device's IPv6 address.
  - **Next Hop Interface**. Enter the network length.
5. Click **Update** to update the page with the latest information on the switch.

## VLAN Configuration

➤ **To configure IPv6 settings on VLAN interfaces:**

1. Click **Routing > IPv6 > Advanced > VLAN Configuration**.
2. Select the check box next to the VLAN **Interface** for which data is to be displayed or configured. All VLAN interfaces are valid.
3. Select **Enable** or **Disable** in the **IPv6 Admin Mode** list. When IPv6 admin mode is enabled, the interface is capable of IPv6 operation. The default value is Disable.
4. In the **Stateless Address AutoConfig Mode** list, select to **Enable** or **Disable** Stateless Address AutoConfig mode on an interface. The default value is disable.
5. In the **Duplicate Address Detection Transmit** field, specify the number of duplicate address detection (DAD) transmits on an interface. DAD transmits values must be in the range 0 to 600. The default is 1.
6. Specify the router advertisement **Life Time Interval** sent from the interface. This value must be greater than or equal to the maximum advertisement interval. 0 means do not use the router as the default router. The range of router life time is 0 to 9000. The default is 1800.
7. In the **Adv NS Interval** field, specify the retransmission time field of router advertisement sent from the interface. A value of 0 means the interval is not specified for the router. The range of neighbor solicit interval is 1000 to 4294967295. The default is 0.
8. In the **Adv Reachable Interval** field, specify the router advertisement time to consider neighbor reachable after ND confirmation. The range of reachable time is 0 to 3600000. The default is 0.
9. Use the **Adv Interval** field to specify the maximum time allowed between sending router advertisements from the interface. The range of maximum advertisement interval is 4 to 1800. The default value is 600.
10. In the **Adv Manage Config Flag** list, select **Enable** or **Disable** to specify the router advertisement of the manage configuration flag. Default value of this flag is Disable.
11. In the **Adv Other Config Flag** list, select **Enable** or **Disable** to specify the router advertisement of the other stateful configuration flag. Default value of this flag is Disable.
12. In the **Adv Suppress Flag** list, select to **Enable** or **Disable** router advertisement suppression on an interface. The default value of this flag is Disable.
13. In the **Destination Unreachables** list, select to **Enable** or **Disable** the Mode of Sending ICMPv6 Destination Unreachables on this interface. If **Disabled**, then this interface will not send ICMPv6 Destination Unreachables. By default, the IPv6 Destination Unreachables mode is Enable.
14. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

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

Field	Description
Operational Mode	Specifies IPv6 operational state of an interface. The possible values are Enable or Disable.
Link State	Indicates the operational state of the specified VLAN interface. Possible values: Link up or Link down.

## IPv6 Addresses

This page enables adding or modifying IPv6 Global addresses. IPv6 Link Local addresses are created automatically when enabling IPv6 admin mode on a VLAN interface and cannot be removed or edited.

➤ **To configure an IPv6 address for an IPv6 Interface:**

1. Select **Routing > IPv6 > Advanced > IPv6 Addresses**.
2. In the **IPv6 Interface Selection** section, select a VLAN interface (to be assigned the IPv6 address).
3. In the IPv6 Interface Configuration section, configure the following:
  - **IPv6 Prefix/Prefix Length**. Select an existing IPv6 prefix and prefix length from the list, or add a new IPv6 prefix and prefix length to the list of IPv6 addresses. The address is in the global address format.
  - **EUI64**. Specify whether the IPv6 address is in EUI-64 format. The default value is Disable.
4. Click **Add** to add a new IPv6 address, or click **Delete** to delete a selected IPv6 address from the list of IPv6 addresses.
5. Click **Apply** to apply the changes to the system.

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

Field	Description
Current State	The state of the IPv6 address. The state is <b>Tent</b> if routing is disabled or DAD fails. The state is <b>Active</b> if the interface is active and DAD is successful. The state is <b>Preferred</b> if the IPv6 address has been verified to be unique on the link and is therefore active.

## Prefix Configuration

➤ **To add an IPv6 prefix that will be advertised on an IPv6 enabled interface:**

1. Click **Routing > IPv6 > Advanced > Prefix Configuration**.
2. From the **Interface** list, select the interface to be configured. When the selection is changed, a screen update occurs, causing all fields to be updated for the newly selected port. All physical interfaces are valid.

3. In the **IPv6 Prefix** field, specify the IPv6 prefix for an interface. The IPv6 Prefix can include only Prefix and not Host ID information. For example 3000:3000::
4. In the **Prefix Length** field, specify the IPv6 prefix length for an interface.
5. In the **Valid Life Time** field, specify the router advertisement per prefix time to consider the prefix valid for the purpose of on-link determination. Valid life time must be in the range 0 to 4294967295. Default value is 2592000.
6. In the **Preferred Life Time** field, specify the router advertisement per prefix time. An auto-configured address generated from this prefix is preferred. Preferred life time must be in the range 0 to 4294967295. Default value is 604800.
7. From the **Onlink Flag** list, select **Onlink**, **No-Onlink** or **Off-Link** according to whether the selected prefix can be used for on-link determination, and whether a prefix will be inserted into the routing table. The default is **Onlink**.
8. In the **Autonomous Flag** list, select **Enable** or **Disable** depending on whether the selected prefix can be used for autonomous address configuration. The default value is **Enable**.
9. Click **Add** to add a new IPv6 address to the interface. Configuration changes take effect immediately.
10. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

## IPv6 Interface Statistics

➤ **To display IPv6 Interface Statistics:**

1. Select **Routing > IPv6 > Advanced > Statistics**.
2. From the **Interface** list, select the VLAN interface on which to display statistics. When the selection is changed, a screen refresh occurs, causing all fields to be updated for the newly selected interface.
3. Click **Update** to update the page with the latest information on the switch.

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

Field	Description
Total Datagrams Received	The total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Header Errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.
Received Datagrams Discarded Due To MTU	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	The number of input datagrams discarded because no route could be found to transmit them to their destination

Field	Description
Received Datagrams With Unknown Protocol	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses(e.g., addresses with unallocated prefixes).For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received Datagrams Discarded Due To Truncated Data	The number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Received Datagrams Reassembly Required	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Datagrams Successfully Reassembled	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
Datagrams Failed To Reassemble	The number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Datagrams Forwarded	The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful.Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.

## Neighbor Table

➤ To display the IPv6 Neighbor Table page:

1. Click **Routing > IPv6 > Advanced > Neighbor Table**.
2. Use the **Search** field to search for IPv6 routes by IPv6 address or interface.

3. To search by IPv6 address, select **IPv6 Address** from the **Search** list. Enter the 128-byte hexadecimal IPv6 address in four-digit groups separated by colons, for example 2001:231F:::1. Then click **Go**. If the address exists, that entry will be displayed. An exact match is required.
4. To search by VLAN, select **Interface** from the **Search** list, enter the VLAN ID, for example "VLAN 1" (VLAN needs to be all capitals) and click **Go**. If the address exists, that entry will be displayed.
5. Click **Clear** to clear the IPv6 neighbors on a selected interface or on all interfaces.
6. Click **Update** to update the page with the latest information on the switch.

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

Field	Description
IPv6 Address	The IPv6 address of the neighbor.
Interface	The interface whose settings are displayed in the current table row.
MAC Address	Specifies MAC address associated with a neighbor.
isRtr	Indicates whether the neighbor is a router. If the neighbor is a router, the value is <b>True</b> . If the neighbor is not a router, the value is <b>False</b> .
Neighbor State	<p>Specifies the state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> <li>• <b>Incomplete</b>. Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.</li> <li>• <b>Reachable</b>. Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.</li> <li>• <b>Stale</b>. More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.</li> <li>• <b>Delay</b>. More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.</li> <li>• <b>Probe</b>. A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.</li> </ul>
Last Updated	Time since the address was confirmed to be reachable.



# Quality of Service

---

# 5

Use the features you access from the QoS tab to configure Quality of Service (QoS) settings on the switch.

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 are 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 packets that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this special treatment 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.

The QoS tab contains menus that provide access to the following sections:

- [CoS](#)
- [Differentiated Services](#)

## CoS

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for various types of network traffic when the complexities of Differentiated Services (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 CoS menu under the QoS tab, you can access the following:

- *CoS Configuration*
- *CoS Interface Configuration*
- *Interface Queue Configuration*
- *802.1p to Queue Mapping*
- *DSCP to Queue Mapping*

### CoS Configuration

Use the CoS Configuration screen to set the Class of Service global trust mode. This global setting is applied to each port in the switch to trust one of the packet fields (802.1p or IP DSCP), or to not trust a packet's priority designation (untrusted mode). This mapping table indicates the CoS queue to which the packet must be forwarded on the appropriate egress ports. The trusted field must exist in the packet for the mapping table to be of any use, so default actions are 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 ports, in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping is unable to be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

#### ➤ To configure global CoS settings:

1. Select **QoS > CoS > Basic > CoS Configuration**.
2. From the **Global Trust Mode** menu, specify whether to trust a particular packet marking at ingress.

Global Trust Mode can be only 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 four internal hardware priority queues. This is the default setting.
  - **DSCP.** The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.
3. Click **Apply** to send the updated configuration to the switch.

## CoS Interface Configuration

Use the CoS Interface Configuration screen to apply an interface ingress rate limit or egress 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 type of interface for CoS settings to be configured:

To configure CoS settings for a physical port, link aggregation group (LAG), or both, click **PORTS**, **LAGS** or **All**, respectively.

3. Select the check box next to the interface to configure.

You can select multiple ports and LAGs to apply the same setting to the selected interfaces.

The **Interface Trust Mode** field displays whether the selected interfaces trust a particular packet marking when the packet enters the port. The data for all the ports is taken from the Global Trust Mode.

- **Untrusted.** Do not trust any CoS packet marking at ingress.
  - **802.1p** or **DSCP.** Apply the global trust mode set in the CoS configuration.
4. In the **Interface Shaping Rate** field, specify the maximum bandwidth allowed.  
This specification is typically used to shape the outbound transmission rate in this range of 64–10000000 Kbps. The shaping rate (KB) value is the value of the interface shaping rate configured. The default value is 0. The value 0 means that the maximum is unlimited.
  5. In the **Interface Ingress Rate Limit** field, specify the ingress rate allowed.  
The range is 100–10000000 Kbps. The default value is 0, which means that the maximum is unlimited.
  6. Click **Apply** to apply the changes to the system.

## Interface Queue Configuration

Use the 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 and the scheduling of packet transmission from the set of all queues on a port. The CoS queue configuration is global.

You can configure eight queues as strict priority or weighted round robin (WRR) priority, or combination of both. If a specific queue is configured as WRR, all the queues with a lower number are also WRR queues. The configuration is global and not per port.

➤ **To configure CoS queue settings:**

1. Select **QoS > CoS > Advanced > Interface Queue Configuration**.
2. Select the check box next to the queue to configure.

You can select multiple queues to apply the same setting to the selected interfaces.

3. Configure any of the following settings:
  - **Minimum Bandwidth.** Enter a value in the range 1–100 that reflects the relative bandwidth of this queue. The bandwidth allocation per queue is the configured weight divided by the sum of all the configured weights. The sum of the minimum bandwidths for all queues does not have to equal 100. This setting is configurable only if the Scheduler type field is set to Weighted.
  - **Scheduler Type.** Select the type of queue processing. Options are Weighted and Strict. Defining on a per-queue basis enables you to create the desired service characteristics for different types of traffic. Eight queues can be configured as strict priority or WRR priority. If a specific queue is configured as WRR, all the queues with a lower number are also WRR queues. The configuration is global and not per port.
    - **Weighted.** Weighted round robin associates a weight to each queue. This association is the default.
    - **Strict.** Services traffic with the highest priority on a queue first.
  - **Queue Management Type.** Displays 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 **Apply** to apply the changes to the system.

## 802.1p to Queue Mapping

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

➤ **To map 802.1p priorities to queues:**

1. Select **QoS > CoS > Advanced > 802.1p to Queue Mapping**.
2. For each **802.1p Priority** value, select the queue to which it will be mapped.

The queue values represent traffic classes. 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.

Traffic classes go 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.

3. Click **Apply** to apply the changes to the system.

## DSCP to Queue Mapping

Use the DSCP to Queue Mapping screen to specify which internal traffic class to map to the corresponding DSCP value.

Do this for each of the following groups, as required:

- Class Selector (CS) Per-hop Behavior (PHB)
- Assured Forwarding (AF) PHB
- Expedited Forwarding (EF) PHB
- Other DSCP Values (Local/Experimental Use)

### ➤ To map DSCP values to queues:

1. Select **QoS > CoS > Advanced > DSCP to Queue Mapping**.
2. For each DSCP value (in each type of differentiated service), 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. The valid range is 0–7.

3. Click **Apply** to apply the changes to the system.

## Differentiated Services

The QoS feature provides Differentiated Services (DiffServ) support that enables traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors. For more information, see [DiffServ Traffic Classes](#) on page 204.

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 might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. Conversely, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

To use DiffServ for QoS, you must first define the following categories and their criteria:

1. **Class.** Create classes and define class criteria.
2. **Policy.** Create policies, associate classes with policies, and define policy statements.
3. **Service.** Add a policy to an inbound interface.

Packets are classified and processed based on defined criteria. A class defines the classification criteria. A policy’s attributes define the processing. Policy attributes might 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 checking the class match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

From the DiffServ menu under the QoS tab, you can access the following:

- *Diffserv Configuration*
- *DSCP Violate Action Mapping*
- *Class Configuration*
- *IPv6 Class Configuration*
- *Policy Configuration*
- *Service Configuration*
- *Service Statistics*

## 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 number of used resources for DiffServ.

### ➤ To view DiffServ general status group information:

Select **QoS > DiffServ > Basic > Diffserv Configuration**.

The following information is displayed:

- The **Admin Mode for DiffServ** is always Enabled.
- The **DiffServ Used Resources** field displays the number of entries used by DiffServ.

## DSCP Violate Action Mapping

When a policer is assigned to a class map (flows), use the DSCP Violate Action Mapping screen to specify the action to take when the amount of traffic in the flows exceeds the QoS-specified limits. The portion of the traffic that causes the flow to exceed its QoS limit is referred to as violate action packets.

When this action occurs, the switch remaps the original DSCP value of the violate action IP packets with a new value based on the DSCP Violate Action Mapping table. The switch uses the new values to assign resources and the egress queues to these packets. The switch also physically replaces the original DSCP value in the violate action packets with the new DSCP value.

This feature changes (remarks) the DSCP tags for incoming traffic switched between trusted QoS domains.

For example, assume that there are three levels of service—A, B, and C—and the DSCP incoming values used to mark these levels are 10, 20, and 30 respectively. If this traffic is forwarded to another service provider that has the same three levels of service, but uses DSCP values 16, 24, and 48, the DSCP violate action mapping changes the incoming values as they are mapped to the outgoing values.

➤ **To configure the DSCP violate action mapping:**

1. Select **QoS > DiffServ > Basic > DSCP Violate Action Mapping**.
2. For each **DSCP In** value, select a **DSCP Out** value (if necessary).

Do this for each of the following groups, as required:

- Class Selector (CS) Per-hop Behavior (PHB)
- Assured Forwarding (AF) PHB
- Expedited Forwarding (EF) PHB
- Other DSCP Values (Local/Experimental Use)

3. Click **Apply** to apply the changes to the system.

## Class Configuration

Use one of the Class Configuration screens to add a DiffServ class name, or to rename or delete an existing class. For IPv4 packets use the Class Configuration screen. For IPv6 packets use the IPv6 Class Configuration screen.

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.

➤ **To add a new class:**

1. Select **QoS > DiffServ > Advanced > Class Configuration**.

All the previously defined classes are displayed.

2. Enter the new class name.
3. Select the class type, and click **Add**.

The switch supports only the Class Type value All, which means all the various match criteria defined for the class must be satisfied for a packet match. All signifies the logical AND of all the match criteria.

4. Click **Apply** to save the class.

To configure this class, proceed to *To configure a class*:

Use the buttons at the top of the screen to perform the following:

- To remove a class, select the check box beside the class name, then click **Delete**.
- To cancel the configuration you just entered, click **Cancel**.

➤ **To configure a class:**

1. Click a class name (which is a hyperlink) for an existing class.

When you click a class name, the configuration part of the Class Configuration screen is displayed. In this part of the screen, you define against which values traffic is checked when this class is applied.

2. To define the criteria to associate with a DiffServ class, select one or more of the following check boxes and enter the following data:
  - **Match Every.** Select Any to add a match condition to the specified class definition whereby all packets are considered to belong to the class. In this case, no other field can be configured.
  - **Class of Service.** Select a Class of Service 802.1 p user priority value to be matched.
  - **VLAN.** Enter a VLAN ID to be matched.
  - **Ethernet Type.** Select an Ethernet type from the list, or select User Value and add a value.
  - **Source MAC.** Enter the source MAC address and the mask.
  - **Destination MAC.** Enter the destination MAC address and the mask.
  - **Protocol Type.** Select the protocol type. If you select Other, enter a protocol number in the field that appears.
  - **Source IP.** Enter a valid source IP address in dotted-decimal format.
  - **Source L4 Port.** Select the desired L4 keyword from the list on which the rule can be based. The options are Other, domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, or www. If you select Other, enter a user-defined port ID.
  - **Destination IP.** Enter a valid destination IP address in dotted-decimal format.
  - **Destination L4 Port.** Enter the desired L4 keyword from the list on which the rule can be based. The options are Other, domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, or www. If you select Other, the screen refreshes and a port ID field appears.
  - **Service Type:**
    - **IP DSCP.** Select the DSCP type from the list or enter a DSCP value to match. If you select Other, enter a custom value in the DSCP Value field that appears. The range is 0–63.
    - **Precedence Value.** Enter a precedence value.
3. Click **Apply** to send the updated configuration to the switch. Configuration changes occur immediately.

## 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.

When you define a class, you must specify if this class rule is for IPv4 or for IPv6 packets by using the correct screen (either Class Configuration or IPv6 Class Configuration).

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 allowed only 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 and DiffServ assignment are appropriate for LAG interfaces. The procedures described by an ACL or DiffServ policy are equally applicable on a port or LAG interface.

➤ **To configure an IPv6 class:**

1. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.
2. Enter the new class name.
3. Select the class type, and click **Add**.

The switch supports only the Class Type value All, which means all the various match criteria defined for the class must be satisfied for a packet match. All signifies the logical AND of all the match criteria.

4. Click **Apply** to save the class. Configuration changes take effect immediately.
5. To configure this class, proceed to *To configure an IPv6 class*: on page 109.

➤ **To configure the class match criteria:**

1. In the IPv6 Class Configuration screen, click on the name of the class (which is a hyperlink).

When you click a class name, the configuration part of the Class Configuration screen is displayed. In this part of the screen, you define against which values traffic is checked when this class is applied.

2. To define the criteria to associate with a DiffServ class, select one or more of the following check boxes and enter the following data:
  - **Match Every.** Select All to add a match condition to the specified class definition whereby all packets are considered to belong to the class. In this case, no other field can be configured.
  - **Protocol Type.** Select a Layer 4 protocol. If you select Other, enter a protocol number in the field that appears.
  - **Source Prefix/Length.** Enter a valid source IPv6 prefix. A prefix is always specified with the prefix length. The valid range for a prefix is 0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. The valid range for a prefix length is 0–128.
  - **Source L4 Port.** Select a keyword for the known source Layer 4 ports. If you select Other, enter a protocol number in the field that appears.
  - **Destination Prefix/Length.** Enter a valid destination IPv6 prefix to compare against an IPv6 packet. A prefix is always specified with the prefix length. The valid range for

a prefix is FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. The valid range for a prefix length is 0–128.

- **Destination L4 Port.** Select a known destination Layer 4 ports. If you select Other, enter a protocol number in the field that appears.
  - **IP DSCP.** Select a known DSCP value. If you select Other, enter a protocol number in the field that appears.
3. Click **Apply** to save the class. Configuration changes take effect immediately.

## 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 name to go to the Policy Configuration screen.

### ➤ To configure a DiffServ policy:

1. Select **QoS > DiffServ > Advanced > Policy Configuration**.
2. Enter a policy name in the **Policy Name** field.

The available policy type is In, which indicates the type is specific to inbound traffic. This field is not configurable.

3. Select an existing DiffServ class in the **Member Class** field to associate with the policy, and click **Add**.

To configure this policy, proceed to *To configure the policy attributes:* on page 110.

### ➤ To configure the policy attributes:

1. In the Policy Configuration screen, click the name of the policy (which is a hyperlink).
2. Configure the policy attributes by selecting the check box associated with the attribute to be configured and then entering the required data:
  - **Assign Queue.** Select the destination queue. There are eight queues with valid values from 0 to 7 (7 is the highest).
  - **Drop.** Select this option to drop packets for this policy-class.
  - **Mark VLAN CoS.** Select the specified Class of Service queue number to mark all packets for the associated traffic stream with the specified Class of Service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted.
  - **Mark IP DSCP.** Select an IP DSCP value. All packets for the associated traffic stream are marked with this value. If you select **Other**, enter a custom value in the DSCP Value field that appears.
  - **Simple Policy.** Select this radio button to establish the traffic policing style for the specified class. The simple form of the policy command uses a single data rate and burst size, resulting in two outcomes: confirm and violate.
3. If you select the **Simple Policy** radio button, you can 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.
- **Committed Rate.** The committed rate is the average bandwidth in bits per seconds specified in kilobits-per-second (Kbps) and is an integer from 100 to 1000000.
- **Committed Burst Size.** The committed burst size is the maximum amount of traffic allowed in one burst (in bytes) and is an integer from 3000 to 19173960.

---

**Note:** The Token Bucket algorithm is used, in which the committed rate is the rate at which the bucket is filled, and the committed burst size is the size of the bucket. This means that the committed burst size is the maximum size of a burst that can be sent.

---

- **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 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 appears.
  - **Violate Action.** Determines what happens to packets that are considered non-conforming (above the police rate). Select one of the following actions:
    - **Send.** These packets are presented unmodified by DiffServ to the system forwarding element.
    - **Drop.** These packets are immediately dropped.
4. Click **Apply** to send the updated configuration to the switch.  
Configuration changes take effect immediately.

## Service Configuration

Use the Service Configuration screen to activate a policy on an interface.

- **To configure DiffServ policy settings on an interface:**
  1. Select **QoS > DiffServ > Advanced > Service Configuration.**
  2. To configure DiffServ policy settings for a physical port, link aggregation group (LAG) or both, click **PORTS**, **LAGS** or **All**, respectively.

3. Select the check box next to the port or LAG to configure.

You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

4. Select a previously defined policy or **None** from the Policy In list and click **Apply**.  
None removes all policies from the interfaces.

## Service Statistics

Use the Service Statistics screen to display service-level statistical information about all interfaces that have DiffServ policies attached.

### ➤ To display and refresh service-level statistical information:

1. Select **QoS > DiffServ > Advanced > Service Statistics**.
2. The following fields are displayed:
  - **Interface**. The interface for which service statistics display.
  - **Direction**. The direction of packets for which service statistics display, which is always In.
  - **Policy Name**. The policy associated with the selected interface.
  - **Operational Status**. The operational status of this service interface, which is either Up or Down.
  - **Member Classes**. Selects the member class for which octet statistics are to display.
3. Click **Update** to update the screen with the most current information.

# Security

---

# 6

Use the features available from the Security tab to configure management security settings for port, user, and server security. The Security tab contains menus that provide links to screens described in the following sections:

- *Management Security Settings*
- *Access*
- *Port Authentication*
- *Traffic Control*
- *ACL*

## 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.

To display the screen, click the **Security > Management Security** tab. The Management Security tab provides links to features described in the following sections:

- [Change Password](#)
- [RADIUS](#)
- [TACACS+](#)
- [Authentication List](#)

### Change 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 a new password in the **New Password** field.  
It does not display as it is typed, and only asterisks (\*) 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 that you entered it correctly.  
This field displays asterisks (\*)
  5. Click **Apply** to apply the new settings to the system.  
Configuration changes take effect immediately.
- **To reset the password for the management interface:**
  1. Select the **Reset Password** check box to reset the password to the default value.
  2. Click **Apply** to apply the new settings to the system.  
Configuration changes take effect immediately.

---

**Note:** In the case of a lost password, press the **Factory Default Reset** button on the front panel for more than two seconds to restore the default. The reset button only reboots the device.

---

## RADIUS

RADIUS servers provide authentication, authorization, and accounting services for networks. The RADIUS server maintains a user database, which contains per-user authentication information. The switch passes information to the configured RADIUS server, which can authenticate a user name and password before authorizing use of the network. RADIUS servers provide a centralized authentication method for:

- Web access
- Access control port (802.1x)

The RADIUS menu contains links to features described in the following sections:

- [Global Configuration](#)
- [Server Configuration](#)
- [Accounting Server Configuration](#)

### Global Configuration

Use the RADIUS Configuration screen to add information about one or more RADIUS servers on the network.

#### ➤ 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 162). The switch supports up to eight configured RADIUS servers. If more than one RADIUS server is 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 maximum number of times a request packet is retransmitted to the RADIUS server. The valid range is 1-15 and the default is 3.
3. In the **Timeout Duration** field, specify the time-out value, in seconds, for request retransmissions. The valid range is 1-30 seconds and the default is 3 seconds.

Consideration to maximum delay time must be given when configuring RADIUS maximum retransmit and RADIUS time-out values. If multiple RADIUS servers are configured, the maximum retransmit value on each is exhausted before the next server is attempted. A retransmit does not occur until the configured time-out value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit \* time-out) for all configured servers. If the RADIUS request is generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a response.

4. From the **Accounting Mode** list, select whether the RADIUS accounting mode is enabled or disabled on the current server. RADIUS accounting is provided for both AAA and 802.1x sessions.
5. Click **Apply**.

Configuration changes take effect immediately.

## Server Configuration

Use the RADIUS Server Configuration screen to view and configure various settings for the current RADIUS server configured on the system.

➤ **To configure a RADIUS server for authentication and authorization:**

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 0–65535. The default port for RADIUS authentication is UDP 1812.

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 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, specify whether the server is a primary or secondary server.
7. Click **Add**.

Configuration changes take effect immediately.

To modify settings for a RADIUS server that is already configured on the switch, select the check box next to the server address field, update the desired fields, and click **Apply**.

## Accounting Server Configuration

Use the Accounting Server Configuration screen to view and configure various settings for a RADIUS accounting server on the network. RADIUS accounting is provided for both AAA and 802.1x sessions.

➤ **To configure the RADIUS accounting server:**

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 use.
3. In the **Port** field, specify the UDP port number the server uses to verify the RADIUS accounting server authentication.

The valid range is 0–65535. The default port for RADIUS accounting is UDP 1813.

4. From the **Secret Configured** list, 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 RADIUS accounting server.
6. From the **Accounting Mode** list, enable or disable the RADIUS accounting mode.
7. Click **Apply** to update the switch with the RADIUS Accounting server settings.

## 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 using 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+ menu contains links to screens described to the following sections:

- [TACACS+ Configuration](#)
- [TACACS+ Server Configuration](#)

### TACACS+ Configuration

The TACACS+ Configuration screen contains the TACACS+ settings for communication between the switch and the TACACS+ server you configure through 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. The default is 5 seconds.

4. Click **Apply** to update the switch with the TACACS+ Accounting server settings.

## TACACS+ Server Configuration

Use the TACACS+ Server Configuration screen to configure up to eight TACACS+ servers with which the switch can communicate.

➤ **To configure TACACS+ server settings:**

1. Select **Security > Management Security > TACACS+ > TACACS+ Server Configuration** link.
2. In the **TACACS+ Server** field, enter the IP address of the server to add
3. In the **Priority** field, specify the order in which the TACACS+ servers are used.  
A value of 0 is the highest priority.
4. In the **Port** field, specify the authentication port number through which the TACACS+ session occurs.  
The default is port 49, and the range is 0–65535.
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. In the **Connection Timeout** field, specify the amount of time that passes before the connection between the device and the TACACS+ server times out.  
The field range is 1–30 seconds. The default value is 5.
7. Click **Add**.

---

**Note:** The Add option is available if fewer than five TACACS+ servers are configured on the system.

---

## Authentication List

The Authentication List link provides access to screens where you can 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.

---

The Authentication List link provides access to the features described in the following sections:

- *HTTP Authentication List*

- *HTTPS Authentication List*

## HTTP Authentication List

Use the HTTP Authentication List screen to configure the default HTTP login list.

➤ **To change the HTTP authentication method for the default list:**

1. Select **Security > Management Security > Authentication List > HTTP Authentication List**.
2. Select the check box next to the **List Name**.
3. From the list in the 1 column, select the HTTP authentication method that must 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 is attempted, even if you have specified more than one method. This parameter does not appear when you first create a 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 is used for authentication. Since the local method does not time out, if you select this option as the first method, no other method is tried, even if you have specified more than one method.
- **None**. The authentication method is unspecified. This option is available only for method 2 and method 3.
- **RADIUS**. The user's ID and password is 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 is 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.

---

**Note:** Each authentication protocol can use up to three authentication methods. Local and None must be the last methods. You cannot configure methods after these two options.

---

4. From the list in the 2 column, select the authentication method, if any, that must appear second in the selected authentication login list.

This method will be used if the first method times out.

If you select a method that does not time out as the second method, the third method is not tried. This parameter does not appear when you first create a login list.

5. From the list in the 3 column, select the authentication method, if any, that must appear third in the selected authentication login list.

This parameter does not appear when you first create a login list.

6. Click **Apply** to update the switch with the HTTP Authentication settings.

## HTTPS Authentication List

Use the HTTPS Authentication List to configure the default HTTPS login list.

➤ **To change the HTTPS authentication method for the default list:**

1. Select **Security > Management Security > Authentication List > HTTPS Authentication List**.
2. Select the check box next to the **List Name**.
3. From the list in the 1 column, select the HTTPS authentication method that must 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 is attempted, even if you have specified more than one method. This parameter does not appear when you first create a 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 is used for authentication. Since the local method does not time out, if you select this option as the first method, no other method is tried, even if you have specified more than one method.
- **None**. The authentication method is unspecified. This option is available only for method 2 and method 3.
- **RADIUS**. The user's ID and password is 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 is 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.

---

**Note:** Each authentication protocol can use up to three authentication methods. Local and None must be the last methods. You cannot configure methods after these two options.

---

4. From the list in the 2 column, select the authentication method, if any, that must appear second in the selected authentication login list.

Use this method 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. This parameter does not appear when you first create a login list.

5. From the list in the 3 column, select the authentication method, if any, that must appear third in the selected authentication login list.

This parameter does not appear when you first create a login list.

6. Click **Apply** to update the switch with the HTTPS Authentication settings.

## Access

From the Access tab, 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 tab contains links features described in the following sections:

- [HTTP](#)
- [HTTPS](#)
- [Access Control](#)

### HTTP

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. In the **HTTP Session Soft Timeout** field, specify the number of minutes an HTTP 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 reenter the password to access the management interface. A value of zero corresponds to an infinite timeout. The default value is 10 minutes.

The **Maximum Number of HTTP Sessions** is 5.

3. Click **Apply** to update the switch with the HTTP Authentication settings.

### HTTPS

Secure HTTP enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. When you manage the switch by using a web interface, secure HTTP can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks.

#### HTTPS Configuration

Use the Secure HTTP 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. Use the radio buttons next to the **HTTPS Admin Mode** to 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. In the **HTTPS Port** field, specify the TCP port to use for HTTPS data.

The value must be in the range of 1–65535. Port 443 is the default value. The currently configured value is shown when the web screen is displayed.

4. In the **HTTPS Session Soft Timeout (Minutes)** field, specify the number of minutes an HTTPS session can be idle before a timeout occurs.

After the session is inactive for the configured amount of time, the administrator is automatically logged out and must reenter the password to access the management interface. The default value is 10 minutes.

The **Maximum Number of HTTPS** sessions is 2.

5. Click **Apply** to update the switch with the HTTPS Authentication settings.

## Certificate Management

Use this screen to generate or delete certificates.

### ➤ To manage certificates:

1. Select **Security > Access > HTTPS > Certificate Management**.

Next to the **Certificate Type**, a **Default**, or **User Defined** status displays.

2. Under **Certificate Management**, select how you want to handle certificates:
  - **None**. Do not display the certificates. This selection is the default selection.
  - **Generate Certificates**. Select this option to generate certificate files.
  - **Import Certificates**. Select this option to import certificate files. In the Certificate field, Public Key field and Private Key fields, paste the certificate, public key and private key from an external file.
  - **Generate Certificate Request**. Select this option to generate a certificate request.
  - **Delete Certificate**. Delete corresponding certificate files, if present.
3. Click **Apply** to start the certification process.

### ➤ To generate a certificate request:

1. Select the **Generate Request** radio button.
2. Specify the **Common Name**, **Organization Unit**, **Organization Name**, **Location**, **State**, **Country**, and **Certificate Request**.
3. Click **Generate Request**.

The **Certificate Generation Status** field displays whether SSL certificate generation is in progress.

## Access Control

Access control is composed of access profiles and access rules.

### Access Profile Configuration

➤ **To set up a security access profile:**

1. Select **Security > Access > Access Control > Access Profile Configuration**.
2. In the **Access Profile Name** field, enter the name of the access profile to be added.  
The maximum length is 32 characters.
3. Select one of the following options:
  - **Activate Profile**. Select to activate an access profile.
  - **Deactivate Profile**. Select to deactivate an access profile.
  - **Remove Profile**. Select to remove an access profile. The access profile must be deactivated before removal.
4. Click **Apply** to update the switch with the new settings.  
The Profile Summary field displays the access rules for the profile. These fields are described below.

### Access Rule Configuration

➤ **To add a security access rule:**

1. Select **Security > Access > Access Control > Access Rule Configuration**.
2. In the **Rule Type** field, select **Permit** or **Deny** as the action to be performed when the rule is matched.
3. In the **Service Type** field, select **HTTP**, **Secure HTTP (SSL)**, or **SNMP**.  
The access rule is restricted according to the service type.
4. In the **Source IP Address** field, enter the IP address from which traffic is originated.
5. In the **Mask** field, enter the IP mask of the source IP addresses.
6. In the **Priority** field, enter a priority for the rule.  
The rules are validated against an incoming management request in the ascending order of their priorities. When a rule match is detected, the rule action is performed and subsequent rules 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 **Add**. Make sure that the access profile is created before adding the rules.

➤ **To configure a security access rule:**

1. Select the checkbox next to the security access rule to be modified.
2. Update the relevant fields.

3. Click **Apply** to update the switch with the new settings.

## 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 (unless Dynamic VLAN Assignment is enabled on port, in which case the user is authenticated individually). 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 mode is the default authentication mode.

The 802.1x network has three components:

- **Authenticators.** Specify the port that is authenticated before permitting system access.
- **Supplicants.** Specify the host connected to the authenticated port requesting access to the system services.
- **Authentication Server.** Specify the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

From the Port Authentication menu, you can access features described in the following sections:

- [802.1x Configuration](#)
- [Port Authentication](#)
- [Port Summary](#)
- [Client Summary](#)

## 802.1x Configuration

Use the 802.1x Configuration screen to enable or disable port access control on the system, to enable, or disable the Guest VLAN (which allows unauthenticated users to have limited access to the network resources) and to enable or disable the forwarding of EAPoL frames when 802.1x is disabled on the device.

### ➤ To configure global 802.1x settings:

1. Select **Security > Port Authentication > Basic > 802.1x Configuration**.
2. Next to the **Port Based Authentication State**, select the radio button to enable or disable 802.1x administrative mode on the switch.
  - **Enable.** Port-based authentication is permitted on the switch.
  - **Disable.** The switch does not check for 802.1x authentication before allowing traffic on any ports, even if the ports are configured to allow only authenticated users.
3. Select the radio button in the **Guest VLAN** field to enable or disable Guest VLAN and have untagged incoming frames go to the Guest VLAN.
4. If you enable the guest VLAN, select the **Guest VLAN ID**.

5. Enter the **Guest VLAN Period**.
6. Next to the **EAPOL Flood Mode** field, select whether to enable or disable radio button forwarding of EAPOL frames when 802.1x is disabled on the device.
7. Click **Apply** to update the switch with the new settings.

## 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 table to view all the fields on the Port Authentication screen.

---

2. Select the check box next to the port to configure.

You can also select multiple check boxes to apply the same settings to the select ports, or select the check box in the heading row to apply the same settings to all ports.

3. For the selected ports, 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. The possible field values are:
    - **Auto.** Automatically detect the mode of the interface.
    - **Authorized.** Place the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.
    - **Unauthorized.** Deny 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.** Authentication is based on the MAC address. MAC authentication requires that a guest VLAN be configured on the switch, and that the port be enabled for guest VLAN. The guest VLAN is configured in the 802.1x Configuration page, and the guest VLAN is enabled on the port in the next field in this page.
  - **Dynamic VLAN Assignment.** Enable or disable this feature on the interface. This feature is also known as RADIUS Assigned VLAN Attribute (RAVA). If this feature is enabled RADIUS servers can assign a VLAN ID to a port based on 802.1 authentication. If a user is authenticated, the user will be assigned to this VLAN. When this feature is enabled on a port, each user is individually authenticated.
  - **Guest VLAN.** Enable or disable the Guest VLAN on the interface.

- **Periodic Reauthentication.** Enable or disable reauthentication of the supplicant for the specified port. The default value is Disable. Changing the selection does not change the configuration until you click **Apply**.
  - **Reauthentication Period.** Enter the time span in which the selected port is reauthenticated. The valid range is 300–4294967295, and the default value is 3600 seconds.
  - **Quiet Period.** Enter the amount of time that the switch remains in the quiet state following a failed authentication exchange. The valid range is 30–65535, and the default value is 60 seconds.
  - **Resending EAP.** Enter 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. The valid range is 30–65535, and the default value is 30 seconds.
  - **Max EAP Requests.** Enter the maximum number of requests for the selected port. This value is the maximum number of times the authenticator state machine on this port retransmits an EAPOL EAP Request/Identity before timing out the supplicant. The valid range is 1–10, and the default value is 2.
  - **Supplicant Timeout.** Enter the number of seconds that elapse before EAP requests are resent to the user. The valid range is 1–65535, and the default is 30 seconds.
  - **Server Timeout.** Enter the number of seconds that elapse before the switch resends a request to the authentication server. The valid range is 1–65535, and the default is 30 seconds.
4. For the selected ports, view the following settings, which are not configurable:
- **Control Direction.** Displays 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.** Displays the protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1x specification.
  - **PAE Capabilities.** Displays the port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant.
  - **Authenticator PAE State.** This field displays 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.** Displays the current state of the backend authentication state machine. Possible values are as follows:
  - Request
  - Response
  - Success
  - Fail
  - Timeout
  - Initialize
  - Idle

5. Click **Apply** to update the switch with the new settings.

## Port Summary

Use the Port Summary screen to view summary information about the port-based authentication settings for each port.

➤ **To view information about the port access control settings on a specific port:**

Select **Security > Port Authentication > Advanced > Port Summary**.

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

Field	Description
Port	The port whose settings are displayed in the current table row.
Control Mode	Defines the port authorization state. The control mode is set only if the link status of the port is link up. The possible field values are: <ul style="list-style-type: none"> <li>• <b>Auto.</b> Automatically detects the mode of the interface.</li> <li>• <b>Force Authorized.</b> Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.</li> <li>• <b>Force Unauthorized.</b> 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.</li> </ul>
Operating Control Mode	Indicates the control mode under which the port is actually operating. The possible values are: <ul style="list-style-type: none"> <li>• ForceUnauthorized</li> <li>• ForceAuthorized</li> <li>• Auto</li> <li>• N/A: If the port is in detached state, it cannot participate in port access control.</li> </ul>
Reauthentication Enabled	Displays if reauthentication is enabled on the selected port. This is a configurable field. The possible values are <i>TRUE</i> and <i>FALSE</i> . If the value is <i>TRUE</i> , reauthentication occurs. Otherwise, reauthentication is not allowed.
Port Status	Displays the authorization status of the specified port. The possible values are <i>Authorized</i> , <i>Unauthorized</i> , and <i>N/A</i> . If the port is in detached state, the value is <i>N/A</i> 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 page:**

Click **Security > Port Authentication > Advanced > Client Summary**

The following table describes the fields on the Client Summary screen.

Field	Description
Port	The port to be displayed.
User Name	This field displays the User Name representing the identity of the supplicant device.
Supplicant MAC Address	This field displays supplicant's device MAC Address.

Field	Description
Session Time	This field displays the time since the supplicant has logged in seconds.
VLAN ID	This field displays VLAN ID assigned by the authenticator to the supplicant device.

## Traffic Control

From the Traffic Control menu, you can configure MAC filters, storm control, port security, and protected port settings.

The Traffic Control folder contains links to features described in the following sections:

- [Storm Control](#)
- [Port Security](#)
- [Protected Ports](#)
- [Private VLAN](#)

## 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 cause the network to time out.

The switch measures separately the incoming packet rate for broadcast, multicast, and unknown unicast packets per port and discards packets when the rate exceeds the defined value. You enable storm control per interface by enabling storm control per packet type and defining the rate at which the packets are transmitted.

Storm control is configured as a percent of the maximum port speed, which is 10Gbps for all ports.

### ➤ To configure storm control settings:

1. Select **Security > Traffic Control > Storm Control**.
2. Select the check box next to the port to configure.

Select multiple check boxes to apply the same setting to all selected ports. Select the check box in the heading row to apply the same settings to all ports.

Storm control can be enabled and a threshold can be defined separately for the following packet types:

- **Unknown Unicast.** If the rate of unknown L2 unicast (destination lookup failure), traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped.
- **Multicast.** If the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped.

- **Broadcast.** If the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped.
3. From the **Status** drop-down menu (for each packet type), select **Enable** or **Disable** to specify the administrative status of the mode.
  4. In the **Threshold** field (for each packet type), specify the maximum rate at which packets are forwarded.  
  
The range is a percentage of the total threshold between 0–100%. The default is 5%. Storm control is configured as a percentage of the maximum port speed.
  5. Click **Apply** to update the switch with the new settings.

## Port Security

A MAC address can be dynamically defined as allowable.

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, 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 0.

The Port Security link provides access to the following:

- [Interface Configuration](#)
- [Security MAC Address](#)

## Interface Configuration

### ➤ To configure port security settings:

1. Select **Security > Traffic Control > Port Security > Interface Configuration**.
2. To configure interface security settings for ports and link aggregation groups (LAGs), click **PORTS**, **LAGS**, or **All**.
3. Select the check box next to the port or LAG to configure.  
  
Select multiple check boxes to apply the same setting to all selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
4. Specify the following settings:
  - **Port Security.** Enable or disable the port security feature for the selected port.
  - **Max Allowed Dynamically Learned MAC.** Sets the maximum number of dynamically learned MAC addresses on the selected interface. The valid range is 0–128. The default value is 128.
  - **Enable Violation Traps.** Select Yes or No to enable or disable the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.
5. Click **Apply** to update the switch with the new settings.

## 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 to static addresses:**

1. Select **Security > Traffic Control > Port Security > Security MAC Address**.
2. Check the **Convert Dynamic Address to Static** check box.
3. Click **Apply**.

The dynamic MAC Address entries are converted to static MAC address entries in a numerically ascending order until the static limit is reached.

The Dynamic MAC Addresses Table section shows the MAC addresses and their associated VLANs learned on the selected port. Use the Port List menu to select the port for which you want to display data.

The following table describes the dynamic MAC addresses table fields..

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

If a port is configured as protected, it does not forward traffic to any other protected port on the switch, but it forwards traffic to unprotected ports. Use the Protected Ports screen to configure the ports as protected or unprotected.

➤ **To configure protected ports:**

1. Select **Security > Traffic Control > Protected Ports**.
2. The Port block displays selectable physical ports. Click the box below each port to configure it as a protected port.

Protected ports are marked with a ?. No traffic forwarding is possible between two protected ports.

3. Click **Apply** to update the switch with the new settings.  
Configuration changes take effect immediately.

## Private VLAN

A private VLAN contains switch ports that cannot communicate with each other, but can access another network. These ports are called private ports. Each private VLAN contains one or more private ports and a single uplink port or uplink aggregation group. Note that all traffic between private ports is blocked at all layers, not just Layer 2 traffic, but also traffic such as FTP, HTTP, and Telnet.

The Private VLAN link contains links to the following pages:

- [Private VLAN Type Configuration](#)
- [Private VLAN Association Configuration](#)
- [Private VLAN Port Mode Configuration](#)
- [Private VLAN Host Interface Configuration](#)
- [Private VLAN Promiscuous Interface Configuration](#)

## Private VLAN Type Configuration

➤ To display the Private VLAN Type Configuration page:

1. Click **Security > Traffic Control > Private VLAN > Private VLAN Type Configuration**.
2. Use **Private VLAN Type** to specify the type of Private VLAN. The following options are available:
  - **Unconfigured**: No Private VLAN type. This is the default setting and means that this VLAN is not part of the Private VLAN configuration
  - **Primary**: Used to allow Layer 2 connectivity from promiscuous ports to isolated ports and to community ports.
  - **Isolated**: Used to allow isolated ports to send traffic to the primary VLAN/ Promiscuous ports.
  - **Community**: Used to allow Layer 2 connectivity from community ports to promiscuous ports and to community ports of the same community.
3. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

The following field is displayed:

Field	Description
VLAN ID	Specifies the VLAN ID for which Private VLAN type is being set. The default is 'Unconfigured'.

## Private VLAN Association Configuration

➤ To display the Private VLAN Association Configuration page:

1. Click **Security > Traffic Control > Private VLAN > Private VLAN Association Configuration**.
2. Use **Primary VLAN** to select the primary VLAN ID of the domain. This is used to associate Secondary VLANs to the domain.
3. Use **Secondary VLAN(s)** to display all the statically created VLANs (excluding the primary and default VLANs). This control is used to associate secondary VLANs - isolated and community, to the selected primary VLAN. A single, isolated VLAN and multiple community VLANs can be associated to a single primary VLAN.

4. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

The following fields are displayed:

Field	Description
Isolated VLAN	Displays the isolated VLAN associated with the selected primary VLAN.
Community VLAN(s)	Displays the list of community VLAN(s) associated with the selected primary VLAN.

## Private VLAN Port Mode Configuration

➤ To display the Private VLAN Port Mode Configuration page:

1. Click **Security > Traffic Control> Private VLAN > Private VLAN Port Mode Configuration**.
2. Use **Switch Port Mode** to select the Switch Port Mode. The default is 'General'.
  - **General**: Sets port in General Mode. This means that the port is not a private VLAN port. This is the default configuration.
  - **Private VLAN Promiscuous**: Sets port in Promiscuous Mode. Used for private VLAN configuration.
  - **Private VLAN Host**: Sets port in Host Mode. Used for Private VLAN configuration.
3. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

The following field is displayed:.

Field	Description
Interface	Select the physical or LAG interface for which you want to display or configure data.

## Private VLAN Host Interface Configuration

Use this page to apply Private VLAN Host interface settings on selected device interfaces.

➤ To display the VLAN Host Interface Configuration page:

1. Click **Security > Traffic Control> Private VLAN > Private VLAN Host Interface Configuration**.
2. Use **Host Primary VLAN** to set the primary VLAN ID for Host Association Mode. The range of the VLAN ID is 2-4093. The drop-down box lists only primary VLANs.
3. Use **Host Secondary VLAN** to set the Secondary VLAN ID for Host Association Mode. The range of the VLAN ID is 2-4093. The configured VLAN ID must be previously configured as a secondary VLAN.
4. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

The following fields are displayed:

Field	Description
Interface	Select the physical or LAG interface for which you want to display or configure data.
Operational VLAN(s)	Displays the operational VLAN(s).

## Private VLAN Promiscuous Interface Configuration

Use this page to apply Private VLAN Promiscuous interface settings on selected device interfaces.

➤ **To display the Private VLAN Promiscuous Interface Configuration page:**

1. Click **Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration**.
2. Use **Promiscuous Primary VLAN** to set the Primary VLAN ID for Promiscuous Association Mode. The range of the VLAN ID is 2-4093.
3. Use **Promiscuous Secondary VLAN ID(s)** to set the Secondary VLAN ID List for Promiscuous Association Mode. This field can accept single VLAN ID or range of VLAN IDs or a combination of both in sequence separated by ','. You can specify individual VLAN ID. Eg: 10 You can specify the VLAN range values separated by '-'. E.g. 10-13 You can specify the combination of both separated by ','. Eg: 12,15,40-43,1000-1005,2000 The range of the VLAN ID is 2-4093.

---

**Note:** The VLAN ID List given in this control will replace the configured Secondary VLAN list in the association.

---

4. If you make changes to the page, click **Apply** to apply the changes to the system. Configuration changes take effect immediately.

The following fields are displayed:

Field	Description
Interface	Select the physical or LAG interface for which you want to display or configure data.
Operational VLAN(s)	Displays the operational VLAN(s).

## ACL

Access control lists (ACLs) ensure that only authorized users have access to specific resources while blocking 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. The switch software supports IPv4, IPv6 and MAC ACLs.

To configure an ACL, first create an IPv4-based, IPv6-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/IPv6 and MAC addresses, and other packet-matching criteria. Finally, use the ID number to assign the ACL to a port or to a LAG.

The ACL menu provides access to features described in the following sections:

- *ACL Wizard*
- *MAC ACL*
- *MAC Rules*
- *MAC Binding Configuration*
- *MAC Binding Table*
- *IP ACL*
- *IP Rules*
- *IP Extended Rules*
- *IPv6 ACL*
- *IPv6 Rules*
- *IP Binding Configuration*
- *IP Binding Table*

## ACL Wizard

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 the rule can be applied to this ACL on the selected ports. The ACL Wizard enables you to create the ACL, but does not allow you to modify it. For more information about how to modify the ACL, see the instructions on the ACL configuration screen.

### ➤ To create an ACL:

1. Select **Security > ACL > ACL Wizard**.
2. From the ACL Type list, select the ACL type used to create the ACL.

You can select from the following optional types:

- **ACL Based on Destination MAC.** Creates an ACL based on the destination MAC address, destination MAC mask, and VLAN.
- **ACL Based on Source MAC.** Creates an ACL based on the source MAC address, source MAC mask, and VLAN.
- **ACL Based on Destination IPv4.** Creates an ACL based on the destination IPv4 address and IPv4 address mask.
- **ACL Based on Source IPv4.** Creates an ACL based on the source IPv4 address and IPv4 address mask.

- **ACL Based on Destination IPv6.** Creates an ACL based on the destination IPv6 prefix and IPv6 prefix length.
  - **ACL Based on Source IPv6.** Creates an ACL based on the source IPv6 prefix and IPv6 prefix length.
  - **ACL Based on Destination IPv4 L4 Port.** Creates an ACL based on the destination IPv4 layer 4 port number.
  - **ACL Based on Source IPv4 L4 Port.** Creates an ACL based on the source IPv4 layer 4 port number.
  - **ACL Based on Destination IPv6 L4 Port.** Creates an ACL based on the destination IPv6 layer 4 port number.
  - **ACL Based on Source IPv6 L4 Port.** Creates an ACL based on the source IPv6 layer 4 port number.
3. Configure the settings in the following table, based on the selection in the ACL Type list:

---

**Note:** The Rule ID, Action, and Match Every fields appear for all ACL types.  
The remaining two fields vary according to the selected ACL type.

---

- In the **Rule ID** field, enter a number that is used to identify the rule. The valid range is 1 - 50.
- In the **Action** field, specify what action must be taken if a packet matches the rule's criteria. The choices are Permit or Deny.
- In the **Match Every** field, specify Enable or Disable.
- In the remaining two fields, specify data according to the table below.

The following table describes the fields on this page: .

ACL Based on	Fields
Destination MAC	<ul style="list-style-type: none"> <li>• <b>Destination MAC.</b> 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.</li> <li>• <b>Destination MAC Mask.</b> 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.</li> </ul>
Source MAC	<ul style="list-style-type: none"> <li>• <b>Source MAC.</b> Specify the source MAC address to compare against an ethernet frame. The valid format is (xx:xx:xx:xx:xx:xx).</li> <li>• <b>Source MAC Mask.</b> 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).</li> </ul>
Destination IPv4	<ul style="list-style-type: none"> <li>• <b>Destination IP Address.</b> Specify the destination IP address.</li> <li>• <b>Destination IP Mask.</b> Specify the destination IP address mask.</li> </ul>
Source IPv4	<ul style="list-style-type: none"> <li>• <b>Source IP Address.</b> Specify the source IP address.</li> <li>• <b>Source IP Mask.</b> Specify the source IP address mask.</li> </ul>
Destination IPv6	<ul style="list-style-type: none"> <li>• <b>Destination Prefix.</b> Specify the destination prefix.</li> <li>• <b>Destination Prefix Length.</b> Specify the destination prefix length.</li> </ul>
Source IPv6	<ul style="list-style-type: none"> <li>• <b>Source Prefix.</b> Specify the source destination prefix.</li> <li>• <b>Source Prefix Length.</b> Specify the source prefix length.</li> </ul>
Destination IPv4 L4 Port	<ul style="list-style-type: none"> <li>• <b>Destination L4 port (protocol).</b> Specify the destination IPv4 L4 port protocol.</li> <li>• <b>Destination L4 port (value).</b> Specify the destination IPv4 L4 port value.</li> </ul>
Source IPv4 L4 Port	<ul style="list-style-type: none"> <li>• <b>Source L4 port (protocol).</b> Specify the source IPv4 L4 port protocol.</li> <li>• <b>Source L4 port (value).</b> Specify the source IPv4 L4 port value.</li> </ul>
Destination IPv6 L4 Port	<ul style="list-style-type: none"> <li>• <b>Destination L4 port (protocol).</b> Specify the destination IPv6 L4 port protocol.</li> <li>• <b>Destination L4 port (value).</b> Specify the destination IPv6 L4 port value.</li> </ul>
Source IPv6 L4 Port	<ul style="list-style-type: none"> <li>• <b>Source L4 port (protocol).</b> Specify the source IPv6 L4 port protocol.</li> <li>• <b>Source L4 port (value).</b> Specify the source IPv6 L4 port value.</li> </ul>

4. In the Binding Configuration area, the Inbound only packet filtering direction for an ACL is selected in the **Direction** field.
5. In the Port Selection Table area, displays the list of all available, valid interfaces for ACL mapping.

All physical interfaces and interfaces participating in the LAG are listed.

To apply the ACL to a selected interface, check the boxes beneath the required interfaces and then click **Add**. Update the switch with the new settings. Configuration changes take effect immediately.

- To apply the ACL to additional interfaces, selected the required ACL and add ports by clicking the box under the interface number. Click **Apply** to update the switch with the new settings.

Configuration changes take effect immediately.

## MAC ACL

A MAC ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (permit or deny) is taken and the additional rules are not checked for a match.

The steps for defining a MAC ACL and applying it to the switch are described in the following sections:

- Use the *MAC ACL* screen to create the ACL ID.
- Use the *MAC Rules* screen to create rules for the ACL.
- Use the *MAC Binding Configuration* screen to assign the ACL by its ID number to a port.
- Optionally, use the *MAC Binding Table* screen to view the configurations.

### ➤ To configure a MAC ACL:

- Select **Security > ACL > Basic > MAC ACL**.
- Specify a name for the MAC ACL in the **Name** field. The name string can include alphabetic, numeric, hyphen, underscore, or space characters only. The name must start with an alphabetic character.
- Click **Add**.

Each configured ACL displays the following information:

- Rules.** Displays the number of rules currently configured for the MAC ACL.
- Direction.** Displays the direction of packet traffic affected by the MAC ACL, which can be Inbound or blank.

To change the name of a MAC ACL, select the check box next to the Name field, update the name, then click **Apply**.

## 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.

### ➤ To configure MAC ACL rules:

- Select **Security > ACL > Basic > MAC Rules**.
- From the **ACL Name** field, specify the existing MAC ACL to which the rule applies.

For information about how to set up a new MAC ACL, use the *MAC ACL* screen.

3. In the **ID** field, enter an ID for the rule.

The valid range is 1-50.

4. Configure the following settings:

- **Action.** Specify what action must 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.
- **Match Every.** Requires a packet to match the criteria of this ACL. Select **Enable** or **Disable**. 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 0s in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a 0 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 list. 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 list. The value you enter specifies a customized EtherType to compare against an Ethernet frame. The valid range is 0x0600–0xFFFF.
- **Source MAC.** Requires a packet's source 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.
- **Source MAC Mask.** If desired, enter the MAC mask for the source MAC address to match. Use Fs and 0s in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a 0 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.** Enables or disables logging of access list (ACL) deny events.

5. Click **Add**.

To change a rule, select the check box associated with the rule, change the desired fields, and click **Apply**.

## 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 **ACL ID** list, select an existing MAC ACL.

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 you do not specify the sequence number, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1–2147483647.

4. Click the appropriate bar 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 ? appears in the box.
  - To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. An ? in the box indicates that the ACL is applied to the interface.
5. Click **Apply** to update the switch with the new settings.

The above fields are displayed in the **Interface Binding Status** block for each interface. In addition, the **ACL Type** (MAC, IPv4 or IPv6) is displayed.

## MAC Binding Table

### ➤ To view or delete the MAC ACL bindings.

1. Select **Security > ACL > Basic > MAC Binding Table**.

The following table describes the information displayed in the MAC Binding Table screen.

Field	Description
Interface	The interface to which the MAC ACL is bound.
Direction	The packet filtering direction for the 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 the selected interface and direction.
ACL ID	The ACL name identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

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

## 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, 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:

- Select **Security > ACL > Advanced > IP ACL**.
- In the **IP ACL ID** field, specify the ACL ID. The ID is an integer in one of the following ranges:
  - 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.

Each configured ACL displays the following information:

- Rules**. Displays the number of rules currently configured for the IP ACL.
  - Type**. Identifies the ACL as either a standard or extended IP ACL.
- Click **Add**.

To change the name of an IP ACL, select the check box next to the IP ACL ID field, update the name, then click **Apply**.

## 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 rule means that if an ACL is applied to a packet and if none of the explicit rules match, the final implicit “deny all” rule applies and the packet is dropped.

---

➤ **To configure IP rules, select the following:**

1. Select **Security > ACL > Advanced > IP Rules**.
2. From the ACL ID field, select the IP ACL for which to create or update a rule.  
The valid range is 1–99.
3. Configure the following fields:
  - **Rule ID.** Specify a number from 1 to 50 to identify the IP ACL rule. You can create up to 50 rules for each ACL.
  - **Action.** Select an ACL forwarding action:
    - **Permit.** Forwards packets which meet the ACL criteria.
    - **Deny.** Drops packets which meet the ACL criteria.
  - **Logging.** When set to Enable, logging is enabled for this ACL rule (subject to resource availability in the device). If the access list trap flag is also enabled, this 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 0 for the current interval. This field is available for a deny action.
  - **Match Every.** Requires a packet to match the criteria of this ACL. Select Enable or Disable. Match Every is exclusive to the other filtering rules, so if Match Every is enabled, the other rules on the screen are not available.
  - **Source IP Address.** Requires a packet’s source IP address to match the address listed here. Enter an IP address using dotted-decimal notation. The address you enter is compared to a packet’s source IP address.
  - **Source IP Mask.** Specifies the source IP address wildcard mask. Wildcard masks determine which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard mask 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.

4. Click **Add**.  
Configuration changes take effect immediately.

To update an IP ACL rule, select the check box associated with the rule, update the desired fields, and click **Apply**. You cannot modify the Rule ID of an existing IP rule.

## 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 rule means that if an ACL is applied to a packet and if none of the explicit rules match, the final implicit “deny all” rule applies and the packet is dropped.

---

### ➤ To configure rules for an IP ACL:

1. Click **Security > ACL > Advanced > IP Extended Rules**.
2. Select the ACL ID to add the rule to, and select the check box in the Extended ACL Rule table.
3. Configure the fields for the new rule.
  - **Rule ID.** Specify a number from 1 to 50 to identify the IP ACL rule. You can create up to 50 rules for each ACL.
  - **Action.** Select an ACL forwarding action:
    - **Permit.** Forwards packets which meet the ACL criteria.
    - **Deny.** Drops packets which meet the ACL criteria.
  - **Logging.** When set to Enable, logging is enabled for this ACL rule (subject to resource availability in the device). If the access list trap flag is also enabled, this 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 0 for the current interval. This field is available for a deny action.
  - **Match Every.** Requires a packet to match the criteria of this ACL. Select Enable or Disable. Match Every is exclusive to the other filtering rules, so if Match Every is enabled, the other rules on the screen are not available.
  - **Protocol Type.** Requires a packet’s protocol to match the protocol listed here. Select a type from the drop-down list, or enter the protocol number in the available field.

- **Source IP Address.** Requires a packet's source IP address to match the address listed here. Enter an IP address using dotted-decimal notation. The address you enter is compared to a packet's source IP address.
  - **Source IP Mask.** Specifies the source IP address wildcard mask. Wildcard masks determine which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard mask 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.
  - **Source L4 Port.** Requires a packet's TCP/UDP source port to match the port listed here. Complete one of the following fields:
    - **Source L4 Keyword:** Select the desired L4 keyword from the 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.
  - **Destination IP Address.** Requires a packet's destination port IP address to match the address listed here. Enter an IP address using dotted-decimal notation. The address you enter is compared to a packet's destination IP address.
  - **Destination IP Mask.** Specifies the destination IP address wildcard mask. Wildcard masks determine which bits are used and which bits are ignored. A wildcard 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.
  - **Destination L4 Port.** Requires 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 the 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 6 bits of the service type octet in the IP header. Select an IP DSCP value from the list. To specify a numeric value in the available field, select Other from the list and type an integer from 0 to 63 in the field.
4. Click **Add**.

To modify an existing IP Extended ACL rule, click in the Rule ID field. The number is a hyperlink to the Extended ACL Rule Configuration screen. If you modify the rule, click **Apply** to submit the changes to the switch.

## IPv6 ACL

An IPv6 ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (permit or deny) is taken, and the additional rules are not checked for a match. On this screen, the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or outbound traffic.

### ➤ To add an IPv6 ACL:

1. Select **Security > ACL**, then click the **Advanced > IPv6 ACL** link.
2. In the **IPv6 ACL** field, configure the name of IPv6 ACL.
  - The number of the rules associated with the IP ACL is displayed in the **Rules** field.
  - The ACL type is IPv6 ACL and is displayed in the **Type** field.
3. Click **Add**.

To delete an IPv6 ACL, select the check box associated with the rule and click **Delete**.

## 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 ACL screen. By default, no specific value is in effect for any of the IPv6 ACL rules.

### ➤ To add an IPv6 rule:

1. Select **Security > ACL > Advanced > IPv6 Rules** link.
2. From the pull-down list in the **ACL Name** field, select the IP ACL for which to create or update a rule.
3. Configure the settings for the new rule.
  - **Rule ID.** Enter a whole number in the range of 1–50 that is used to identify the rule. An IPv6 ACL might have up to 50 rules.
  - **Action.** Specify what action must be taken if a packet matches the rule's criteria. The choices are Permit or Deny.
  - **Logging.** When set to Enable, logging is enabled for this ACL rule (subject to resource availability in the device). If the access list trap flag is also enabled, this 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 0 for the current interval. This field is visible for a deny action.
  - **Match Every.** Select Enable or Disable. Enable signifies that all packets that match the selected IPv6 ACL and rule are either permitted or denied. In this case, since all

packets match the rule, the option of configuring other match criteria is not offered. To configure specific match criteria for the rule, remove the rule and recreate it, or for Match Every select Disable for the other match criteria to be visible.

- **Protocol.** There are two ways to configure IPv6 protocol:
    - After selecting protocol keyword **other**, specify an integer ranging from 0 to 255. This number represents the IPv6 protocol.
    - Select name of a protocol from the existing list of IPv6, ICMPv6, TCP, and UDP.
  - **Source Prefix and Source Prefix Length.** Specify the IPv6 Prefix combined with IPv6 Prefix length of the network or host from which the packet is being sent. The valid range for the prefix length is 0–128.
  - **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 list, and specify the number of the port. The valid range is 0 - 65535.
    - Select one of the keywords 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 a port range.
  - **Destination Prefix and Destination Prefix Length.** Enter a prefix of up to 128 bit combined with prefix length to be compared to a packet's destination IP address as a match criteria for the selected IPv6 ACL rule. The valid range for a prefix length is 0 - 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 list, and specify the number of the port. The valid range is 0 - 65535.
    - Select one of the keywords 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 a port range.
  - **IPv6 DSCP Service.** Select the IPv6 DSCP service. If you prefer, you can select the **Other** option in the drop-down list and enter the numeric value of the DSCP in the adjacent field. The DSCP is defined as the high-order 6 bits of the service type octet in the IPv6 header. This configuration is optional. Enter an integer from 0 to 63.
4. To add an IPv6 rule, select the global check box and click **Add**.

Click **Apply** to submit the changes to the switch.  
Configuration changes take effect immediately.

## 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 configure IP ACL interface bindings:**

1. Select **Security > ACL > Advanced > IP Binding Configuration**.
2. Select an existing IP ACL from the **ACL ID** menu.

The packet filtering **Direction** for ACL is Inbound, which means the IP ACL rules are applied to traffic entering the port.

3. 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, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1–2147483647.

4. Click the appropriate bar to display the available ports or LAGs.
  - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that an ? appears in the box.
  - To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. An ? in the box indicates that the ACL is applied to the interface.
5. Click **Apply** to save any changes to the running configuration.

## IP Binding Table

Use the IP Binding Table screen to view or delete the IP ACL bindings.

➤ **To display the IP Binding Table:**

Click **Security > ACL > Advanced > IP Binding Table**.

The following table describes the information displayed in the IP Binding Table..

Field	Description
Interface	The interface to which the IP ACL is bound.
Direction	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 the selected interface and direction. IP and IPv6 appear together.
ACL ID	Displays the ACL number identifying the ACL assigned to the selected interface and direction.
Sequence Number	Displays the sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.



# 7 Monitoring

---

# 7

Use the features available from the Monitoring tab to view various information about the switch and its ports and to configure how the switch monitors events. The Monitoring tab contains menus that provide access to the following features:

- *Ports*
- *Logs*
- *Port Mirroring*
- *System Resources Utilization*

## Ports

The screens available from the Ports menu contain various information about the number and type of traffic transmitted from and received on the switch. From the Ports menu, you can access the following sections:

- *Switch Statistics*
- *Port Statistics*
- *Port Detailed Statistics*
- *EAP Statistics*
- *Cable Test*

### Switch Statistics

The Switch Statistics screen displays detailed statistical information about the traffic the switch handles.

#### ➤ To display switch statistics:

Select **Monitoring > Ports > Switch Statistics**.

The following fields are displayed:

- **ifIndex**. The ifIndex of the interface table entry associated with the processor of this switch. The only available option is CPU, which displays traffic related to the CPU.
- **Octets Received**. The total number of octets of data received by the processor (excluding framing bits, but including FCS octets).
- **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.
- **Octets Transmitted**. The total number of octets transmitted out of the interface, including framing characters.
- **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.

- **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.
- **Static VLAN Entries.** The number of presently active VLAN entries on the switch that have been created statically.

## Port Statistics

The Port Statistics screen displays a summary of per-port traffic statistics on the switch.

### ➤ To display a summary of per-port traffic statistics and clear or refresh the counters:

1. Select **Monitoring > Ports > Port Statistics**.

The following fields are displayed:

- **Interface.** 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 were not transmitted because of errors.
  - **Collision Frames.** The best estimate of the total number of collisions on this Ethernet segment.
2. Click either **PORTS**, **LAGS** or **All** to display statistics for a specific type of interface or for all interfaces.
  3. Use the buttons at the top of the screen to perform the following actions on either ports, LAGs or both:
    - To clear all the counters for all interfaces on the switch, select the check box in the row heading and click **Clear**. The button sets all statistics for all ports to 0.
    - To clear the counters for a specific interfaces, select the check box associated with the port and click **Clear**. You can also enter the interface name in the **Go To Interface** field and click **GO**. This selects the interface and clears its counters.

## Port Detailed Statistics

The Port Detailed Statistics screen displays a variety of per-port traffic statistics.

➤ **To display a summary of per-port traffic statistics and clear or refresh the counters:**

1. Select **Monitoring > Ports > Port Detailed Statistics**.
2. Select the **Interface** for which data is to be displayed.
3. Select the **MST ID** for which statistics are displayed.

The following fields are displayed for the selected interface in the selected MST instance:

- **ifIndex.** 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 more information about port mirroring and probe ports, see *Port Mirroring* on page 160.
  - **Probe.** Indicates that the port has been configured as a monitoring port and is the destination port in a port mirroring session. For more information about port mirroring and probe ports, see *Port Mirroring* on page 160.
  - **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 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 can 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.** Spanning Tree Protocol is enabled for this port.
  - **Disable.** Spanning Tree Protocol is disabled for this port.
- **STP State.** The port 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 places 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.
- **LACP Mode.** The Link Aggregation Control Protocol administration state:

- **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.** The port speed and duplex mode. In autonegotiation mode, the duplex mode and speed are set from the autonegotiation process.
- **Physical Status.** The port speed and duplex mode status.
- **Link Status.** Indicates whether the port link is up or down.
- **Link Trap.** Determines whether to send a trap when link status changes. The factory default is Enable.
  - **Enable.** The system sends a trap when the link status changes.
  - **Disable.** The system does not send a trap when the link status changes.
- **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.
- **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 65 through 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 128 through 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 256 through 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 512 through 1023 octets in length inclusive (excluding framing bits but including FCS octets).
- **Packets Received > 1024 Octets.** The total number of packets received that were in excess of 1024 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
- **Total Packets Received Without Errors.** The total number of packets received that were without errors.
- **Unicast Packets Received.** The number of subnetwork-unicast packets delivered to a higher-layer protocol.
- **Multicast Packets Received.** The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
- **Broadcast Packets Received.** The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.

- **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 from the definition in IEEE 802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is 20–150 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 from 64 through 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 64 through 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 was not able to keep up with the inflow.
- **802.3x Pause Frames Received.** A count of MAC control frames received on this interface with an operation code indicating the pause operation. This counter does not increment when the interface is operating in half-duplex mode.
- **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.
- **Total Packets Transmitted Successfully.** The number of frames that have been transmitted by this port to its segment.
- **Unicast Packets Transmitted.** The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
- **Multicast Packets Transmitted.** The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
- **Broadcast Packets Transmitted.** The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
- **Total Transmit Errors.** The sum of single, multiple, and excessive collisions.
- **Tx FCS Errors.** The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of from 64 through 1518 octets, inclusive, but had a bad FCS with an integral number of octets.

- **Tx Oversized.** The total number of frames that exceeded the maximum permitted frame size. This counter has a maximum increment rate of 815 counts per second at 10 Mb/s.
- **Total Transmit Packets Discarded.** The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
- **Single Collision Frames.** The number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
- **Multiple Collision Frames.** The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
- **Excessive Collision Frames.** The number of frames for which transmission on a particular interface fails due to excessive collisions.
- **802.3x Pause Frames Transmitted.** The number of MAC control frames transmitted on this interface with an operation code indicating the pause operation. This counter does not increment when the interface is operating in half-duplex mode.
- **EAPOL Frames Received.** The number of valid EAPOL frames of any type received by this authenticator.
- **EAPOL Frames Transmitted.** The number of EAPOL frames of any type transmitted by this authenticator.

Use the buttons at the top of the screen to perform the following actions:

- Click **Clear** to clear all the counters. This resets all statistics for this port to 0.
- Click **Update** to display the most current statistics.

## EAP Statistics

Use the EAP Statistics screen to display information about EAP packets received on a specific port.

### ➤ To display a EAP Statistic:

1. Select **Monitoring > Ports > EAP Statistics**.
2. Select the interface for which data is to be displayed.

This can be done by either clicking the check box by the required port or by entering the port name in the **Go to Interface** field and clicking **Go**.

The following table describes the EAPOL and EAP statistics displayed.

- **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 top 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 **Clear**. The button resets all statistics for all ports to 0.
- To clear the counters for a specific port, select the check box associated with the port and click **Clear**.

## Cable Test

Use the Cable Test screen to display information about the cables connected to switch ports. The Cable test is effective for interfaces which are sync at 10Gbps speed.

### ➤ To display cable information:

1. Select **Monitoring > Ports > Cable Test**.
2. Select the interface for which cable data is to be displayed.

This can be done by either clicking the check box by the required port or by entering the port name in the **Go to Interface** field and clicking **Go**.

3. Click **Apply** to execute the test per port.

The following fields are displayed:

- **Cable Status:**
  - **Normal.** The cable is working correctly.
  - **Open Cable.** A cable is connected to the port, but it is not connected to the other side (no link). Open Cable status at close to 0M may indicate that no cable is inserted in the port.
  - **Short Cable.** There is an electrical short in the cable.
  - **Cable Test Failed.** The cable status was not able to be determined. The cable might in fact be working.

- **Untested.** The test has not been performed.
- **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. This is of rough accuracy (0–50m, 50–80m, 80–110m). **Not Supported** is displayed if the cable length was not 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 Cable, Short Cable, or No Cable.

## Logs

The switch might generate messages in response to 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 tab contains menus that provide access to the following features

- *Buffered Logs*
- *Flash Logs*
- *Server Log*
- *Trap Logs*

## Buffered Logs

The buffered log stores messages in RAM memory based on the settings for message component and severity. Use the Buffered Logs 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 Buffered Logs settings:

1. Select **Monitoring > Logs > Buffered Logs**.
2. In the **Admin Status** field select **Enable** to enable system logging or **Disable** to disable it. The factory default setting is Enable.
3. In the **Behavior** field, select the Wrap behavior of the log when it is full.  
In this behavior, when the buffer is full, the oldest log messages are deleted as the system logs new messages.
4. If you change the buffered logs settings, click **Apply** to apply the changes to the system and save them.

The **Total Number of Messages** field is displayed. This contains the number of messages the system has logged in memory. Only the 128 most recent entries are displayed.

The rest of the screen displays the buffered logs messages. Messages logged to a collector or relayed through syslog have the following format:

```
10 Oct 2012 14:17:43%AAA-I-DISCONNECT: http connection for user
admin, source 10.5.70.19 destination 10.5.234.201 TERMINATED
```

```
10 Oct 2012 13:52:00%AAA-I-CONNECT: New http connection for user
admin, source 10.5.70.19 destination 10.5.234.201 ACCEPTED
```

The syslog message includes the following fields:

- Date
- Time
- Module (AAA in the example above).
- Severity (I in the example above).
- Action (DISCONNECT in the example above).
- Description (http connection for user admin, source 10.5.70.19 destination 10.5.234.201 TERMINATED in the example above).

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

## Flash Logs

Flash logs are stored in the Flash and so are not lost when the device reboots.

### ➤ To configure the Flash Logs settings:

1. Select **Monitoring > Logs > Flash Logs**.
2. In the **Admin Status** field select **Enable** to enable system logging or **Disable** to disable it. The factory default setting is **Disable**.
3. In the **Severity Filter** field, select the level of severity of SYSLOGs that will be logged.
4. If you change the settings, click **Apply** to apply the changes to the system and save them.

The **Total Number of Messages** field is displayed. This contains the number of messages the system has logged in memory. Only the first 128 most recent entries are displayed.

The rest of the screen displays the flash logs messages. Messages logged to a collector or relayed through syslog have the following format:

```
214483269 13 Feb 2015 14:17:43%AAA-I-DISCONNECT: http connection
for user admin, source 10.5.70.19 destination 10.5.234.201
TERMINATED
```

```
214483270 10 Oct 2012 13:52:00%AAA-I-CONNECT: New http connection
for user admin, source 10.5.70.19 destination 10.5.234.201
ACCEPTED
```

The syslog message includes the following fields:

- **Log index** (214483269 in the example above)
- **Log Time** (13 Feb 2015 14:17:43 in the example above)
- **Description** (%AAA-W-REJECT: New console connection, source 0.0.0.0 destination 0.0.0.0 REJECTED, aggregated (in the example above).

## Server Log

Use the Server Log screen to allow the switch to send log messages to the remote logging hosts configured on the system. The SYSLOG message supports the SYSLOG header according to RFC 5424.

### ➤ To add a remote log server:

#### 1. Select **Monitoring > Logs > Server Log**.

Specify the following settings and click **Add**.

- **Host Address.** Specify the IP address or host name 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.** 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 level 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 must only be performed by qualified support personnel.

The **Status** field in the Server Log table shows whether the remote logging host is active.

To modify the settings for an existing host, select the check box next to the host, change the desired information, and click **Apply**.

## Trap Logs

Use the Trap Logs screen to view information about the SNMP traps generated on the switch.

➤ **To view SNMP traps:**

Select **Monitoring > Logs > Trap Logs**.

The **Number of Traps Since Last Reset** field is displayed.

---

**Note:** Check the detailed contents of the reported traps through the SNMP trap server. This action is not within the scope of this guide.

---

## Port Mirroring

The screen you access from the Mirroring menu enables 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.

You can mirror up to eight ports to a single destination port.

➤ **To configure port mirroring:**

1. Select **Monitoring > Port Mirroring**.
2. Select the check box next to a port to configure it as a source port, or enter its name in the **Go To Interface** field and click **Go**.
3. From the **Destination Port** list, select the port to which port traffic is to be copied. Use the xg1, xg2,... format to specify the port. You can configure only one destination port on the system.
4. From the **Session Mode** list, select the mode for port mirroring on the selected port:

- **Enable.** Multiple-port mirroring is active on the selected port (that is, on all the configured source ports).
  - **Disable.** Port mirroring is not active on the selected port, but the mirroring information is retained.
5. From the **Direction** list, select the direction of the traffic to be mirrored from the configured mirrored ports.

The default value is Tx and Rx.

- **Tx and Rx.** Enable both transmitting and receiving on the selected ports.
  - **Tx only.** Enable only transmitting on the selected ports.
  - **Rx only.** Enable only receiving on the selected ports.
6. Click **Apply** to apply the settings to the system.
- If the port is configured as a source port, the Mirroring Port field value is Mirrored.

## System Resources Utilization

The switch architecture uses a Ternary Content Addressable Memory (TCAM) to support packet actions in wire speed. TCAM holds the rules produced by other applications. The maximum number of TCAM rules that can be allocated by all applications on the device is 2048. This resource is used by the following features:

- DiffServe
- ACLs
- Dynamic VLAN Assignment (DVA)
- DHCP snooping

Some applications allocate rules upon their initiation. Additionally, processes that initialize during system boot allocate some of their rules during the startup process.

The System Resources Utilization screen displays the system resource utilization and maximum number of TCAM entries.

### ➤ To view TCAM utilization:

Select **Monitoring > System Resources Utilization**.

The following fields are displayed:

- **System Resources Utilization.** Percentage of TCAM utilization
- **Max System Resource Entries.** Maximum number of TCAM entries available
- **ACLs.** Number of TCAM entries used by ACLs
- **DiffServe.** Number of TCAM entries used by DiffServe
- **DVA.** Number of TCAM entries used by Dynamic VLAN Assignment (DVA)
- **DHCP Snooping.** Number of TCAM entries used by DHCP snooping



# Maintenance

---

# 8

Use the features available from the Maintenance tab to help you manage the switch. The Maintenance tab contains menus that provide access to the following features:

- *Reset*
- *Upload*
- *Download*
- *File Management*
- *Troubleshooting*

## Reset

The Reset menu contains links that provide access to the features described in the following sections:

- [Device Reboot](#)
- [Factory Default](#)

### Device Reboot

Use the Device Reboot screen to reboot the switch.

➤ **To reboot the switch:**

1. Select **Maintenance > Reset > Device Reboot**.

Select the check box.

2. Click **Apply**.

The switch resets immediately.

The management interface is not available until the switch completes the boot cycle. After the switch resets, the login screen appears.

### 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 lose network connectivity after you reset the switch to the factory defaults, see [Connect the Switch to the Network](#) on page 6.

---

➤ **To reset the switch to the factory default settings:**

1. Select **Maintenance > Reset > Factory Default**.
2. Select the check box.
3. Click **Apply**.

The switch resets immediately.

## Upload

The switch supports system file uploads from the switch to a remote system by using either TFTP or HTTP.

## Upload File Types

The following types of files can be uploaded from the switch:

- **Archive.** The archive is the system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy and the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process.
- **Text Configuration.** You can edit a text-based configuration 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 download a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name, IP address), and upload it to that device.
- **Flash Log.** The log entry file stored in the Flash.

The Upload menu contains links that provide access to the features described in the following sections:

- [TFTP File Upload](#)
- [HTTP File Upload](#)
- [USB File Upload](#)

## TFTP File Upload

Use the TFTP File Upload screen to upload configuration (ASCII), log (ASCII), and image (binary) files from the switch to a TFTP server on the network.

### ➤ To upload a file from the switch to the TFTP server:

1. Select **Maintenance > Upload > TFTP File Upload**. Use the File Type list to select the type of file you want to upload.

For more information, see [Upload File Types](#) on page 165.

- **Archive.** Retrieve the active software image file.
- **Text Configuration.** Retrieve the stored text configuration file.
- **Flash Logs.** Retrieve the flash log file.

The factory default is **Archive**.

2. From the **Server Address Type** field, select the format to use for the address you type in the Server Address field:
  - **IPv4.** The TFTP server address is an IP address in dotted-decimal format.
  - **DNS.** The TFTP server address is a host name.
3. 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.

4. 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 slash or 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.

5. In the **Transfer File Name** field, specify a destination file name for the file to upload.
6. You can enter up to 32 characters. The transfer fails if you do not specify a file name. For a code transfer, use the .ros file extension.
7. Select the **Start File Transfer** check box to enable the file upload when you click **Apply**
8. Click **Apply** to begin the file transfer (upload).

When the transfer actually begins, the bottom part of page **Transfer Status** displays information about the progress of the file transfer. The screen refreshes automatically until the file transfer completes or fails. Upon completion or failure of file transfer a relevant message will be displayed.

## HTTP File Upload

Use the HTTP File Upload screen to upload configuration text files from the switch to the management system by using an HTTP session (for example, through your web browser).

### ➤ To upload a file from the switch to another system by using HTTP:

1. Select **Maintenance > Upload > HTTP File Upload**.
2. The **File Type** list displays the type of file that can be uploaded, which is the Text Configuration file.
3. Click **Apply**.

Upon completion of file transfer a relevant message is displayed.

A window appears to allow you to open the text file on the management system in order to view or save it to the management system.

## USB File Upload

Use the USB File Upload screen to upload files of various types from the switch to a USB device connected to the USB port on the device front panel.

### ➤ To display the USB File Upload page:

1. click **Maintenance > Upload > USB File Upload**.
2. Use **File Type** to specify what type of file you want to upload:
  - **Archive**. Retrieve the active software image file.
  - **Text Configuration** Retrieve the stored text configuration file. The factory default is **Archive**.
3. Use **File Path** to enter the path to the destination path on USB to store file.

You can enter up to 32 characters. Include the slash or 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 USB directory.

4. Use **USB File** to give a name along with path for the file you want to upload. You may enter up to 32 characters. The transfer fails if you do not specify a file name.

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

## Download

The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.

### Download File Types

The following types of files can be downloaded to the switch:

- **Archive.** The archive is the system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy and the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process. The downloaded archive (software image) is downloaded to the non-active image on the switch.
- **Text Configuration.** You can edit a text-based configuration 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 upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name, IP address), and download it to that device.

The Download menu contains links that provide access to the features described in the following sections:

- [TFTP File Download](#)
- [HTTP File Download](#)
- [USB File Download](#)

### TFTP File Download

Use the TFTP Download File screen to download device software, and the configuration files from a TFTP server to the switch.

You can also download files through HTTP. See [HTTP File Download](#) on page 169 for more information.

Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.

➤ **To download a file to the switch from a TFTP server:**

1. Select **Maintenance > Download > TFTP File Download**.
2. From the File Type list, select the type of file you want to download to the switch. For more information, see *Download File Types* on page 167.
  - **Archive**. Software image file. The software image download also updates the device boot file, if such an update is available.

---

**Note:** The system always downloads the software image to the non-active image.

---

- **Text Configuration**. A text-based configuration file.

---

**Note:** The configuration is downloaded to the startup configuration, following which the device automatically reboots to this new configuration. A message indicating this behavior is displayed and must be confirmed.

---

3. From the **Server Address Type** field, select the format for the address you type in the TFTP Server Address field:
  - **IPv4**. The TFTP server address is an IP address in dotted-decimal format.
  - **DNS**. The TFTP server address is a host name.
4. In the **TFTP Server IP** 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 the file is located.  
You can enter up to 32 characters. Include the slash or backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to copy the file from the root TFTP directory.
6. In the **Remote File Name** field, select the name of the file to download from the TFTP server. The transfer fails if you do not specify a file name.  
You can enter up to 32 characters. A file name with a space is not accepted.
7. Select the **Start File Transfer** check box to enable the file upload when you click **Apply**.
8. Click **Apply** to initiate the file transfer.

When the transfer actually begins, the bottom part of page **Transfer Status** displays information about the progress of the file transfer. The screen refreshes automatically

until the file transfer completes or fails. Upon completion or failure of file transfer a message is displayed.

To activate a software image that you downloaded to the switch, see [File Management](#) on page 170.

## HTTP File Download

Use the HTTP File Download screen to download files of various types to the switch using an HTTP session (for example, via your web browser).

### ➤ To download a file to the switch from by using HTTP:

1. Select **Maintenance > Download > HTTP File Download**.
2. From the **File Type** list, select the type of file you want to download to the switch.

For more information, see [Download File Types](#) on page 167.

- **Archive.** Software image file.

---

**Note:** The system always downloads the software image to the non-active image.

---

- **Text Configuration.** A text-based configuration file.

---

**Note:** The configuration is downloaded to the startup configuration, following which the device automatically reboots to this new configuration. A message indicating this behavior is displayed and must be confirmed.

---

3. In the **Select File** field, enter the name of the file that you want to download or click **Choose File** to open a file upload window to locate the file.
4. Click the **Apply** button to initiate the file download.

---

**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.

---

## USB File Download

Use the USB File Upload screen to download a file to the switch from a USB device connected to the USB port on device front panel.

➤ **To display the USB File Download page**

1. click **Maintenance > Download > USB File Download**.
2. Use **File Type** to specify what type of file you want to download:
  - **Archive**. Software image file.
  - **Text Configuration**. A text-based configuration file. The factory default is **Archive**.

---

**Note:** The configuration is downloaded to the startup configuration, following which the device automatically reboots to this new configuration. A message indicating this behavior is displayed and must be confirmed.

---

3. Use **File Path** to enter the path to the destination path on USB where the file will be stored.
4. You can enter up to 32 characters. Include the slash or backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to copy the file from the root USB directory
5. Use **USB File** to give a name along with path for the file you want to download. You may enter up to 32 characters. The transfer fails if you do not specify a file name.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
8. **Transfer Status** displays the status of the file transfer to the switch. When the transfer actually begins, this block displays information about the progress of the file transfer. The screen refreshes automatically until the file transfer completes or fails. Upon completion or failure of file transfer, a message is displayed.

## 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.

The File Management menu contains links that provide access to the features described in the following sections:

- [Dual Image Configuration](#)
- [Dual Image Status](#)

### Dual Image Configuration

The system running a legacy software version ignores (does not load) a configuration file created by the 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.

Use the Dual Image Configuration screen to set the boot image, or configure an image description.

➤ **To configure Dual Image settings:**

1. Select **Maintenance > File Management > Dual Image > Dual Image Configuration**.
2. In the **Image Name** field, select one of the images from the list.  
The **Current-active** field displays the name of the active image.
3. To configure a descriptive name for the selected software image, type the name in the **Image Description** field.  
The valid range is 0–160 characters. The factory default is blank.
4. To set the selected image as the active image, select the **Activate Image** check box.

---

**Note:** After activating an image, you must perform a system reset of the switch to run the new code.

---

5. Click **Apply** to apply the settings to the switch.

## Dual Image Status

The Dual Image Status screen displays system images.

➤ **To display Dual Image settings:**

Select **Maintenance > File Management > Dual Image > Dual Image Status**.

The Dual Image Status screen displays the following:

- **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 unit.
- **Next-active.** The image used on the next restart of this unit.
- **Image1 Description.** The description associated with the image1 code file.
- **Image2 Description.** The description associated with the image2 code file.

## Troubleshooting

The Troubleshooting menu contains links that provide access to the features described in the following sections:

- [Ping IPv4](#)

- [Ping IPv6](#)
- [Traceroute IPv4](#)
- [Traceroute IPv6](#)
- [Tech Support Info](#)

## Ping IPv4

Use the Ping IPv4 screen to instruct the switch to send a ping request to a specified IPv4 address. You can use this feature to check whether the switch can communicate with a particular network host.

Subnet broadcast ping and loopback ping is not supported. The device cannot ping the special broadcast address 255.255.255.255, the local network broadcast address, or a reachable network broadcast address.

### ➤ To configure the settings and ping a host on the network:

1. Select **Maintenance > Troubleshooting > Ping IPv4**.
2. In the **IP Address/Host Name** field, specify the IP address or the host name of the station you want the switch to ping.

The initial value is blank. This information is not retained across a power cycle. The maximum number of characters in a name is 160.

3. Optionally, configure the following settings:
  - In the **Count** field, specify the number of pings to send. The valid range is 1–15.
  - In the **Interval (secs)** field, specify the number of seconds between pings sent. The valid range is 1–60.
  - In the **Size** field, specify the size of the ping (ICMP) packet data to send. The valid range is 0–65000.
  - The **Results** field displays the result after the switch sends a ping request to the specified address.
4. Click **Apply** to send the ping. The switch sends the number of pings specified in the Count field, and the results are displayed in the Results field.
  - If a reply to the ping is received, 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, the message: “Tx = 1, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec” is displayed.

## Ping IPv6

Use the Ping IPv6 screen to send a ping request to a specified host name or IPv6 address. This checks whether the switch can communicate with a particular IPv6 station. When you click **Apply**, the switch sends three pings, and the results are displayed.

➤ **To configure the settings and ping a host on the network:**

1. Select **Maintenance > Troubleshooting > Ping IPv6**.
2. In the **Ping** field, select either **Global** or **Link Local** to select either the global IPv6 Address or host name or link local address to ping.  
if **Link Local** is selected, select the outgoing VLAN interface for ping.
3. Configure the following settings:
  - In the **IPv6 Address/Host Name** field, enter the IPv6 address or host name of the station you want the switch to ping. The initial value is blank. The IPv6 address or host name you enter is not retained across a power cycle. The valid range is 0–160 characters.
  - In the **Datagram Size** field, enter the datagram size of the ping packets. The valid range is 48–2048.
  - The **Result** field displays the result after the switch sends a ping IPv6 request to the specified IPv6 address.
4. Click **Apply** to send the ping.

The switch sends the number of pings specified in the Count field, and the results are displayed in the Results field.

- If a reply to the ping is received, you see “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 message is displayed (with sample numbers): Send count = 3, Receive count = 0 from IP/HOST Average round trip time = 680 ms.

## Traceroute IPv4

Use the Traceroute utility to discover the paths that a packet takes to a remote destination.

➤ **To configure the Traceroute settings and send probe packets to discover the route to a host on the network:**

1. Select **Maintenance > Troubleshooting > Traceroute IPv4**.
2. In the **IP Address/Hostname** field, specify the IPv4 address or the host name of the station you want the switch to ping.  
The initial value is blank. This information is not retained across a power cycle.
3. Configure the following settings:
  - **Probes Per Hop**. Specify the number of times each hop must be probed. The valid range is 1–10. The default value is 3.
  - **MaxTTL**. Specify the maximum time-to-live for a packet in number of hops. The valid range is 1–255. The default value is 30.
  - **InitTTL**. Specify the initial time-to-live for a packet in number of hops. The valid range is 1–255. The default value is 1. The InitTTL you enter is not retained across a power cycle.

- **MaxFail.** Specify the maximum number of failures allowed in the session. The default value is 5. The range is 0 to 255. The MaxFail you enter is not retained across a power cycle.
  - **Interval (secs).** Specify the time between probes in seconds. The default value is 3. The range is 1 to 60. The Interval you enter is not retained across a power cycle.
  - **Port.** Specify the UDP destination port in probe packets. The default value is 33434. The range is 1- 65535. The port you enter is not retained across a power cycle.
  - **Size.** Specify the size of probe packets. The default value is 0. The range is 64 to 1472. The Size you enter is not retained across a power cycle.
4. Click **Apply** to initiate the traceroute. The results display in the Results field.

## Traceroute IPv6

Use this screen to tell the switch to send a TraceRoute request to a specified IPv6 address or Hostname. You can use this to discover the paths packets take to a remote destination. Once you click the **Apply** button, the switch will send a traceroute and the results will be displayed below the configurable data.

If a reply to the traceroute is received, the following is a sample of what may be displayed.

```
1 10.5.225.33 20 ms 10 ms 30 ms
2 10.5.225.225 10 ms 10 ms 10 ms
3 192.254.254.3 10 ms 30 ms 20 ms
Hop Count = 3 Test attempt = 9 Test Success = 3
```

### ➤ To display the Traceroute IPv6 page.

1. Click **Maintenance > Troubleshooting > Traceroute IPv6**.
2. Use **IPv6 Address/Hostname** to enter the IPv6 address or hostname of the station you want the switch to discover path. The initial value is blank. The IPv6 address must be a Global one. The IPv6 Address or Hostname you enter is not retained across a power cycle.
3. Configure the following settings:
  - **Probes Per Hop.** Specify the number of times each hop must be probed. The valid range is 1–10. The default value is 3.
  - **MaxTTL.** Specify the maximum time-to-live for a packet in number of hops. The valid range is 1–255. The default value is 30.
  - **InitTTL.** Specify the initial time-to-live for a packet in number of hops. The valid range is 1–255. The default value is 1. The InitTTL you enter is not retained across a power cycle.
  - **MaxFail.** Specify the maximum number of failures allowed in the session. The default value is 5. The range is 0 to 255. The MaxFail you enter is not retained across a power cycle.
  - **Interval (secs).** Specify the time between probes in seconds. The default value is 3. The range is 1 to 60. The Interval you enter is not retained across a power cycle.
  - **Port.** Specify the UDP destination port in probe packets. The default value is 33434. The range is 1- 65535. The port you enter is not retained across a power cycle.

- **Size.** Specify the size of probe packets. The default value is 0. The range is 64 to 1472. The Size you enter is not retained across a power cycle.

The results of the trace after the switch sends a traceroute request to the specified IPv6 address or hostname is displayed in the Results field.

4. Click **Apply** to initiate the traceroute. The results display in the Results area.

## Tech Support Info

### ➤ To view technical support information:

1. Select **Maintenance > Troubleshooting > Tech Support Info**.
2. Click **Generate Request** to display the technical support information that is uploaded from the device and displayed in the text window. You can then mark this text and copy it to a local text file on the PC.

The technical support information consists of a list of multiple show commands to provide a broad view of the device configuration status, as well as protocol-level status. This is usually used for debug purposes, where multiple configuration and information items are required. Device information can be gathered with one operation and provided to support engineers



## 9 Help

---

# 9

Use the features available from the Help tab to connect to online resources for assistance, and to register your device.

## Online Help

The Online Help link provides links to the sections described in the following sections:

- [Support](#)
- [User Guide](#)

## Support

Use the Support screen to connect to the online support site at netgear.com.

➤ **To connect to online support:**

1. Select **Help > Online Help > Support**.
2. Click **Apply** to connect to the NETGEAR support site for the switch.

## User Guide

Use the User Guide screen to access this guide, which is available on the NETGEAR website.

➤ **To access the user guide:**

1. Select **Help > Online Help > User Guide**.
2. To access the user guide that is available on line, click **Apply**.

## Registration

Use the Registration screen to register your switch. Completing the registration confirms your email address, lowers technical support resolution time, and ensures your shipping address accuracy. NETGEAR makes an effort to incorporate your feedback into future product development.

For the product registration process to proceed, the administrative system running the browser must meet the following requirements:

- The administrative system must have Internet access.
- The browser must allow pop-up windows.
- If the browser is Internet Explorer, ActiveX must be enabled.

If you have not registered the product or have not disabled the registration reminders, the pop-up window displays each time you successfully log on to the switch.

It includes the following buttons:

- **TURN OFF.** Use this button to turn off the product registration feature and to prevent the registration reminder pop-up window from appearing on subsequent successful login sessions.

- **REMIND ME LATER.** The pop-up window closes and no action is taken, and the registration reminder pop-up appears on next successful login.
- **REGISTER NOW.** The NETGEAR registration server is contacted to initiate the registration process.

---

**Note:** NETGEAR will never sell or rent your email address, and you can opt out of communications at any time.

---

➤ **To register the switch:**

Select **Help > Registration**. Click **REGISTER** to register the switch.

The switch attempts to contact the NETGEAR registration server. If the switch successfully contacts the registration server, the NETGEAR product registration screen opens in a new browser window. The product serial number and model number fields are pre-populated. After you provide some basic information and click **REGISTER**, the registration process is complete.



# Hardware Specifications and Default Values

---

# 10

The XS728T switches conform to the TCP/IP, UDP, HTTP, ICMP, TFTP, DHCP, IEEE 802.1D, IEEE 802.1 p, and IEEE 802.1Q standards.

They also conform to the IEEE802.3 1000Base-T and 10GBase-T and IEEE802.3az (EEE) standards.

Feature	Value
Interfaces	28 1000/10000 Mbps switching ports: <ul style="list-style-type: none"><li>• Ports xg1-xg24 are copper ports (RJ45).</li><li>• Ports xg25-xg28 are fiber ports (SFP+).</li></ul>
Flash memory size	256 MB NAND
SDRAM size and type	512 MB DDR3
Switching capacity	Non blocking full wire speed on all packet sizes
Forwarding method	Store and forward
Packet forwarding rate	1G: 1,488,000 pps 10G: 14,880,000 pps
MAC addresses	16 K
Green Ethernet	Automatic power-down on port when link is down, short cable mode and EEE mode

## Switch Features and Defaults

Feature	Sets Supported	Default
Auto negotiation/static speed/duplex	All ports	Auto-negotiation
Auto MDI/MDIX	N/A	Enabled
802.3x flow control/back pressure	1 (per system)	Disabled
Port mirroring	1 destination port and 8 source ports	Disabled
Port trunking (aggregation)	8	Pre-configured
802.1D spanning tree	1	Disabled
802.1w RSTP	1	Enabled
802.1s spanning tree	16 instances	Disabled
Static 802.1Q tagging	512	Default VLAN ID = 1
Learning process	Supports static and dynamic MAC entries	Dynamic learning is enabled by default
Storm control per each packet type (unicast, broadcast, multicast)	All ports	Disabled
Jumbo frame	All ports	Enabled. Max.= 10 KB
Number of queues	8	N/A
Port based	N/A	N/A
802.1p	1	Enabled
DSCP	1	Disabled
Rate limiting	All ports	Disabled
Auto-QoS	All ports	Disabled
802.1x	All ports	Disabled
MAC ACL	164 (shared with IP and IPv6 ACLs)	All MAC addresses allowed
IP ACL	164 (shared with MAC and IPv6 ACLs)	All IP addresses allowed
IPv6 ACL	164 (shared with IP ACL and MAC ACL)	All IP addresses allowed

## XS728T ProSAFE 28-Port 10-Gigabit L2+ Smart Switch

Feature	Sets Supported	Default
Password control access	1	Idle time-out = 10 minutes 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
Boot code update	Boot code is automatically updated together with firmware upgrade.	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
Factory default reset	1 (web and front-panel button)	N/A
Dual image support	1	Enabled
Multi-session web connections	5	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	4 (buffered flash, server & traps)	Buffer Log enabled
MIB Support	1	Enabled
Smart Control Center	N/A	Enabled
Statistics	N/A	N/A
IGMP snooping v1/v2/v3	All VLANs	Disabled
IGMP Snooping Querier	All VLANs	Disabled
Configurations upload/download	1	N/A
EAPoL flooding	All ports	Disabled
BPDU flooding	All ports	Disabled
Multicast groups	512	Disabled
Filter Multicast control	1	Disabled
Number of static routes	64 for IPv4 and IPv6, respectively	N/A

## XS728T ProSAFE 28-Port 10-Gigabit L2+ Smart Switch

Feature	Sets Supported	Default
Number of routed VLANs	32 for IPv4 and IPv6, respectively	N/A
Number of ARP cache entries	1024	N/A
Number of DHCP snooping bindings	1024	N/A
Number of DHCP static entries	1024	N/A
MLD snooping v1/v2	All VLANs	Disabled
MLD Snooping Querier	All VLANs	Disabled
Private VLAN	Primary, Community and Isolated	Disabled
GVRP	All ports	Disabled
Protocol and MAC based VLAN	1	Disabled
OUI based Voice VLAN	All ports	Disabled
Auto-VOIP	All ports	Disabled
IP MTU settings	Up to 9000. Globally Per IPv4 and Ipv6	1500
USB port & USB flash device	1	NA

# Configuration Examples

---

# 11

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

- *Virtual Local Area Networks (VLANs)*
- *Access Control Lists (ACLs)*
- *Differentiated Services (DiffServ)*
- *802.1x*
- *MSTP*
- *Configure VLAN Routing with Static Route*

## Virtual Local Area Networks (VLANs)

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic must go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of computers, 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 who communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID tag number. Each port has a default VLAN ID setting that is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed in the Port PVID Configuration screen. See [Port PVID Configuration](#) on page 55.
- When a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID setting. The packet proceeds to the VLAN specified by its VLAN ID tag number.
- If the port through which the packet entered does not have membership with the VLAN specified by the VLAN ID tag, the packet is dropped.
- If the port is a member of the VLAN specified by the packet's VLAN ID, the packet can be sent to other ports with the same VLAN ID.

- Packets leaving the switch are either tagged or untagged, depending on the setting for that port's VLAN membership properties. A U for a given port means that packets leaving the switch from that port are untagged. Inversely, a T for a given port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

The example given in this section describes a wide range of configurations to help provide an understanding of tagged VLANs.

## Sample VLAN Configuration

This example demonstrates several scenarios of VLAN use and describes how the switch handles tagged and untagged traffic.

In this example, you create two new VLANs, change the port membership for default VLAN 1, and assign port members to the two new VLANs:

1. In the VLAN Configuration screen (see [VLAN Configuration](#) on page 53), create the following VLANs:
  - A VLAN with VLAN ID 10
  - A VLAN with VLAN ID 20
2. In the VLAN Membership screen (see [VLAN Membership](#) on page 54), specify the VLAN membership as follows:
  - For the VLAN with VLAN ID 10, specify the following members: port 1 (U), port 2 (U), and port 3 (T).
  - For the VLAN with VLAN ID 20, specify the following members: port 4 (U), port 5 (T), and port 6 (U).
3. In the Port PVID Configuration screen (see [Port PVID Configuration](#) on page 55), specify the PVID for ports xg1 and xg4 so that packets entering these ports are tagged with the port VLAN ID:
  - **Port xg1.** PVID 10
  - **Port xg4.** PVID 20
4. This VLAN configuration produces the following results:
  - If an untagged packet enters port 1, the switch tags it with VLAN ID 10. The packet has access to port 2 and port 3. The outgoing packet is stripped of its tag to leave port 2 as an untagged packet. For port 3, the outgoing packet leaves as a tagged packet with VLAN ID 10.
  - If a tagged packet with VLAN ID 10 enters port 3, the packet has access to port 1 and port 2. If the packet leaves port 1 or port 2, it is stripped of its tag to leave the switch as an untagged packet.
  - If an untagged packet enters port 4, the switch tags it with VLAN ID 20. The packet has access to port 5 and port 6. The outgoing packet is stripped of its tag to become an untagged packet as it leaves port 6. For port 5, the outgoing packet leaves as a tagged packet with VLAN ID 20.

## Access Control Lists (ACLs)

ACLs ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and provide security for the network. ACLs are normally used in firewall routers that are positioned between the internal network and an external network, such as the Internet. They can also be used on a router positioned between two parts of the network to control the traffic entering or exiting a specific part of the internal network. The added packet processing required by the ACL feature does not affect switch performance. That is, ACL processing occurs at wire speed.

Access lists are a sequential collection of permit and deny conditions. This collection of conditions, known as the filtering criteria, is applied to each packet that is processed by the device. The forwarding or dropping of a packet is based on whether the packet matches the specified criteria.

Traffic filtering requires the following two basic steps:

1. Create an access list definition.

The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can assign traffic that matches the criteria to a particular queue. A default denies all rule is the last rule of every list.

2. Apply the access list to an interface in the inbound direction.

The switch enables ACLs to be bound to physical ports and LAGs. The switch software supports MAC ACLs IPv4 ACLs and IPv6 ACLs.

## Sample MAC ACL Configuration

The following example shows how to create a MAC-based ACL that permits Ethernet traffic from the Sales department on specified ports and denies all other traffic on those ports.

1. In the MAC ACL screen, create an ACL with the name Sales\_ACL for the Sales department of your network.

For more informations, see [MAC ACL](#) on page 150.

By default, this ACL is bound on the inbound direction, which means the switch examines traffic as it enters the port.

2. In the MAC Rules screen, create a rule for the Sales\_ACL with the following settings:
  - **ID.** 1
  - **Action.** Permit
  - **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

For more information about MAC ACL rules, see [MAC Rules](#) on page 150.

3. In the MAC Binding Configuration screen, assign the Sales\_ACL to Ethernet ports 6, 7, and 8 and click **Apply**.

For more information, see [MAC Binding Configuration](#) on page 152

You can assign an optional sequence number to indicate the order of this access list relative to other access lists if any are already assigned to this interface and direction.

4. The MAC Binding Table displays the interface and MAC ACL binding information.

For more information, see [MAC Binding Table](#) on page 152.

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 more traffic to enter these ports, you must add a permit rule with the desired match criteria and bind the rule to interfaces 6, 7, and 8.

## Sample Standard IP ACL Configuration

The following example shows how to create an IP-based ACL that prevents any IP traffic from the Finance department from being allowed on the ports that are associated with other departments. Traffic from the Finance department is identified by each packet's network IP address.

1. In the IP ACL screen, create an IP ACL with an IP ACL ID of 1.  
For more information, see [IP ACL](#) on page 153.
2. In the IP Rules screen, create a rule for IP ACL 1 with the following settings:
  - **Rule ID.** 1
  - **Action.** Deny
  - **Match Every.** False
  - **Source IP Address.** 192.168.187.0
  - **Source IP Mask.** 0.0.0.255

For more information about IP ACL rules, see [IP Rules](#) on page 154.

3. Click **Add**.
4. In the IP Rules screen, create a second rule for IP ACL 1 with the following settings:
  - **Rule ID.** 2

- **Action.** Permit
  - **Match Every.** True
5. Click **Add**.
  6. In 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, see [IP Binding Configuration](#) on page 158.  
By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch.
  7. Click **Apply**.
  8. Use the IP Binding Table screen to view the interfaces and IP ACL binding information.  
For more information, see [IP Binding Table](#) on page 159.

The IP ACL in this example matches all packets with the source IP address and subnet mask of the Finance department network and denies it on the Ethernet interfaces 2, 3, and 4 of the switch. The second rule permits all non-Finance traffic on the ports. The second rule is required because there is an explicit deny all rule as the lowest priority rule.

## Differentiated Services (DiffServ)

Standard IP-based networks are designed to provide best effort data delivery service. Best effort service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide consistent, predictable data delivery by distinguishing between packets 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. For this reason, 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 support DiffServ.

The DiffServ feature contains a number of conceptual QoS building blocks you can use to construct a differentiated service network. Use these same blocks in various ways to build other types of QoS architectures.

There are three key QoS building blocks needed to configure DiffServ:

- Class
- Policy
- Service (that is, 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 and destination MAC addresses
- EtherType
- Class of Service (802.1 p priority) value (first or only VLAN tag)
- VLAN ID range (first or 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 and destination ports
- Source and destination IP addresses

From a DiffServ point of view, there are two types of classes:

- DiffServ traffic classes
- DiffServ service levels or 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 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 (that is, exclude option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes, or PHBs identified by a given DSCP value, on the egress interface. You define the service levels by configuring BA classes for each.

## Create Policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, there are two types of policies:

- **Traffic Conditioning Policy.** A policy applied to a DiffServ traffic class
- **Service Provisioning Policy.** A policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

### Traffic Conditioning Policy

Traffic conditioning pertains to actions performed on incoming traffic. Several distinct QoS actions are associated with traffic conditioning:

- **Dropping.** Drops a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
- **Marking IP DSCP.** Marks and remarks the DiffServ code point in a packet with the DSCP value representing the service level associated with a particular DiffServ traffic class.
- **Marking CoS (802.1p).** Sets the 3-bit priority field in the first or 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 exist. This is useful for assigning a Layer 2 priority level based on a DiffServ forwarding class (that is, DSCP or IP precedence value) definition to convey some QoS characteristics to downstream switches that do not routinely look at the DSCP value in the IP header.
- **Policing.** A method of limiting 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.** 802.1p user priority bits are marked or re-marked and forwarded.
  - **Mark DSCP.** The packet DSCP is marked or 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 considers the current packet marking when determining the policing outcome. An auxiliary traffic class is used 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 might be optionally specified as well.

- **Counting.** Updates 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 [Switch Statistics](#) on page 161.
- **Assigning QoS Queue.** Directs traffic stream to the specified QoS queue. This enables a traffic classifier to specify which one of the supported hardware queues is used for handling packets belonging to the class.

## Sample DiffServ Configuration

### ➤ To create a DiffServ Class or Policy and attach it to a switch interface:

1. In the QoS Class Configuration screen, create a class with the following settings:

- **Class Name.** Class1
- **Class Type.** All

For more information about this screen, see [Class Configuration](#) on page 116.

2. Click **Class1** 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.** 0.0.0.255
- **Source L4 Port.** Other, and enter **4567** as the source port value
- **Destination IP Address.** 192.12.2.0
- **Destination Mask.** 0.0.0.255
- **Destination L4 Port.** Other, and enter **4568** as the destination port value

For more information about this screen, see [Class Configuration](#) on page 116.

4. Click **Apply**.

5. In the Policy Configuration screen, create a policy with the following settings:

- **Policy Selector.** Policy1
- **Member Class.** Class1

For more information about this screen, see [Policy Configuration](#) on page 119.

6. Click **Add** to add the new policy.

7. Click the **Policy1** to view the Policy Class Configuration screen for this policy.

8. Configure the policy attributes as follows:

- **Assign Queue.** 7
- **Policy Attribute.** Simple Policy
- **Color Mode.** Color Blind

- **Committed Rate.** 10,000 Kbps
- **Committed Burst Size.** 128 KB
- **Confirm Action.** Send
- **Violate Action.** Drop

For more information about this screen, see *Policy Configuration* on page 119.

9. In the Service Configuration screen, select the check box next to interfaces xg7 and xg8 to attach the policy to these interfaces, and click **Apply**.

For more information, see *Service Configuration* on page 121.

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 7.

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 10,000 Kbps and burst size of 128 KB. Packets that violate the committed rate and burst size are dropped.

## 802.1x

Local area networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments, it might 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 or 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 to offer services to other systems reachable through the LAN. Port-based network access control allows the operation of a switch's ports to be controlled in order to ensure that access to its services is permitted only 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.

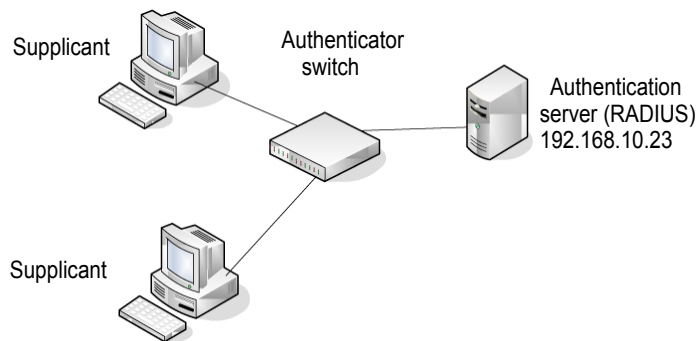
Access control is achieved by enforcing authentication of supplicants that are attached to a controlled ports of the authenticator. The result of the authentication process determines whether the supplicant is authorized to access services on that controlled port.

A port access entity (PAE) is able to adopt one of the following roles within an access control interaction:

- **Authenticator.** A port that enforces authentication before allowing access to services available through that port.
- **Supplicant.** A port that attempts to access services offered by the authenticator.
- **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 so that the credentials can be checked, which determines the authorization state of the port. The authenticator PAE controls the authorized or unauthorized state of the controlled port depending on the outcome of the RADIUS-based authentication process.



## Sample 802.1x Configuration

This example shows how to configure the switch so that 802.1x-based authentication is required on the ports in a corporate conference room (xg1–xg8). These ports are available to visitors and need to be authenticated before they are granted 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. In the Port Authentication screen, select ports xg1 through xg8.
2. From the Port Control list, select **Auto**.

The Port Control setting for all other ports where authentication is not needed must be Authorized. When the Port Control setting is Authorized, the port is unconditionally put in a force-authorized state and does not require any authentication. When the Port Control setting is Auto, the authenticator PAE sets the controlled port mode.

3. In the Guest VLAN field for ports xg1–xg8, enter **150** to assign these ports to the guest VLAN.

You can configure more settings to control access to the network through the ports. See [Port Security](#) on page 142 for information about the settings.

4. Click **Apply**.
5. In the 802.1x Configuration screen, set the port-based authentication state and guest VLAN mode to **Enable** and click **Apply**.

For more information, see [Port Security](#) on page 142.

This example uses the default values for the port authentication settings, but you can configure several more settings. For example, the EAPoL Flood Mode field allows you to enable the forwarding of EAPoL frames when 802.1x is disabled on the device.

6. In the RADIUS Server Configuration screen, configure a RADIUS server with the following settings:
  - **Server Address.** 192.168.10.23
  - **Secret Configured.** Yes
  - **Secret.** secret123

- **Active.** Primary

For more information, see [RADIUS](#) on page 125.

7. Click **Add**.

8. In the Authentication List screen, configure the default list to use RADIUS as the first authentication method.

For more information, see [Authentication List](#) on page 128.

This example enables 802.1x-based port security on the switch and prompts the hosts connected on ports xg1–xg8 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 point-to-point and edgeport. MSTP is compatible with both RSTP and STP and behaves appropriately to STP and RSTP bridges.

An MSTP bridge can be configured to behave entirely as an RSTP bridge or an STP bridge. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provide 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 enables 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 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 only one of the MSTIs or the IST within the region, that the assignment is consistent among all the networking devices in the region, and that the stable connectivity of each MSTI and IST at the boundary of the region matches that of the CST. The stable active topology of the bridged LAN with respect to frames consistently classified as belonging to any given VLAN thus simply and fully connects

all LANs and networking devices throughout the network, though frames belonging to different VLANs can take different paths within any region, per IEEE DRAFT P802.1s/D13.

All bridges, whether they use STP, RSTP or MSTP, send information in configuration messages through bridge protocol data units (BPDUs) to assign port roles that determine each port's participation in a fully and simply connected active topology based on one or more spanning trees. The information communicated is known as the spanning tree priority vector. The BPDU structure for each of these different protocols is different. An MSTP bridge transmits the appropriate BPDU depending on the received type of BPDU from a particular port.

An MST region comprises of one or more MSTP bridges that have the same MST configuration identifier, using the same MSTIs that have no bridges attached that cannot receive and transmit MSTP BPDUs. The MST configuration identifier has the following components:

1. Configuration identifier format selector
2. Configuration name
3. Configuration revision level
4. Configuration digest: 16-byte signature of type HMAC-MD5 created from the MST Configuration table (a VLAN ID to MSTID mapping)

As there are multiple instances of spanning tree, there is an MSTP state maintained on a per-port, per-instance basis (or on a per port, per VLAN basis, as any VLAN can be in only one MSTI or CIST). For example, port A can be forwarding for example 1 while discarding for example 2. The port states have changed since IEEE 802.1D specification.

To support multiple spanning trees, an 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 VID 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, every VLAN is assigned to only one MSTI. The CIST is also an instance of spanning tree with an MSTID of 0.

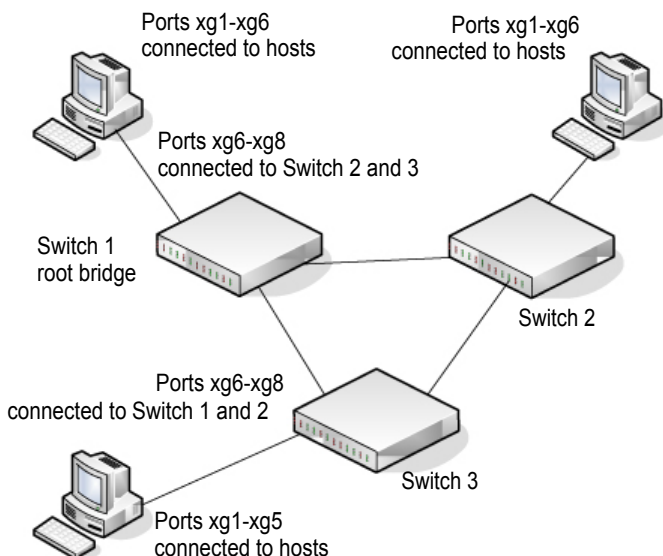
An instance might occur that has no VIDs allocated to it, but every VLAN must be allocated to one of the other instances of spanning tree.

The portion of the active topology of the network that connects any two bridges in the same MST region traverses only MST bridges and LANs in that region, and never bridges of any kind outside the region. In other words connectivity within the region is independent of external connectivity.

## Sample MSTP Configuration

This example shows how to create an MSTP instance from the switch. The sample network has three different switches that serve different locations in the network.

In this example, ports xg1–xg5 are connected to host stations, so those links are not subject to network loops. Ports xg6–xg8 are connected across Switches 1, 2, and 3.



➤ **Perform the following procedures on each switch to configure MSTP:**

1. Use the VLAN Configuration screen to create VLANs 300 and 500.  
For more information, see [VLAN Configuration](#) on page 53.
2. Use the VLAN Membership screen to include ports xg1–xg8 as tagged (T) or untagged (U) members of VLAN 300 and VLAN 500.  
For more information, see [VLAN Membership](#) on page 54.
3. In the STP Configuration screen, enable the Spanning Tree State option.  
For more information, see [STP Configuration](#) on page 66.  
Set the STP Operation Mode to MSTP. Use the default values for the rest of the STP configuration settings. By default, the configuration name is the switch MAC address.
4. In 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.

For more information, see [CST Configuration](#) on page 68.

5. In the CST Port Configuration screen, select ports xg1–xg8 and select **Enable** from the STP Status list.

For more information, see [CST Port Configuration](#) on page 69.

6. Click **Apply**.

7. Select ports xg1–xg5 (edge ports), and select **Enable** from the Fast Link list.

Since the edge ports are not at risk for network loops, ports with Fast Link are enabled transition directly to the forwarding state.

8. Click **Apply**.

You can use the CST Port Status screen to view spanning tree information about each port.

9. In the MST Configuration screen, create an MST instance with the following settings:

- **MST ID.** 1
- **Priority.** Use the default (32768)
- **VLAN ID.** 300

For more information, see [MST Configuration](#) on page 71.

10. Click **Add**.

11. Create a second MST instance with the following settings:

- **MST ID.** 2
- **Priority.** 49152
- **VLAN ID.** 500

12. Click **Add**.

In this example, assume that Switch 1 has become the Root bridge for the MST instance 1, and Switch 2 has become the Root bridge for MST instance 2. Switch 3 has hosts in the Sales department (ports xg1, xg2, and xg3) and in the Human Resources department (ports xg4 and xg5). Switches 1 and 2 also have hosts in the Sales and HR 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.

## Configure VLAN Routing with Static Route

### VLAN Routing Overview

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 NETGEAR switches 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 can also be used when a VLAN spans multiple physical networks, or when more segmentation or security is required.

### Sample VLAN Routing Configuration

➤ **To configure a switch to perform inter-VLAN routing:**

1. Use the IP Configuration screen to enable routing on the switch.

For more information, see *IP Configuration on page 20*.

2. Use *VLAN Configuration* on page 53 pages to 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 or 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. Configure the VLAN interfaces by using VLAN configuration screens.

For information about this, see *Sample VLAN Configuration* on page 187 Assign the VLAN the IP address identified using the VLAN routing configuration, for example, IP address 10.1.2.1 and mask 255.255.255.0.

4. Repeat this process for all VLANs to be configured as routing interfaces.

---

**Note:** You can use the VLAN Routing Wizard for creating VLANs, adding ports, and enabling them for routing by assigning the IP address and mask.

---