NETGEAR®

User Manual

Nighthawk S8000
Gaming & Streaming Advanced 8-Port Gigabit Ethernet Switch

Model GS808E

December 2018
202-11732-06

NETGEAR, Inc.
350 E. Plumeria Drive
San Jose, CA 95134, USA

Support

Thank you for purchasing this NETGEAR product. You can visit https://www.netgear.com/support/ to register your product, get help, access the latest downloads and user manuals, and join our community. We recommend that you use only official NETGEAR support resources.

Compliance and Conformity

For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.
See the regulatory compliance document before connecting the power supply.

Do not use this device outdoors. If you connect cables or devices that are outdoors to this device, see http://kb.netgear.com/000057103 for safety and warranty information.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11732-06	December 2018	Published the manual in a new format. Changed Methods to Discover or Access the Switch on page 17.
202-11732-05	August 2018	Added Safety Instructions and Warnings on page 11. Added Change the Language of the Local Browser Interface on page 25. Added the chapter Use VLANS for Traffic Segmentation on page 45. Added Enable a Link Aggregation Group on page 74. Added Enable a VLAN for IGMP Snooping on page 76. Added Control Management Access to the Switch on page 88. Added Change or Lift Access Restrictions to the Switch on page 89. Added Manage the DoS Prevention Mode on page 90. Removed the screen shots. Made multiple minor changes and adjustment to reflect changes in the local browser interface
202-11732-04	December 2017	Added Access the Switch From a Mac or Windows-Based Computer Using the NETGEAR Switch Discovery Tool on page 19. Removed information about accessing a switch from a Mac using a Firefox plug-in.
202-11732-03	November 2017	Added Methods to Discover or Access the Switch on page 17. Added information about accessing a switch from a Mac using a Firefox plug-in. Added Use the NETGEAR Insight App to Access the Switch on page 24. Added information about the NETGEAR Switch Discovery Tool.

(Continued)

Publication Part Number	Publish Date	Comments
202-11732-02	June 2017	Changed Apply the Gaming Preset Mode on page 29. Changed Apply the Media Streaming Preset Mode on page 30. Changed Apply the Standard Preset Mode on page 31. Changed Use Port-Based Quality of Service and Set Port Priorities on page 35. Added Set the Priority for a Port on page 40. Changed Set Up Static Link Aggregation on page 72. Changed Manage IGMPv3 IP Header Validation on page 77. Added Use the RESET Button to Renew the DHCP IP Address or Reenable DHCP on page 88. Updated multiple figures and made minor changes to many other sections.
202-11732-01	March 2017	First publication.

Contents

Chapter 4 Use VLANS for Traffic Segmentation

Chapter 5 Manage the Switch in Your Network

Appendix B Additional Switch Discovery and Access Information

1

Hardware Overview of the Switch

The NETGEAR Nighthawk® S8000 Gaming & Streaming Advanced 8-Port Gigabit Ethernet Switch (GS808E), in this manual referred to as the switch, provides high-performance switching for the home for multiplayer, online, or VR gaming and 4K resolution HD and UHD (ultra-high-definition) television media streaming.

With one click you can optimize settings for gaming, media steaming, and standard networking, but you can also manually optimize Quality of Service (QoS) and set up prioritization and rate limiting for individual ports. The switch supports IGMP snooping for multicast operation and link aggregation for a connection of up to 4 Gbps to link aggregation–enabled devices such as ReadyNAS.

The chapter contains the following sections:

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

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

Related Documentation

The following related documentation is available at netgear.com/support/download/:

- Installation guide
- Data sheet

Switch Package Contents

The package contains the switch, AC power adapter (localized to the country of sale), and installation guide.

Status LEDs

Status LEDs are located on the top panel and back panel of the switch.

Figure 1. Power LED

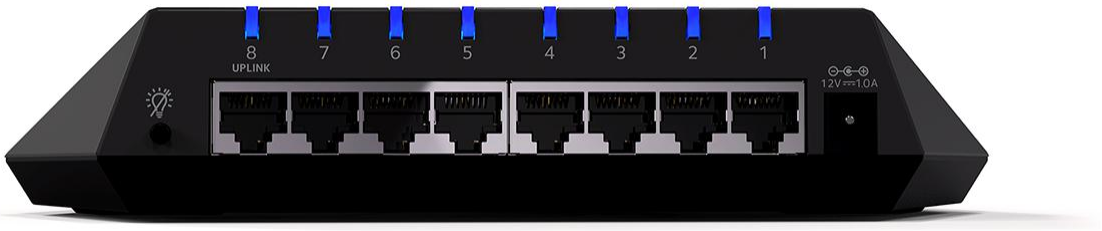

Figure 2. Port LEDs

Table 1. LED descriptions

LED	Description
Power LED	**Off**. No power is supplied to the switch or the switch functions in Stealth Mode with its Power LED disabled (see Control the Power LED on page 93). **Solid blue**. Power is supplied to the switch and the switch is ready for operation.
Port LEDs (1 through 8)	**Off**. No link with a powered-on device is detected or the active ports function in Stealth Mode with their Port LEDs disabled (see Control the Port LEDs on page 92). **Solid blue**. A link with a powered-on device is detected. **Blinking blue**. Traffic is detected. **All port LEDs blinking red in a scrolling pattern**. Firmware is being loaded onto the switch. **All port LEDs for ports in use blinking blue fast**. The switch detected a network loop. For more information, see Detect a Network Loop on page 98.

For information about controlling the LEDs, see Control the Power LED on page 93 and Control the Port LEDs on page 92.

Back Panel

The back panel of the switch provides a button, eight ports, and a DC power connector.

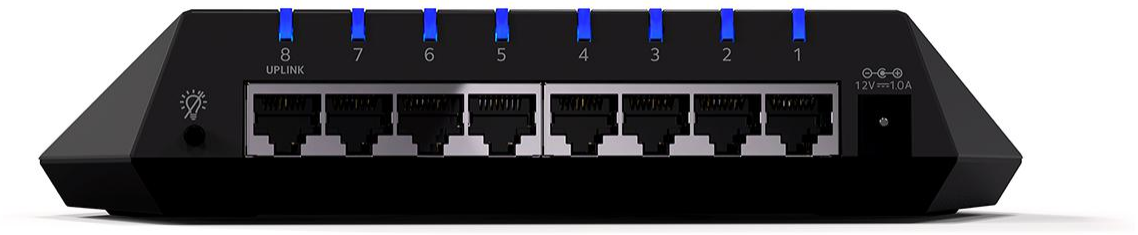

Figure 3. Switch back panel

Viewed from left to right, the back panel contains the following components:

- **LED button**. One button to turn the Power LED and port LEDs on and off.
- **Gigabit Ethernet ports**. Eight Gigabit Ethernet RJ-45 LAN ports:
  - **Port 8 (UPLINK)**. Connect this port to a LAN port on a router that is connected to the Internet.
  - **Ports 7 through 3**. Connect these ports to your network devices, other than your main streaming device (see Port 2) and main gaming device (see Port 1).

- **Port 2**. Connect this port to your main streaming device.
- **Port 1**. Connect this port to your main gaming device.

We recommend these port connections for the one-touch performance presets (see Apply a Performance Preset Mode on page 29). However, you can save custom performance presets and use different port connections (see Manage Custom Performance Preset Modes on page 32).

- **DC power connector**. One 12V, 1.0 A DC connector for the power adapter.

Note: The **RESET** button is located on the bottom panel of the switch. Press the **RESET** button for five seconds to reset the switch to factory default settings. For more information, see Return the Switch to Its Factory Default Settings on page 86.

Switch Label

The switch label on the bottom panel of the switch shows the serial number, MAC address, and default login information of the switch.

Figure 4. Switch label

Safety Instructions and Warnings

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions:

- This product is designed for indoor use only in a temperature-controlled and humidity-controlled environment. For more information, see the environmental specifications in the appendix or the data sheet.
  Any device that is located outdoors and connected to this product must be properly grounded and surge protected.
  Failure to follow these guidelines can result in damage to your NETGEAR product, which might not be covered by NETGEAR's warranty, to the extent permissible by applicable law.
- Observe and follow service markings:
  - Do not service any product except as explained in your system documentation. Some devices should never be opened.
  - If applicable to your device, opening or removing covers that are marked with the triangular symbol with a lightning bolt can expose you to electrical shock. We recommend that only a trained technician services components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
  - Depending on your device, the power adapter, power adapter cable, power cable, extension cable, or plug is damaged.
  - An object fell into the product.
  - The product was exposed to water.
  - The product was dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide, or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- If applicable to your device, allow the product to cool before removing covers or touching internal components.

- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To avoid damaging your system, if your device uses a power supply with a voltage selector, be sure that the selector is set to match the power at your location:
  - 115V, 60 Hz in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  - 100V, 50 Hz in eastern Japan and 100V, 60 Hz in western Japan
  - 230V, 50 Hz in most of Europe, the Middle East, and the Far East
- Be sure that attached devices are electrically rated to operate with the power available in your location.
- Depending on your device, use only a supplied power adapter or approved power cable:
  If your device uses a power adapter:
  - If you were not provided with a power adapter, contact your local NETGEAR reseller.
  - The power adapter must be rated for the product and for the voltage and current marked on the product electrical ratings label.

  If your device uses a power cable:
  - If you were not provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable approved for your country.
  - The power cable must be rated for the product and for the voltage and current marked on the product electrical ratings label. The voltage and current rating of the cable must be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets.
- If applicable to your device, the peripheral power cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a three-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.

- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables, power adapter cables, or power cables carefully. Route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power adapters, power adapter cables, power cables or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local and national wiring rules.

2

Install and Access the Switch in Your Network

This chapter describes how you can install and access the switch in your network.

The chapter contains the following sections:

Set Up the Switch in Your Network and Power On the Switch

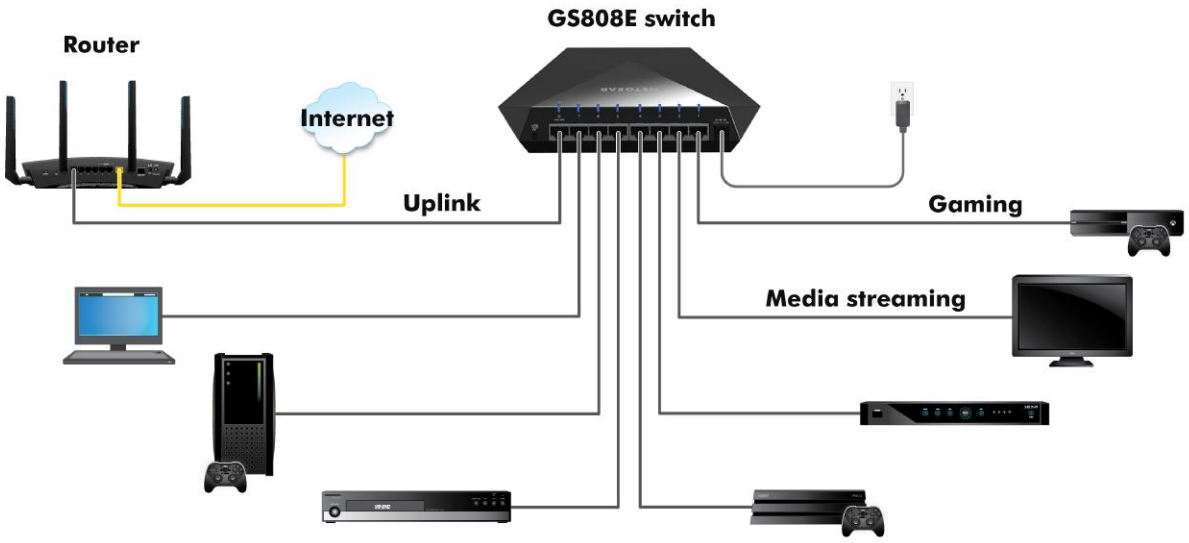

Figure 5. Example connections

To set up the switch in your network and power on the switch:

1. Connect LAN port 8 (UPLINK) on the switch to a LAN port on a router that is connected to the Internet.
2. On the switch, connect your devices as follows:
   - Connect your gaming device to port 1.
   - Connect your streaming device to port 2.
   - Connect all other devices (including additional gaming and streaming devices) to remaining ports 3 through 7.

   We recommend these port connections for the one-touch performance presets (see Apply a Performance Preset Mode on page 29). However, you can save custom performance presets and use different port connections (see Manage Custom Performance Preset Modes on page 32).
3. Connect the power adapter to the switch and plug the power adapter into an electrical outlet.

   The blue Power LED on top of the switch lights and the port LEDs for connected devices light.

Methods to Discover or Access the Switch

You can use any of the following methods to discover the switch in your network or access the switch to configure and manage it:

- **Computer and web browser**. Use a computer and a web browser to discover the switch in your network and access the local browser–based management interface of the switch:
  - Access the Switch From a Windows-Based Computer on page 17
  - Access the Switch From a Mac Using Bonjour on page 18
  - Access the Switch From a Mac or Windows-Based Computer Using the NETGEAR Switch Discovery Tool on page 19
  - Set Up a Fixed IP Address for the Switch on page 21
- **Insight app**. Install the NETGEAR Insight app on a smartphone or tablet to discover the switch in your network and access the local browser interface of the switch (see Use the NETGEAR Insight App to Access the Switch on page 24).

Access the Switch and Discover the IP Address of the Switch

By default, the switch receives an IP address from a DHCP server (or a router that functions as a DHCP server) in your network.

For information about setting up a fixed (static) IP address on the switch, see Set Up a Fixed IP Address for the Switch on page 21.

Access the Switch From a Windows-Based Computer

To access the switch from a Windows-based computer and discover the switch IP address:

1. Open Windows Explorer or File Explorer.
2. Click the **Network** link.
3. If prompted, enable the Network Discovery feature.
4. Under Network Infrastructure, locate the Nighthawk S8000 switch.
5. Double-click **Nighthawk S8000 (xx:xx:xx:xx:xx:xx)**, in which xx:xx:xx:xx:xx:xx is the MAC address of the switch.

The login page of the local browser interface opens.

6. Enter the switch password.

   The default password is **password**. The password is case-sensitive.

   The HOME page displays.

   The right pane (or, depending on the size of your browser window, the middle pane) shows the IP address that is assigned to the switch.

   Tip: You can copy and paste the IP address into a new shortcut or bookmark it for quick access on your computer or mobile device. However, if you restart the switch, a dynamic IP address (assigned by a DHCP server) might change and the bookmark might no longer link to the login page for the switch. In that situation, you must repeat this procedure so that you can discover the new IP address of the switch in the network and update your bookmark accordingly. You can also set up a fixed (static) IP address for the switch (see Set Up a Fixed IP Address for the Switch on page 21) to make sure that the new bookmark always links to the login page for the switch, even after you restart the switch.

Access the Switch From a Mac Using Bonjour

If your Mac supports Bonjour, you can use the following procedure. If your Mac does not support Bonjour, see Access the Switch From a Mac or Windows-Based Computer Using the NETGEAR Switch Discovery Tool on page 19.

To access the switch from a Mac using Bonjour and discover the switch IP address:

1. Open the Safari browser.
2. Select **Safari > Preferences**.

   The General page displays.
3. Click the **Advanced** tab.

   The Advanced page displays.
4. Select the **Include Bonjour in the Bookmarks Menu** check box.
5. Close the Advanced page.
6. Depending on your Mac OS version, select one of the following, in which xx:xx:xx:xx:xx:xx is the MAC address of the switch:

   - **Bookmarks > Bonjour > Nighthawk S8000 (xx:xx:xx:xx:xx:xx)**
   - **Bookmarks > Bonjour > Webpages Nighthawk S8000 (xx:xx:xx:xx:xx:xx)**

   The login page of the local browser interface opens.

7. Enter the switch password.

   The default password is **password**. The password is case-sensitive.

   The HOME page displays.

   The right pane (or, depending on the size of your browser window, the middle pane) shows the IP address that is assigned to the switch.

   Tip: You can copy and paste the IP address into a new shortcut or bookmark it for quick access on your computer or mobile device. However, if you restart the switch, a dynamic IP address (assigned by a DHCP server) might change and the bookmark might no longer link to the login page for the switch. In that situation, you must repeat this procedure so that you can discover the new IP address of the switch in the network and update your bookmark accordingly. You can also set up a fixed (static) IP address for the switch (see Set Up a Fixed IP Address for the Switch on page 21) to make sure that the new bookmark always links to the login page for the switch, even after you restart the switch.

Access the Switch From a Mac or Windows-Based Computer Using the NETGEAR Switch Discovery Tool

The NETGEAR Switch Discovery Tool lets you discover the switch in your network and access the local browser interface of the switch from a Mac or a 64-bit Windows-based computer. If your Mac does not support Bonjour, use the following procedure.

To install the NETGEAR Switch Discovery Tool, discover the switch in your network, access the switch, and discover the switch IP address:

1. Download the Switch Discovery Tool by visiting netgear.com/support/product/netgear-switch-discovery-tool.aspx.

   Depending on the computer that you are using, download either the Mac version or the version for a 64-bit Windows-based computer.

2. Temporarily disable the firewall, Internet security, antivirus programs, or all of these on the computer that you use to configure the switch.
3. Unzip the Switch Discovery Tool files, double-click the **.exe** or **.dmg** file (for example, `NETGEAR+Switch+Discovery+Tool+Setup+1.2.101.exe` or `NetgearSDT-V1.2.101.dmg`), and install the program on your computer.

   Depending on your computer setup, the installation process might add the **NETGEAR Switch Discovery Tool** icon to the Dock of your Mac or the desktop of your Windows-based computer.

4. Reenable the security services on your computer.

5. Power on the switch.

   The DHCP server assigns the switch an IP address.

6. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection. The computer and the switch must be on the same Layer 2 network.

7. Open the Switch Discovery Tool.

   If the **NETGEAR Switch Discovery Tool** icon is in the Dock of your Mac or on the desktop of your Windows-based computer, click or double-click the **NETGEAR Switch Discovery Tool** icon to open the program.

   The initial page displays a menu and a button.

8. From the **Choose a connection** menu, select the network connection that allows the Switch Discovery Tool to access the switch.
9. Click the **Start Searching** button.

   The Switch Discovery Tool displays a list of Smart Managed Plus Switches that it discovers on the selected network.

   For each switch, the tool displays the IP address.

10. To access the local browser interface of the switch, click the **ADMIN PAGE** button.

    The login page of the local browser interface opens.

11. Enter the switch password.

    The default password is **password**. The password is case-sensitive.

    The HOME page displays.

    The right pane (or, depending on the size of your browser window, the middle pane) shows the IP address that is assigned to the switch.

    Tip: You can copy and paste the IP address into a new shortcut or bookmark it for quick access on your computer or mobile device. However, if you restart the switch, a dynamic IP address (assigned by a DHCP server) might change and the bookmark might no longer link to the login page for the switch. In that situation, you must repeat this procedure so that you can discover the new IP address of the switch in the network and update your bookmark accordingly. You can also set up a fixed (static) IP address for the switch (see Set Up a Fixed IP Address for the Switch on page 21) to make sure that the new bookmark always links to the login page for the switch, even after you restart the switch.

Set Up a Fixed IP Address for the Switch

By default, the switch receives an IP address from a DHCP server (or a router that functions as a DHCP server) in your network. However, the DHCP server might not always issue the same IP address to the switch. For easy access to the switch local browser interface, you can set up a fixed (static) IP address on the switch. This allows you to manage the switch anytime from a mobile device because the switch IP address remains the same.

To change the IP address of the switch, you can connect to the switch by one of the following methods:

- **Through a network connection**. If the switch and your computer are connected to the same network (which is the most likely situation), you can change the IP address of the switch through a network connection (see Set Up a Fixed IP Address for the Switch Through a Network Connection on page 21).
- **Through a direct connection**. In the unlikely situation that the switch is not connected to a network, or for some reason you cannot connect to the switch over a network connection, you can change the IP address of the switch by using an Ethernet cable and making a direct connection to the switch (see Set Up a Fixed IP Address for the Switch by Connecting Directly to the Switch Off-Network on page 22).

Set Up a Fixed IP Address for the Switch Through a Network Connection

If the switch and your computer are connected to the same network (which is the most the likely situation), you can change the IP address of the switch through a network connection.

To disable the DHCP client of the switch and change the IP address of the switch to a fixed IP address by using a network connection:

1. Open a web browser from a computer that is connected to the same network as the switch.
2. Enter the IP address that is assigned to the switch.

   The login page displays.
3. Enter the switch password.

   The default password is **password**. The password is case-sensitive.

   The HOME page displays.

   The right pane (or, depending on the size of your browser window, the middle pane) shows the IP address that is assigned to the switch.

4. Select **IP Address (DHCP On)**.

   The button bar in the DHCP section displays green because the DHCP client of the switch is enabled.

5. Click the button in the DHCP section.

   The button bar displays gray, indicating that the DHCP client of the switch is disabled, and the IP address fields become editable.

6. Enter the fixed (static) IP address that you want to assign to the switch and the associated subnet mask and gateway IP address.

   You can also either leave the address in the **IP Address** field as it is (with the IP address that was issued by the DHCP server) or change the last three digits of the IP address to an unused IP address.

7. Write down the complete fixed IP address.

   You can bookmark it later.

8. Click the **APPLY** button.

   Your settings are saved. Your switch web session is disconnected when you change the IP address.

9. If the login page does not display, in the address field of your web browser, enter the new IP address of the switch.

   The login page displays.

10. For easy access to the local browser interface, bookmark the page on your computer.

Set Up a Fixed IP Address for the Switch by Connecting Directly to the Switch Off-Network

In the unlikely situation that the switch is not connected to a network, or for some reason you cannot connect to the switch over a network connection, you can change the IP address of the switch by using an Ethernet cable and making a direct connection to the switch.

To disable the DHCP client of the switch and change the IP address of the switch to a fixed IP address by using a direct connection:

1. Connect an Ethernet cable from your computer to an Ethernet port on the switch.
2. Change the IP address of your computer to be in the same subnet as the default IP address of the switch.

The default IP address of the switch is 192.168.0.239. This means that you must change the IP address of the computer to be on the same subnet as the default IP address of the switch (192.168.0.x).

The method to change the IP address on your computer depends on the operating system of your computer.

3. Open a web browser from a computer that is connected to the switch directly through an Ethernet cable.
4. Enter **192.168.0.239** as the IP address of the switch.
   The login page displays.
5. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
   The right pane (or, depending on the size of your browser window, the middle pane) shows the IP address that is assigned to the switch.
6. Select **IP Address (DHCP On)**.
   The button bar in the DHCP section displays green because the DHCP client of the switch is enabled.
7. Click the button in the DHCP section.
   The button bar displays gray, indicating that the DHCP client of the switch is disabled, and the IP address fields become editable.
8. Enter the fixed (static) IP address that you want to assign to the switch and the associated subnet mask and gateway IP address.
9. Write down the complete fixed IP address.
   You can bookmark it later.
10. Click the **APPLY** button.
    Your settings are saved. Your switch web session is disconnected when you change the IP address.
11. Disconnect the switch from your computer and install the switch in your network.
    For more information, see Set Up the Switch in Your Network and Power On the Switch on page 16.
12. Restore your computer to its original IP address.

13. Verify that you can connect to the switch with its new IP address:
    a. Open a web browser from a computer that is connected to the same network as the switch.
    b. Enter the new IP address that you assigned to the switch.
    The login page displays.
    c. Enter the switch password.
    The default password is **password**. The password is case-sensitive.
    The HOME page displays.

Use the NETGEAR Insight App to Access the Switch

The NETGEAR Insight app lets you discover the switch in your network and access the local browser interface of the switch from your smartphone or tablet.

To access the switch from the Insight app:

1. On your iOS or Android mobile device, go to the app store, search for NETGEAR Insight, and download and install the app.
2. If the switch is directly connected to a WiFi router or access point, connect your mobile device to the WiFi network of the router or access point.
3. Select **LOG IN** to log in to your existing NETGEAR account or tap the **CREATE NETGEAR ACCOUNT** button to create a new account.
4. After you log in to your account, name your network and specify a device admin password that applies to all devices that you add to this network, and tap the **NEXT** button.
5. You can now add a device. Choose one of the following options:
    - Add a device by scanning your network.
    - Add a device by entering its serial number.
    - Add a device by scanning its barcode.

    Note: Pages might display and suggest that you connect the switch to power and to an uplink. If you already did this, on these pages, tap the **NEXT** button.

6. If the switch is not yet connected to the same WiFi network as your mobile device, connect it now to the same WiFi network, wait two minutes, and then tap the **NEXT** button.

The switch is discovered and registered on the network.

7. In the Insight app, select the switch and tap the **Visit Web Interface** link.
   The login page of the local browser interface opens.
8. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.

Change the Language of the Local Browser Interface

By default, the language of the local browser interface is set to Auto so that the switch can automatically detect the language. However, you can set the language to a specific one.

To change the language of the local browser interface:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **System Info**.
   The System Info fields display.
5. From the **Language** menu, select a language.
6. Click the **APPLY** button.
   A pop-up warning window opens.
7. Click the **CONTINUE** button.
   Your settings are saved and the language changes.

Change the Switch Password

The default password to access the local browser interface of the switch is **password**. We recommend that you change this password to a more secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 20 characters.

To change the switch password:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **CHANGE PASSWORD**.
   The CHANGE PASSWORD page displays.
6. In the **Current Password** field, type the current password for the switch.
7. Type the new password in the **New Password** field and in the **Retype New Password** field.
8. Click the **APPLY** button.
   Your settings are saved. Keep the new password in a secure location so that you can access the switch in the future.

Register the Switch

We recommend that you use the NETGEAR Insight mobile app to register the switch (see Use the NETGEAR Insight App to Access the Switch on page 24).

Registering the switch allows you to receive email alerts and streamlines the technical support process. However, you can also register the switch through the local browser interface, in which case the switch must be connected to the Internet.

To register the switch through the local browser interface:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **PRODUCT REGISTRATION**.
   The PRODUCT REGISTRATION page displays.
6. Click the **REGISTER** button.
   The switch contacts the registration server.
7. Follow the onscreen process to register the switch.

3

Optimize the Switch Performance

This chapter describes how you can optimize the performance of the switch.

The chapter contains the following sections:

Apply a Performance Preset Mode

The switch comes with three predefined preset modes that let you optimize the performance of the switch with a preset configuration. These modes include a gaming mode, a media streaming mode, and a standard mode. The switch also provides two custom preset modes that you can define with a preset configuration and save for easy retrieval (see Manage Custom Performance Preset Modes on page 32).

A preset mode affects the Quality of Service (QoS) and port prioritization of the switch.

Apply the Gaming Preset Mode

The Gaming Preset mode minimizes the data delay (latency) of traffic that the switch manages so that gaming network traffic can be processed very quickly. If you use the Gaming Preset mode, be sure that you connect your gaming device to port 1 and the uplink to your router to port 8.

Applying the Gaming Preset mode does the following:

- Sets the QoS port priority for ports 1 and 8 to Critical.
- Sets the QoS port priority for ports 2 through 7 to Low.
- Enables IGMP snooping for the switch (for more information, see Manage IGMP Snooping on page 75).
- Disables flow control for all ports (for more information, Manage Flow Control for a Port on page 41).
- Disables power saving for the switch (for more information, see Manage the Power Saving Mode on page 91).
- Sets the QoS mode to port-based (for more information, see Use Port-Based Quality of Service and Set Port Priorities on page 35).

Before you apply the Gaming Preset mode, you can save your current QoS, port prioritization, multicast, flow control, and IGMP snooping settings and other settings as a custom preset mode (see Save Your Quality of Service Settings as a Custom Preset Mode on page 32) so that you can easily revert to your current QoS configuration.

To apply the Gaming Preset mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.

The default password is **password**. The password is case-sensitive.

The HOME page displays.

4. Select **PRESET MODES**.
   The PRESET MODES page displays. The **LOAD** tab is automatically selected.
5. Select **GAMING PRESET**.
   The PREVIEW GAMING PRESET section shows the settings for the Gaming Preset mode.
6. Click the **APPLY** button.
   Your settings are saved.

Apply the Media Streaming Preset Mode

The Media Streaming Preset mode maximizes the throughput of traffic that the switch manages so that streaming media such as music, videos, and movies can be processed very quickly. If you use the Media Streaming mode, be sure that you connect your media streaming device to port 2 and the uplink to your router to port 8.

Applying the Media Streaming Preset mode does the following:

- Sets the QoS port priority for ports 2 and 8 to Critical.
- Sets the QoS port priority for ports 1 and 3 through 7 to Low.
- Enables IGMP snooping for the switch (for more information, see Manage IGMP Snooping on page 75).
- Disables flow control for all ports (for more information, Manage Flow Control for a Port on page 41).
- Disables power saving for the switch (for more information, see Manage the Power Saving Mode on page 91).
- Sets the QoS mode to port-based (for more information, see Use Port-Based Quality of Service and Set Port Priorities on page 35).

Before you apply the Media Streaming Preset mode, you can save your current QoS, port prioritization, multicast, flow control, and IGMP snooping settings and other settings as a custom preset mode (see Save Your Quality of Service Settings as a Custom Preset Mode on page 32) so that you can easily revert to your current QoS configuration.

To apply the Media Streaming Preset mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

The login page displays.

3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **PRESET MODES**.
   The PRESET MODES page displays. The **LOAD** tab is automatically selected.
5. Select **MEDIA STREAMING PRESET**.
   The PREVIEW MEDIA STREAMING PRESET section shows the settings for the Media Streaming Preset mode.
6. Click the **APPLY** button.
   Your settings are saved.

Apply the Standard Preset Mode

The Standard Preset mode, which is the default mode, gives all ports equal prioritization.

Applying the Standard Preset mode does the following:

- Sets the QoS port priority for all ports to High.
- Enables IGMP snooping for the switch (for more information, see Manage IGMP Snooping on page 75).
- Disables flow control for all ports (for more information, Manage Flow Control for a Port on page 41).
- Disables power saving for the switch (for more information, see Manage the Power Saving Mode on page 91).
- Sets the QoS mode to port-based (for more information, see Use Port-Based Quality of Service and Set Port Priorities on page 35).

Before you apply the Standard Preset mode, you can save your current QoS, port prioritization, multicast, flow control, and IGMP snooping settings and other settings as a custom preset mode (see Save Your Quality of Service Settings as a Custom Preset Mode on page 32) so that you can easily revert to your current QoS configuration.

To apply the Standard Preset mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.

3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **PRESET MODES**.
   The PRESET MODES page displays. The **LOAD** tab is automatically selected.
5. Select **STANDARD PRESET (DEFAULT)**.
   The PREVIEW STANDARD PRESET section shows the settings for the Standard Preset mode.
6. Click the **APPLY** button.
   Your settings are saved.

Manage Custom Performance Preset Modes

You can save your current Quality of Service (QoS) settings as a custom preset mode, including the settings for IGMP snooping, flow control, the power saving mode, the QoS mode, and the priorities of the individual ports. You can also rename or delete these custom preset modes.

Save Your Quality of Service Settings as a Custom Preset Mode

Before you apply a performance preset mode (see Apply a Performance Preset Mode on page 29), you can save your current Quality of Service (QoS) settings as a custom preset mode.

To save your QoS settings as a custom preset mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **PRESET MODES**.

The PRESET MODES page displays. The **LOAD** tab is automatically selected.

5. Click the **SAVE** tab.
   The SAVE PRESET MODES page displays.
6. In the **Preset Mode Name** field, enter a name from 1 to 16 characters for the custom preset mode.
7. Select the Slot **1** or **2** button.
   You can save two custom preset modes, one in each slot.
8. Click the **APPLY** button.
   Your settings are saved. The preset custom mode is displayed on the PRESET MODES page.

Rename a Custom Preset Mode

After you save a custom preset mode, you can rename the mode.

To rename a custom preset mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **PRESET MODES**.
   The PRESET MODES page displays. The **LOAD** tab is automatically selected.
5. Click the **SAVE** tab.
   The SAVE PRESET MODES page displays.
6. Select the Slot **1** or **2** button.
7. In the **Preset Mode Name** field, enter a new name from 1 to 16 characters for the custom preset mode.
8. Click the **RENAME** button.
   Your settings are saved.

Delete a Custom Preset Mode

You can delete a custom preset mode that you no longer need.

To delete a custom preset mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **PRESET MODES**.
   The PRESET MODES page displays. The **LOAD** tab is automatically selected.
5. Select the custom preset mode.
   The PREVIEW page displays.
6. Click the **DELETE** button.
   Your settings are saved. The custom preset mode is removed from the PRESET MODES pages.

Manually Set the Quality of Service Mode and Port Rate Limits

Instead of using preset performance modes, you can manually set the Quality of Service (QoS) modes to manage traffic:

- **Port-based QoS mode**. Lets you set the priority (low, medium, high, or critical) for individual port numbers and lets you set rate limits for incoming and outgoing traffic for individual ports. If broadcast filtering is enabled, you can also set the storm control rate for incoming traffic for individual ports.
- **802.1P/DSCP QoS mode**. Applies pass-through prioritization that is based on tagged packets and lets you set rate limits for incoming and outgoing traffic for individual ports. If broadcast filtering is enabled, you can also set the storm control rate for incoming traffic for individual ports.

This QoS mode applies only to devices that support 802.1P and Differentiated Services Code Point (DSCP) tagging. For devices that do not support 802.1P and DSCP tagging, ports are not prioritized but the configured rate limit is still applied.

You can limit the rate of incoming traffic, outgoing traffic, or both on a port to prevent the port (and the device that is attached to it) from taking up too much bandwidth on the switch. Rate limiting, which you can set for individual ports in either QoS mode, simply means that the switch slows down all traffic on a port so that traffic does not exceed the limit that you set for that port. If you set the rate limit on a port too low, you might, for example, see degraded video stream quality, sluggish response times during online activity, and other problems.

Use Port-Based Quality of Service and Set Port Priorities

Port-based priority is the default QoS mode on the switch and the preset performance modes (gaming, media streaming, and standard) are port-based.

Note: If the QoS mode on the switch is 802.1P/DSCP, we recommend that you first save your current QoS settings as a custom preset mode before you change the QoS mode to the Port-based mode. For more information, see Save Your Quality of Service Settings as a Custom Preset Mode on page 32.

For each port, you can set the priority and the rate limits for both incoming and outgoing traffic:

- **Port priority**. The switch services traffic from ports with a critical priority before traffic from ports with a high, medium, or low priority. Similarly, the switch services traffic from ports with a high priority before traffic from ports with a medium or low priority. If severe network congestion occurs, the switch might drop packets with a low priority.
- **Port rate limits**. The switch accepts traffic on a port at the rate (the speed of the data transfer) that you set for incoming traffic on that port. The switch transmits traffic from a port at the rate that you set for outgoing traffic on that port. You can select each rate limit as a predefined data transfer threshold from 512 Kbps to 512 Mbps.

Note: If you set a port rate limit, the actual rate might fluctuate, depending on the type of traffic that the port is processing.

To use the Port-based QoS mode and set the priority and rate limits for ports:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   The login page displays.

3. Enter the switch password.

   The default password is **password**. The password is case-sensitive.

   The HOME page displays.

4. From the menu at the top of the page, select **SWITCHING**.
   The Quality of Service (QoS) page displays.

5. If the selection from the **QoS Mode** menu is **802.1P/DSCP**, do the following to change the selection to **Port-based**:
   a. From the **QoS Mode** menu, select **Port-Based**.
      A pop-up warning window opens.
   b. Click the **CONTINUE** button.
      The pop-up window closes.

   Note: For information about broadcast filtering, see Manage Broadcast Filtering and Set Port Storm Control Rate Limits on page 38.

6. To set the port priorities, do the following:
   a. Click the **PRIORITY** tab.
   b. Click the purple **pencil** icon.
      The EDIT PRIORITY page displays.
   c. For each port for which you want to set the priority, select **Low**, **Medium**, **High**, or **Critical** from the individual menu for the port.
      The default selection is High.
   d. Click the **APPLY** button.
      Your settings are saved and the EDIT PRIORITY page closes.

7. To set rate limits, do the following:
   a. Click the **RATE LIMITS** tab.
   b. Click the purple **pencil** icon.
      The EDIT RATE LIMITS page displays.
   c. For each port for which you want to set rate limits, select the rate in Kbps or Mbps from the individual **In Limits** and **Out Limits** menus for the port.
      The default selection is No Limit.
   d. Click the **APPLY** button.
      Your settings are saved and the EDIT RATE LIMITS page closes.

Use 802.1P/DSCP Quality of Service

In the 802.1P/DSCP QoS mode, the switch uses the 802.1P or DSCP information in the header of an incoming packet to prioritize the packet. With this type of QoS, you cannot control the port prioritization on the switch because the device that sends the traffic (that is, the packets) to the switch prioritizes the traffic. However, you can set the rate limits for individual ports on the switch.

The switch accepts traffic on a port at the rate (the speed of the data transfer) that you set for incoming traffic on that port. The switch transmits traffic from a port at the rate that you set for outgoing traffic on that port. You can select each rate limit as a predefined data transfer threshold from 512 Kbps to 512 Mbps.

Note: If the QoS mode on the switch is Port-based, we recommend that you first save your current QoS settings as a custom preset mode before you change the QoS mode to the 802.1P/DSCP QoS mode. For more information, see Save Your Quality of Service Settings as a Custom Preset Mode on page 32.

To use 802.1P/DSCP QoS mode and set the rate limits for ports:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The Quality of Service (QoS) page displays.
5. If the selection from the **QoS Mode** menu is **Port-based**, do the following to change the selection to **802.1P/DSCP**:
   a. From the **QoS Mode** menu, select **802.1P/DSCP**.
      A pop-up warning window opens.
   b. Click the **CONTINUE** button.
      The pop-up window closes.

      Note: For information about broadcast filtering, see Manage Broadcast Filtering and Set Port Storm Control Rate Limits on page 38.

6. To set rate limits, do the following:
   a. Click the **RATE LIMITS** tab.
      If broadcast filtering is disabled, only the RATE LIMITS tab displays.
   b. Click the purple **pencil** icon.
      The EDIT RATE LIMITS page displays.
   c. For each port for which you want to set rate limits, select the rate in Kbps or Mbps from the individual **In Limits** and **Out Limits** menus for the port.
      The default selection is No Limit.
   d. Click the **APPLY** button.
      Your settings are saved and the EDIT RATE LIMITS page closes.

Manage Broadcast Filtering and Set Port Storm Control Rate Limits

A broadcast storm is a massive transmission of broadcast packets that are forwarded to every port on the switch. If they are not blocked, broadcast storm packets can delay or halt the transmission of other data and cause problems. However, you can block broadcast storms on the switch.

You can also set storm control rate limits for each port. Storm control measures the incoming broadcast, multicast, and unknown unicast frame rates separately on each port, and discards the frames if the rate that you set for the port is exceeded. By default, no storm control rate limit is set for a port. You can select each storm control rate limit as a predefined data transfer threshold from 512 Kbps to 512 Mbps.

To manage broadcast filtering and set the storm control rate limits for ports:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The Quality of Service (QoS) page displays.

5. If the selection from the **QoS Mode** menu is not the QoS mode that you want to configure, do the following to change the QoS mode:
   a. From the **QoS Mode** menu, select **Port-Based** or **802.1P/DSCP**.
      A pop-up warning window opens.
   b. Click the **CONTINUE** button.
      The pop-up window closes and the QoS mode is changed.
6. Click the **Broadcast Filtering** button.
   When broadcast filtering is enabled, the button bar displays green.
7. Click the **APPLY** button.
   Broadcast filtering is enabled. In the right pane, the **STORM CONTROL RATE** tab displays.
8. To set storm control rate limits, do the following:
   a. Click the **STORM CONTROL RATE** tab.
   b. Click the purple **pencil** icon.
      The EDIT STORM CONTROL RATE page displays.
   c. For each port for which you want to set storm control rate limits, select the rate in Kbps or Mbps from the individual menu for the port.
      The default selection is No Limit.
   d. Click the **APPLY** button.
      Your settings are saved and the EDIT STORM CONTROL RATE page closes.

Manage Individual Port Settings

For each individual port, you can set the port priority, set rate limits for incoming and outgoing traffic, set the port speed (by default, the speed is set automatically), enable flow control, and change the port name label.

Set Rate Limits for a Port

You can limit the rate of incoming (ingress) traffic, outgoing (egress) traffic, or both on a port to prevent the port (and the device that is attached to it) from taking up too much bandwidth on the switch. Rate limiting simply means that the switch slows down all traffic on a port so that traffic does not exceed the limit that you set for that port. If you

set the rate limit on a port too low, you might, for example, see degraded video stream quality, sluggish response times during online activity, and other problems.

You also can set port rate limits (the same feature) as part of the Quality of Service configuration on the switch (see Manually Set the Quality of Service Mode and Port Rate Limits on page 34).

To set rate limits for incoming and outgoing traffic on a port:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
   The PORT STATUS pane displays on the right or the bottom of the HOME page, depending on the size of your browser window.
   A port that is in use shows as UP. A port that is not in use shows as AVAILABLE.
4. Select the port.
   The pane displays detailed information about the port.
5. Click the **EDIT** button.
   The EDIT PORT page displays for the selected port.
   If the QoS mode on the switch is Port-based (the default setting), the **Priority** menu displays on the page. If the QoS mode is 802.1P/DSCP, the **Priority** menu does not display.
6. From the **In Rate Limit** menu, **Out Rate Limit** menu, or both, select the rate in Kbps or Mbps.
   The default selection is No Limit.
7. Click the **APPLY** button.
   Your settings are saved.

Set the Priority for a Port

If the QoS mode on the switch is Port-based (the default setting), you can set the priority for a port.

The switch services traffic from ports with a critical priority before traffic from ports with a high, medium, or low priority. Similarly, the switch services traffic from ports with a high priority before traffic from ports with a medium or low priority. If severe network congestion occurs, the switch might drop packets with a low priority.

You also can set the priority for a port (the same feature) as part of the Quality of Service configuration on the switch (see Use Port-Based Quality of Service and Set Port Priorities on page 35).

To set the priority for a port:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
   The PORT STATUS pane displays on the right or the bottom of the HOME page, depending on the size of your browser window.
   A port that is in use shows as UP. A port that is not in use shows as AVAILABLE.
4. Select the port.
   The pane displays detailed information about the port.
5. Click the **EDIT** button.
   The EDIT PORT page displays for the selected port.
   If the QoS mode on the switch is Port-based (the default setting), the **Priority** menu displays on the page. If the QoS mode is 802.1P/DSCP, the **Priority** menu does not display.
6. From the **Priority** menu, select **Low**, **Medium**, **High**, or **Critical**.
   The default selection is High.
7. Click the **APPLY** button.
   Your settings are saved.

Manage Flow Control for a Port

IEEE 802.3x flow control works by pausing a port if the port becomes oversubscribed (that is, the port receives more traffic than it can process) and dropping all traffic for small bursts of time during the congestion condition.

You can enable or disable flow control for an individual port. By default, flow control is disabled for all ports.

To manage flow control for a port:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
   The PORT STATUS pane displays on the right or the bottom of the HOME page, depending on the size of your browser window.
   A port that is in use shows as UP. A port that is not in use shows as AVAILABLE.
4. Select the port.
   The pane displays detailed information about the port.
5. Click the **EDIT** button.
   The EDIT PORT page displays for the selected port.
   If the QoS mode on the switch is Port-based (the default setting), the **Priority** menu displays on the page. If the QoS mode is 802.1P/DSCP, the **Priority** menu does not display.
6. In the Flow Control section, enable or disable flow control by clicking the button.
   When flow control is enabled, the button bar displays green.
7. Click the **APPLY** button.
   Your settings are saved.

Change the Speed for a Port or Disable a Port

By default, the port speed on all ports is set automatically (that is, the setting is Auto) after the switch determines the speed using autonegotiation with the linked device. We recommend that you leave the Auto setting for the ports. However, you can select a specific port speed setting for each port or disable a port by shutting it down manually.

To change the speed for a port or disable a port:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
   The PORT STATUS pane displays on the right or the bottom of the HOME page, depending on the size of your browser window.
   A port that is in use shows as UP. A port that is not in use shows as AVAILABLE.
4. Select the port.
   The pane displays detailed information about the port.
5. Click the **EDIT** button.
   The EDIT PORT page displays for the selected port.
   If the QoS mode on the switch is Port-based (the default setting), the **Priority** menu displays on the page. If the QoS mode is 802.1P/DSCP, the **Priority** menu does not display.
6. Select one of the following options from the **Speed** menu:
   - **Auto**. The port speed is set automatically after the switch determines the speed using autonegotiation with the linked device. This is the default setting.
   - **Disable**. The port is shut down (blocked).
   - **10M half**. The port is forced to function at 10 Mbps with half-duplex.
   - **10M full**. The port is forced to function at 10 Mbps with full-duplex.
   - **100M half**. The port is forced to function at 100 Mbps with half-duplex.
   - **100M full**. The port is forced to function at 100 Mbps with full-duplex.

   Note: You cannot select Gigabit Ethernet as the port speed. However, if the setting from the **Speed** menu is **Auto**, the switch can use autonegotiation to automatically set the port speed to Gigabit Ethernet if the linked device supports that speed.
7. Click the **APPLY** button.
   Your settings are saved.

Add or Change the Name Label for a Port

By default, only ports 1, 2, and 8 contain a port name label:

- **Port 1**. Gaming
- **Port 2**. Media Streaming
- **Port 8**. Uplink

You can change these name labels. Other ports do not contain name labels, but you can add them. Adding or changing a name label does not change the nature of a port, that is, it is just a label.

To add or change a name label for a port:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
   The PORT STATUS pane displays on the right or the bottom of the HOME page, depending on the size of your browser window.
   A port that is in use shows as UP. A port that is not in use shows as AVAILABLE.
4. Select the port.
   The pane displays detailed information about the port.
5. Click the **EDIT** button.
   The EDIT PORT page displays for the selected port.
   If the QoS mode on the switch is Port-based (the default setting), the **Priority** menu displays on the page. If the QoS mode is 802.1P/DSCP, the **Priority** menu does not display.
6. In the **Port Name** field, type a name label for the port.
   The name label can be from 1 to 16 characters.
7. Click the **APPLY** button.
   Your settings are saved.

4

Use VLANS for Traffic Segmentation

This chapter describes how you can use VLANs to segment traffic on the switch.

The chapter contains the following sections:

VLAN Overview

Virtual LANs (VLANs) are made up of networked devices that are grouped logically into separate networks. You can group ports on a switch to create a virtual network made up of the devices connected to the ports.

You can group ports in VLANs using either port-based or 802.1Q criteria:

- **Port-based VLANs**. Assign ports to virtual networks. Ports with the same VLAN ID are placed in the same VLAN. This feature provides an easy way to partition a network into private subnetworks.
  If the switch is the only switch in your network and you do not need a VLAN to function across multiple network devices (such as a router, another switch, a WiFi AP, or any network device that supports VLANs), we recommend that you use a port-based VLAN. If you need a single VLAN on a single port (other than the uplink port), use the basic port-based VLAN configuration. If you need multiple VLANs on a single port, use the advanced port-based VLAN configuration.
  The switch supports the following port-based VLAN modes:
  - **Basic Port-Based VLAN**. In a basic port-based VLAN configuration, ports with the same VLAN ID are placed into the same VLAN. Except for the uplink port, you can assign each port to a single VLAN only. The number of VLANs is limited to the number of ports on the switch.
  - **Advanced Port-Based VLAN**. In an advanced port-based VLAN configuration, ports with the same VLAN ID are also placed into the same VLAN, but you can assign a single port to multiple VLANs.

- **802.1Q VLANs**. Create virtual networks using the IEEE 802.1Q standard. 802.1Q uses a VLAN tagging system to determine which VLAN an Ethernet frame belongs to. To use an 802.1Q VLAN that is set up on another device, you must know the VLAN ID.
  If you need a VLAN to function across multiple network devices (such as a router, another switch, a WiFi AP, or any network device that supports VLANs), we recommend that you use an 802.1Q VLAN. If you do not need to customize tagging on a single port and you do not need a voice VLAN, use the basic 802.1Q VLAN configuration. If you do need to customize tagging on a single port or you do need a voice VLAN, use the advanced 802.1Q VLAN configuration.
  The switch supports the following 802.1Q VLAN modes:
  - **Basic 802.1Q VLAN**. In a basic 802.1Q VLAN configuration, VLAN 1 is added to the switch and all ports (1 through 8) function in access mode as members of VLAN 1. You can change the mode for a port to trunk mode, you can add more VLANs, and you can assign a different VLAN to a port. A port that functions in access mode can belong to a single VLAN only and does not tag the traffic that

it processes. A port that functions in trunk mode automatically belongs to all VLANs on the switch and tags the traffic that it processes.

- **Advanced 802.1Q VLAN**. In an advanced 802.1Q VLAN configuration, VLAN 1 is added to the switch and all ports (1 through 8) are untagged members of VLAN 1. You can tag ports, untag ports, exclude ports, add more VLANs, assign a different VLAN to a port, manage port PVIDs, and manage a voice VLAN.

The following table provides an overview of VLAN features that are supported on the switch.

Table 2. Supported VLAN modes

VLAN Feature	Basic Port-Based VLAN	Advanced Port-Based VLAN	Basic 802.1Q VLAN	Advanced 802.1Q VLAN
Total number of VLANs	8	8	8	64
Egress tagging	No	No	Yes (trunk port only)	Yes
Multiple VLANs on a single port	No	Yes	Yes (trunk port only)	Yes
Voice VLAN	No	No	No	Yes

Activate the Basic Port-Based VLAN Mode and Assign VLANs

By default, all types of VLANs are disabled on the switch.

When you activate the Basic Port-Based VLAN mode, VLAN 1 through VLAN 8 are added to the switch (because the switch provides a total of 8 ports) and all ports are made members of VLAN 1. This is the default VLAN in the Basic Port-Based VLAN mode.

In the Basic Port-Based VLAN mode, you can assign each port (other than the uplink port) to a single VLAN only.

To activate the Basic Port-Based VLAN mode and assign VLANs:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.

3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
6. In the Basic Port-Based VLAN section, click the **ACTIVATE MODE** button.
   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **CONTINUE** button.
   Your settings are saved and the pop-up window closes. By default, VLAN 1 through VLAN 8 are added and each port is a member of VLAN 1.
8. To assign one or more ports to other VLANs, do the following:
   a. For each port that you want to assign to another VLAN, select a VLAN ID from the **VLAN** menu for the individual port.
      Each port can be assigned to a single VLAN only. However, for the port that you want to use as the uplink port to the Internet connection or a server, select **All** from the **VLAN** menu for the individual port.
   b. Click the **APPLY** button.
      Your settings are saved.

Manage Advanced Port-Based VLANs

In an advanced port-based VLAN configuration, ports with the same VLAN ID are placed into the same VLAN, but you can assign a single port to multiple VLANs.

For more information about port-based VLANs, see the following sections:

- Activate the Advanced Port-Based VLAN Mode
- Create an Advanced Port-Based VLAN
- Change an Advanced Port-Based VLAN
- Delete an Advanced Port-Based VLAN

Activate the Advanced Port-Based VLAN Mode

By default, all types of VLANs are disabled on the switch.

When you activate the Advanced Port-Based VLAN mode, VLAN 1 is added to the switch and all ports are made members of VLAN 1. This is the default VLAN in the Advanced Port-Based VLAN mode.

To activate the Advanced Port-Based VLAN mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
6. In the Advanced Port-Based VLAN section, click the **ACTIVATE MODE** button.
   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **CONTINUE** button.
   Your settings are saved and the pop-up window closes. By default, VLAN 1 is added and all ports are members of VLAN 1.
   For information about creating an advanced port-based VLAN, see Create an Advanced Port-Based VLAN on page 49.

Create an Advanced Port-Based VLAN

An advanced port-based VLAN configuration lets you create VLANs and assign ports on the switch to a VLAN. The number of VLANs is limited to the number of ports on the switch. In an advanced port-based VLAN configuration, one port can be a member of multiple VLANs.

By default, all ports are members of VLAN 1, but you can change the VLAN assignment.

To create an advanced port-based VLAN and assign ports as members:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

The login page displays.

3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
   If you did not yet activate the Advanced Port-Based VLAN mode, see Activate the Advanced Port-Based VLAN Mode on page 48.
6. In the Advanced Port-Based VLAN section, click the **ADD VLAN** button.
7. Specify the settings for the new VLAN:
   - **VLAN Name**. Enter a name from 1 to 14 characters.
   - **VLAN ID**. Enter a number from 1 to 8.
   - **Ports**. Select the ports that you want to include in the VLAN through a combination of the following actions:
     - Click the icon for an unselected port to add the port to the VLAN.
     - Click the icon for a selected port to remove the port from the VLAN.
     - Click the **Select All** link to add all ports to the VLAN.
     - Click the **Remove All** link to remove all selected ports from the VLAN.

     The icon for a selected port displays purple.

   Note: If ports are members of the same LAG, you must assign them to the same VLAN.

8. Click the **APPLY** button.
   Your settings are saved. The new VLAN is added to the VLAN table, which shows the port members for each VLAN.

Change an Advanced Port-Based VLAN

You can change the settings for an existing advanced port-based VLAN.

To change an advanced port-based VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
6. In the Advanced Port-Based VLAN section, click the VLAN that you want to change (you can click anywhere in the row for the VLAN) and click the **EDIT** button.
   The Advanced Port-Based VLAN pane displays.
7. Change the settings for the VLAN:
   - **VLAN Name**. Enter a name from 1 to 14 characters.
     You cannot change the VLAN ID. If you need to change the VLAN ID, delete the VLAN and create a new VLAN with another VLAN ID.
   - **Ports**. Select the ports that you want to include in the VLAN through a combination of the following actions:
     - Click the icon for an unselected port to add the port to the VLAN.
     - Click the icon for a selected port to remove the port from the VLAN.
     - Click the **Select All** link to add all ports to the VLAN.
     - Click the **Remove All** link to remove all selected ports from the VLAN.

     The icon for a selected port displays purple.

   Note: If ports are members of the same LAG, you must assign them to the same VLAN.

8. Click the **APPLY** button.
   Your settings are saved. The modified VLAN shows in the VLAN table.

Delete an Advanced Port-Based VLAN

You can delete an advanced port-based VLAN that you no longer need. You cannot delete the default VLAN.

Note: If you deactivate the basic or advanced port-based VLAN mode, all port-based VLANs are deleted.

To delete an advanced port-based VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
6. In the Advanced Port-Based VLAN section, click the VLAN that you want to delete (you can click anywhere in the row for the VLAN).
7. Click the **DELETE** button.
   Your settings are saved. The VLAN is deleted.

Manage Basic 802.1Q VLANs

In a basic 802.1Q VLAN configuration, VLAN 1 is added to the switch and all ports (1 through 8) function in access mode as members of VLAN 1. You can change the mode for a port to trunk mode, you can add more VLANs, and you can assign a different VLAN to a port.

After you activate the Basic 802.1Q VLAN mode, you can create VLANs, assign the VLANs to ports that function in access mode, and assign the trunk mode, which carries traffic for all VLANs.

For more information about basic 802.1Q VLANs, see the following sections:

- Activate the Basic 802.1Q VLAN Mode
- Create a Basic 802.1Q VLAN and Assign Ports as Members
- Assign the Port Mode in a Basic 802.1Q VLAN Configuration
- Change a Basic 802.1Q VLAN
- Delete a Basic 802.1Q VLAN

Activate the Basic 802.1Q VLAN Mode

By default, all types of VLANs are disabled on the switch.

When you activate the Basic 802.1Q VLAN mode, VLAN 1 is added to the switch and all ports (1 through 8) function in access mode (rather than trunk mode) as untagged members of VLAN 1. This is the default VLAN in the Basic 802.1Q VLAN mode.

To activate the Basic 802.1Q VLAN mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
6. In the Basic 802.1Q VLAN section, click the **ACTIVATE MODE** button.
   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **CONTINUE** button.
   Your settings are saved and the pop-up window closes. By default, VLAN 1 is added.
   For information about adding VLANs, see Create a Basic 802.1Q VLAN and Assign Ports as Members on page 54.
   For all ports, the default selection from the **Mode** menu is **Access**. For more information about access mode and trunk mode, see Assign the Port Mode in a Basic 802.1Q VLAN Configuration on page 55.

8. If you already determined which ports must function in trunk mode, for those ports, select **Trunk (uplink)** from the **Mode** menu.
9. Click the **SAVE** button.
   Your settings are saved.

Create a Basic 802.1Q VLAN and Assign Ports as Members

A basic 802.1Q VLAN configuration lets you create VLANs and assign ports on the switch to a VLAN. A port that functions in access mode can be member of a single VLAN only. The number of VLANs is limited to the number of ports on the switch. You can assign a VLAN ID number in the range of 1–4093.

To create a basic 802.1Q VLAN and assign ports as members:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
   If you did not yet activate the Basic 802.1Q VLAN mode, see Activate the Basic 802.1Q VLAN Mode on page 53.
   By default, the **Port Configuration** tab is selected and the 802.1Q-BASED PORT CONFIGURATION pane displays.
6. To add a VLAN and then assign ports as members of the VLAN, do the following:
   a. Click the **Edit VLAN** button.
      The 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane displays.
   b. Click the **ADD VLAN** button.
      The BASIC 802.1Q VLAN pop-up window opens.
   c. In the **VLAN Name** field, enter a name from 1 to 14 characters.
   d. In **VLAN ID** field, enter a number from 1 to 4093.

e. Click the **APPLY** button.
Your settings are saved. The new VLAN shows in the 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane.

f. Click the **Port Configuration** tab.
The 802.1Q PORT CONFIGURATIONS pane displays

g. For each port that you want to make a member of the new VLAN, select the VLAN from the **VLAN** menu for the individual port.

Note: If ports are members of the same LAG, you must assign them to the same VLAN.

7. For a port that functions in access mode, to add a VLAN by using the **VLAN** menu for the individual port, do the following:
   a. From the **VLAN** menu for the individual port, select **Add VLAN**.
   The BASIC 802.1Q VLAN pop-up window opens.
   b. In the **VLAN Name** field, enter a name from 1 to 14 characters.
   c. In the **VLAN ID** field, enter a number from 1 to 4093.
   d. Click the **APPLY** button.
   The pop-up window closes. The VLAN is added as a possible selection in the **VLAN** menu for each individual port.
   e. For each port that you want to make a member of the new VLAN, select the VLAN from the **VLAN** menu for the individual port.

   Note: If ports are members of the same LAG, you must assign them to the same VLAN.

8. Click the **SAVE** button.
   Your settings are saved.

   Note: For information about assigning the port mode, see Assign the Port Mode in a Basic 802.1Q VLAN Configuration on page 55.

Assign the Port Mode in a Basic 802.1Q VLAN Configuration

In an 802.1Q VLAN configuration, you can assign one of the following port modes:

- **Access mode**. A port that functions in access mode can belong to a single VLAN only and does not tag the traffic that it processes. You would typically use access

mode for a port that is connected to an end device such as a gaming device, media device, or computer. When a port that functions in access mode receives data that is untagged, the data is delivered normally. When a port that functions in access mode receives data that is tagged for a VLAN other than the one the port belongs to, the data is discarded.

- **Trunk mode**. A port that functions in trunk mode automatically belongs to all VLANs on the switch and tags the traffic that it processes. You would typically use trunk mode for a port that is connected to another network device. For example, you would assign trunk mode for an uplink to another switch or router and for a downlink to a WiFi access point.

To assign the port mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
   If you did not yet activate the Basic 802.1Q VLAN mode, see Activate the Basic 802.1Q VLAN Mode on page 53.
   By default, the **Port Configuration** tab is selected and the 802.1Q-BASED PORT CONFIGURATION pane displays.
6. For each individual port that you want to change, from the **Mode** menu, select either **Trunk (uplink)** to let the port function in trunk mode or **Access** to let the port function in access mode.
   If you place a port in trunk mode, the selection from the **VLAN** menu changes to **All** because all VLANs must be supported on a trunk port.
7. Click the **SAVE** button.
   Your settings are saved.

Change a Basic 802.1Q VLAN

You can change an existing basic 802.1Q VLAN.

To change a basic 802.1Q VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
   By default, the **Port Configuration** tab is selected and the 802.1Q-BASED PORT CONFIGURATION pane displays.
6. To change the name for the VLAN, do the following:
   a. Click the **Edit VLAN** button.
      The 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane displays.
   b. Click the VLAN that you want to change (you can click anywhere in the row for the VLAN).
   c. Click the **EDIT** button.
      The BASIC 802.1Q VLAN pop-up window opens.
   d. Change the VLAN name.
      You cannot change the VLAN ID. If you need to change the VLAN ID, delete the VLAN and create a new VLAN with another VLAN ID.
   e. Click the **APPLY** button.
      Your settings are saved. The modified VLAN shows in the 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane.
7. To change the membership of the VLAN, for each port that you want to make a member, select the VLAN from the **VLAN** menu for the individual port in the 802.1Q-BASED PORT CONFIGURATION pane.
8. Click the **SAVE** button.

Your settings are saved.

Delete a Basic 802.1Q VLAN

You can delete a basic 802.1Q VLAN that you no longer need. You cannot delete the default VLAN.

Note: If you deactivate the Basic 802.1Q VLAN mode, all 802.1Q VLANs are deleted.

To delete a basic 802.1Q VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
6. Click the **Edit VLAN** button.
   The 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane displays.
7. Click the VLAN that you want to delete (you can click anywhere in the row for the VLAN).
8. Click the **DELETE** button.
   Your settings are saved. The VLAN is deleted.

Manage Advanced 802.1Q VLANs

In an advanced 802.1Q VLAN configuration, VLAN 1 is added to the switch and all ports (1 through 8) are untagged members of VLAN 1. Advanced 802.1Q VLANs provide you with most configuration options: You can tag ports, untag ports, exclude ports, add

more VLANs, assign a different VLAN to a port, manage port PVIDs, and manage a voice VLAN, including the OUI table.

For more information about advanced 802.1Q VLANs, see the following sections:

- Activate the Advanced 802.1Q VLAN Mode
- Create an Advanced 802.1Q VLAN
- Change an Advanced 802.1Q VLAN
- Specify a Port PVID for an Advanced 802.1Q VLAN
- Set an Existing Advanced 802.1Q VLAN as the Voice VLAN and Adjust the CoS Value
- Change the OUI Table for the Voice VLAN
- Delete an Advanced 802.1Q VLAN

Activate the Advanced 802.1Q VLAN Mode

By default, all types of VLANs are disabled on the switch.

When you activate the Advanced 802.1Q VLAN mode, VLAN 1 is added to the switch and all ports (1 through 8) function as untagged members of VLAN 1. This is the default VLAN in the Advanced 802.1Q VLAN mode.

In an advanced 802.1Q VLAN configuration, you can set up VLANs to which you can add tagged or untagged ports. Port tagging allows a port to be associated with a particular VLAN and allows the VLAN ID tag to be added to data packets that are sent through the port. The tag identifies the VLAN that must receive the data. You can also manage the VLAN IDs (PVIDs) of the ports (see Specify a Port PVID for an Advanced 802.1Q VLAN on page 63).

To activate the Advanced 802.1Q VLAN mode and manage port tagging for the default VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.

6. In the Advanced 802.1Q VLAN section, click the **ACTIVATE MODE** button.
   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **CONTINUE** button.
   Your settings are saved and the pop-up window closes. By default, VLAN 1 is added and all ports are made untagged members of VLAN 1.
   For information about creating an advanced 802.1Q VLAN, see Create an Advanced 802.1Q VLAN on page 60.
8. To change the port tagging for the default VLAN (VLAN 1), do the following:
   a. In the table, click **1** or **Default** (you can click anywhere in the row for VLAN 1).
   b. Click the **EDIT** button.
   c. Select the port tags and whether ports are members of the VLAN through a combination of the following actions:
      - Click the **T** button for an individual port to make the port a tagged member of the VLAN.
      - Click the **U** button for an individual port to make the port an untagged member of the VLAN.
      - Click the **E** button for an individual port to exclude the port from the VLAN.
      - Click the **Tag All** link to make all ports tagged members of the VLAN.
      - Click the **Untag All** link to make all ports untagged members of the VLAN.
      - Click the **Exclude All** link to exclude ports from the VLAN.
   d. Click the **APPLY** button.
      Your settings are saved.

Create an Advanced 802.1Q VLAN

In an advanced 802.1Q VLAN configuration, you can set up VLANs to which you can add tagged or untagged ports. Port tagging allows a port to be associated with a particular VLAN and allows the VLAN ID tag to be added to data packets that are sent through the port. You can create a total of 64 advanced 802.1Q VLANs.

To create an advanced 802.1Q VLAN and assign ports as tagged or untagged members:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

The login page displays.

3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the Advanced 802.1Q VLAN Mode on page 59.
6. In the right pane, click the **ADD VLAN** button.
   The Advanced 802.1Q VLAN pane displays.
7. Specify the VLAN settings and assign ports as tagged or untagged members:
   a. In the **VLAN Name** field, enter a name from 1 to 14 characters.
   b. In the **VLAN ID** field, enter a number from 1 to 4094.
   c. Select the port tags and whether ports are members of the VLAN through a combination of the following actions:
      - Click the **T** button for an individual port to make the port a tagged member of the VLAN.
      - Click the **U** button for an individual port to make the port an untagged member of the VLAN.
      - Click the **E** button for an individual port to exclude the port from the VLAN.
      - Click the **Tag All** link to make all ports tagged members of the VLAN.
      - Click the **Untag All** link to make all ports untagged members of the VLAN.
      - Click the **Exclude All** link to exclude ports from the VLAN.

      Note: If ports are members of the same LAG, you must assign them to the same VLAN.
8. Click the **APPLY** button.
   Your settings are saved. The new VLAN shows in the Advanced 802.1Q VLAN pane.

Change an Advanced 802.1Q VLAN

You can change the settings for an existing advanced 802.1Q VLAN.

To change an advanced 802.1Q VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
6. In the table in the right pane, click the VLAN that you want to change (you can click anywhere in the row for the VLAN).
7. Click the **EDIT** button.
8. Change the VLAN settings as needed:
   - In the **VLAN Name** field, enter a name from 1 to 14 characters.
     You cannot change the VLAN ID. If you need to change the VLAN ID, delete the VLAN and create a new VLAN with another VLAN ID.
   - Select the port tags and whether ports are members of the VLAN through a combination of the following actions:
     - Click the **T** button for an individual port to make the port a tagged member of the VLAN.
     - Click the **U** button for an individual port to make the port an untagged member of the VLAN.
     - Click the **E** button for an individual port to exclude the port from the VLAN.
     - Click the **Tag All** link to make all ports tagged members of the VLAN.
     - Click the **Untag All** link to make all ports untagged members of the VLAN.
     - Click the **Exclude All** link to exclude ports from the VLAN.

9. Click the **APPLY** button.
   Your settings are saved. The modified VLAN shows in the Advanced 802.1Q VLAN pane.

Specify a Port PVID for an Advanced 802.1Q VLAN

A default port VLAN ID (PVID) is a VLAN ID tag that the switch assigns to incoming data packets that are not already addressed (tagged) for a particular VLAN. For example, if you connect a computer to port 6 of the switch and you want it to be a part of VLAN 2, add port 6 as a member of VLAN 2 and set the PVID of port 6 to 2. This configuration automatically adds a PVID of 2 to all data that the switch receives from the computer and makes sure that the data from the computer on port 6 can be seen only by other members of VLAN 2. You can assign only one PVID to a port.

Note: If you did not yet create an advanced 802.1Q VLAN, all ports are assigned PVID 1 and you cannot assign another PVID to a port. In this situation, first create an advanced 802.1Q VLAN (see Create an Advanced 802.1Q VLAN on page 60).

To assign a PVID to a port:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the Advanced 802.1Q VLAN Mode on page 59.
6. In PVID Table section in the right pane, click the **PVID Table** link.
   The Port and VLAN IDs pane displays.
7. Click the icon for a port.
   A menu displays. The menu lets you select a PVID for the port.

8. From the menu, select a VLAN ID and name.
   You can select only a VLAN that the selected port is a member of.
9. Click the **APPLY** button.
   Your settings are saved. The Port and VLAN IDs pane displays again. The VLAN ID that is assigned as the PVID displays with an asterisk (*) next to the port.
10. Click the **BACK** button.
    The Advanced 802.1Q VLAN pane displays.

Set an Existing Advanced 802.1Q VLAN as the Voice VLAN and Adjust the CoS Value

The switch can support a single advanced 802.1Q VLAN as the voice VLAN to facilitate voice over IP (VoIP) traffic. Because a voice VLAN might require a single port to join to multiple VLANs as an untagged member, you can set up a voice VLAN only as an advanced 802.1Q VLAN. For information about creating an advanced 802.1Q VLAN, see Create an Advanced 802.1Q VLAN on page 60.

A port that is a member of the voice VLAN sends all its voice packets through the voice VLAN but other types of packets (for example, data packets) that come in on the port are forwarding according to the PVID setting on the port.

The default Class of Service (CoS) value for the voice VLAN is 6, which you can adjust to any value from 0 (the lowest priority) to 7 (the highest priority). The voice VLAN CoS value applies to all traffic on the voice VLAN. You *can* set the default VLAN (VLAN 1) as the voice VLAN.

To set an existing advanced 802.1Q VLAN as the voice VLAN and adjust the CoS value for the voice VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.

5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the Advanced 802.1Q VLAN Mode on page 59.
6. In the table in the right pane, click the VLAN that you want to make the voice VLAN (you can click anywhere in the row for the VLAN).
7. Click the **EDIT** button.
8. In the Voice VLAN section, click the button so that the button bar display green.
   The VLAN is selected to be set as the voice VLAN.
9. From the **Class of Service** menu, select a CoS value.
   A value of 0 is the lowest priority and a value of 7 is the highest priority. The default value is 6.
   For information about viewing and changing the OUI settings, see Change the OUI Table for the Voice VLAN on page 65.
10. Click the **APPLY** button.
    Your settings are saved. The voice VLAN shows in the Advanced 802.1Q VLAN pane with a telephone icon.

Change the OUI Table for the Voice VLAN

For the voice VLAN, the switch supports default Organizationally Unique Identifiers (OUIs), which are associated with VoIP phones of specific manufacturers. All traffic received on voice VLAN ports from VoIP phones with a listed OUI is forwarded on the voice VLAN.

You can add, change, and remove OUIs, including the default OUIs. The maximum number of OUI entries in the table is 15. The first 3 bytes of the MAC address contain a manufacturer identifier, and the last 3 bytes contain a unique station ID. You must add an OUI prefix in the format AA:BB:CC.

You can add a new OUI, change an existing OUI, and delete an OUI that you no longer need.

To change the OUI table for the voice VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.

3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
   The voice VLAN shows with a telephone icon.
6. In the table in the right pane, click the voice VLAN (you can click anywhere in the row for the voice VLAN).
7. Click the **EDIT** button.
8. In the OUI Table section, click the **OUI Settings** link.
   The Voice VLAN pane displays and shows the OUI table.
9. To add a new OUI, do the following:
   a. Click the **ADD OUI** button.
      The OUI Entry page displays.
   b. Enter the new OUI and description.
   c. Click the **APPLY** button.
      Your settings are saved.
10. To change an existing OUI, do the following:
    a. Select the OUI that you want to change and click the **EDIT** button.
    b. Change the OUI, description, or both.
    c. Click the **APPLY** button.
       Your settings are saved.
11. To delete an OUI that you no longer need, select the OUI and click the **DELETE** button.
    Your settings are saved and the OUI is deleted.
12. Click the **BACK** button.
    The Advanced 802.1Q VLAN pane displays and shows the voice VLAN settings.
13. Click the **APPLY** button.
    Your settings are saved.

Delete an Advanced 802.1Q VLAN

You can delete an advanced 802.1Q VLAN that you no longer need. You cannot delete the default VLAN. You cannot delete a VLAN that is in use as the PVID for a port either. You must first remove the VLAN as the PVID for the port before you can delete the VLAN.

Note: If you deactivate the Advanced 802.1Q VLAN mode, all 802.1Q VLANs are deleted.

To delete an advanced 802.1Q VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
6. In the table in the right pane, click the VLAN that you want to delete (you can click anywhere in the row for the VLAN).
7. Click the **DELETE** button.
   Your settings are saved. The VLAN is deleted.

Deactivate a Port-Based or 802.1Q VLAN Mode and Delete All VLANs

If you activated the Basic Port-Based VLAN mode, Advanced Port-Based VLAN mode, Basic 802.1Q VLAN mode, or Advanced 802.1Q VLAN mode, you can deactivate the VLAN mode and delete the default VLAN and all other VLANs.

To deactivate a VLAN mode and delete all VLANs:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The QOS page displays.
5. From the menu on the left, select **VLAN**.
   The VLAN page displays.
6. In the NO VLANs section, click the **ACTIVATE MODE** button.
   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **CONTINUE** button.
   Your settings are saved, the pop-up window closes, and all VLANs are deleted.

5

Manage the Switch in Your Network

This chapter describes how you can manage the switch in your network.

The chapter contains the following sections:

Manage Switch Discovery Protocols

It is important to know the IP address of the switch so that you can access the local browser interface of the switch. The switch supports Universal Plug and Play (UPnP), Bonjour, and NETGEAR Switch Discovery Protocol (NSDP), which are protocols that can discover the switch. A device that functions in the same network as the switch and that supports one of these protocols can discover the switch and obtain the IP address.

As a security measure, you can disable one or more discovery protocols. However, we recommend that you leave at least one discovery protocol enabled so that a device can discover the switch if the switch IP address changes.

Manage Universal Plug and Play

A Windows-based device that supports Universal Plug and Play (UPnP) can discover the switch in the network so that you can find the switch IP address and log in to the local browser interface of the switch. UPnP is enabled by default. You can disable UPnP for security reasons.

To manage UPnP:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **SWITCH DISCOVERY**.
   The SWITCH DISCOVERY page displays.
6. Enable or disable UPnP by clicking the button in the UPnP section.
   When UPnP is enabled, the button bar displays green.
7. Click the **APPLY** button.
   Your settings are saved.

Manage Bonjour

A Mac OS device that supports Bonjour can discover the switch in the network so that you can find the switch IP address and log in to the local browser interface of the switch. Bonjour is enabled by default. You can disable Bonjour for security reasons.

To manage Bonjour:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **SWITCH DISCOVERY**.
   The SWITCH DISCOVERY page displays.
6. Enable or disable Bonjour by clicking the button in the Bonjour section.
   When Bonjour is enabled, the button bar displays green.
7. Click the **APPLY** button.
   Your settings are saved.

Manage NETGEAR Switch Discovery Protocol

A NETGEAR device or application that supports NETGEAR Switch Discovery Protocol (NSDP) can discover the switch in the network so that you can find the switch IP address and log in to the local browser interface of the switch. NSDP is enabled by default. You can disable NSDP for security reasons.

To manage NSDP:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.

The default password is **password**. The password is case-sensitive.

The HOME page displays.

4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **SWITCH DISCOVERY**.
   The SWITCH DISCOVERY page displays.
6. Enable or disable NSDP by clicking the button in the NSDP section.
   When NSDP is enabled, the button bar displays green.
7. Click the **APPLY** button.
   Your settings are saved.

Set Up Static Link Aggregation

Static link aggregation on the switch allows you to combine multiple Ethernet ports into a single logical link. Your network devices treat the aggregation as if it were a single link. Depending on how link aggregation is set up in your network, the link supports either increased bandwidth (a larger pipe) or fault tolerance (if one port fails, another one takes over).

The switch supports two static LAGs with up to four ports each. That means that one static LAG can support a link of up to 4 Gbps.

Note: The switch does not support Link Aggregation Control Protocol (LACP).

You set up static link aggregation on the switch through a link aggregation group (LAG) in the following order:

1. Set up the LAG on the switch (see Set Up a Link Aggregation Group on page 73).
2. Connect the ports that must be members of the LAG on the switch to the ports that must be members of the LAG on *another* device in your network (see Make a Link Aggregation Connection on page 74).
3. Enable the LAG on the switch (see Enable a Link Aggregation Group on page 74) and on the other device.

Set Up a Link Aggregation Group

You set up static link aggregation on the switch by adding up to four ports to a link aggregation group (LAG) and by enabling the LAG. However, for a LAG to take effect, you first must make sure that all ports that participate in the LAG (that is, the ports on both devices) use the same speed, duplex mode, and flow control setting (see Manage Individual Port Settings on page 39 for information about changing these settings on the switch) and you must set up a physical link aggregation connection (see Make a Link Aggregation Connection on page 74).

After you set up a link aggregation group and make a physical link aggregation connection, you can enable the link aggregation group (see Enable a Link Aggregation Group on page 74).

To set up one or more link aggregation groups on the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **LINK AGGREGATION**.
   The LINK AGGREGATION page displays.
6. To add ports to LAG 1, click two, three, or all port numbers from **1** to **4**.
   A selected port displays purple.
   LAG 1 must consist of at least two ports but can consist of all ports in the range from 1 through 4.
7. To add ports to LAG 2, click two, three, or all port numbers from **5** to **8**.
   A selected port displays purple.
   LAG 2 must consist of at least two ports but can consist of all ports in the range from 5 through 8.
8. Click the **APPLY** button.
   Your settings are saved.

Make a Link Aggregation Connection

Before you make a physical link aggregation connection to another network device (usually a router or another switch) that also supports link aggregation, you must first set up a link aggregation group (LAG) on the switch (see Set Up a Link Aggregation Group on page 73). If you do not, the LAG cannot take effect. Whether a LAG on the switch functions to support increased bandwidth or fault tolerance depends on the LAG configuration on the other network device.

All ports that participate in a LAG (that is, the ports on both devices) must use the same speed, full duplex mode, and flow control setting. For information about changing these settings on the switch, see Manage Individual Port Settings on page 39.

To make link aggregation connections between the switch and another network device:

Using Ethernet cables, connect each port that must be a member of the LAG on the switch to each port that must be a member of the same LAG on another network device.

LAG 1 can include ports 1 through 4. LAG 2 can include ports 5 through 8.

The port numbers on the other network device do not matter as long as the ports on the other network device are members of the same LAG, the LAG consists of the same total number of ports, and the ports use the same speed, full duplex mode, and flow control setting as the ports in the LAG on the switch.

Enable a Link Aggregation Group

After you set up a link aggregation group (see Set Up a Link Aggregation Group on page 73) and make a physical link aggregation connection (see Make a Link Aggregation Connection on page 74), you can enable the link aggregation group.

Note: You must also enable the link aggregation group on the other network device.

To enable a link aggregation group on the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   The login page displays.
3. Enter the switch password.

   The default password is **password**. The password is case-sensitive.

   The HOME page displays.

4. From the menu at the top of the page, select **SWITCHING**.
   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **LINK AGGREGATION**.
   The LINK AGGREGATION page displays.
6. Click the button under LAG 1, the button under LAG 2, or both buttons.
   The button bar for a LAG that is enabled displays green.
7. Click the **APPLY** button.
   Your settings are saved.

Manage Multicast

Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by Class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Internet Group Management Protocol (IGMP) snooping allows the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic rather than to all ports, which could affect network performance.

IGMP snooping helps to optimize multicast performance and is especially useful for bandwidth-intensive IP multicast applications such as online media streaming applications.

Manage IGMP Snooping

Internet Group Management Protocol (IGMP) snooping is enabled by default. Under some circumstances you might want to temporarily disable IGMP snooping.

To manage IGMP snooping:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

The Quality of Service (QoS) page displays.

5. From the menu on the left, select **MULTICAST**.
   The MULTICAST page displays.
6. Enable or disable IGMP snooping by clicking the button in the IGMP Snooping section.
   When IGMP snooping is enabled, the button bar displays green.
7. Click the **APPLY** button.
   Your settings are saved.

Enable a VLAN for IGMP Snooping

You can enable IGMP for a VLAN only if you enabled a port-based VLAN mode or an 802.1Q VLAN mode (see Use VLANS for Traffic Segmentation on page 45).

To enable IGMP snooping for a VLAN:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **MULTICAST**.
   The MULTICAST page displays.
6. In the VLAN ID Enabled for IGMP Snooping section, enter a VLAN ID in the field.
   If you enabled either a port-based VLAN mode or an 802.1Q VLAN mode, the default VLAN for IGMP snooping is VLAN 1.
7. Click the **APPLY** button.
   Your settings are saved.

Manage Blocking of Unknown Multicast Addresses

As a way to limit unnecessary multicast traffic, you can block multicast traffic from unknown multicast addresses. If you do this, the switch forwards multicast traffic only to ports in the multicast group that the switch learned through IGMP snooping. By default, multicast traffic from unknown addresses is allowed.

To manage blocking of unknown multicast addresses:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **MULTICAST**.
   The MULTICAST page displays.
6. Enable or disable the blocking of unknown multicast traffic by clicking the button in the Block Unknown Multicast Address section.
   When the blocking of unknown multicast traffic is enabled, the button bar displays green.
7. Click the **APPLY** button.
   Your settings are saved.

Manage IGMPv3 IP Header Validation

You can enable IGMPv3 IP header validation so that the switch inspects whether IGMPv3 packets conform to the IGMPv3 standard. By default, IGMPv3 IP header validation is disabled. If IGMPv3 IP header validation is enabled, IGMPv3 messages must include a

time-to-live (TTL) value of 1 and a ToS byte of 0xC0 (Internetwork Control). In addition, the router alert IP option (9404) must be set.

Note: If IGMPv3 IP header validation is enabled, switch does not drop IGMPv1 and IGMPv2 traffic but processes this traffic normally.

To manage IGMPv3 IP header validation:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **MULTICAST**.
   The MULTICAST page displays.
6. Enable or disable IGMPv3 IP header validation by clicking the button in the Validate IGMPv3 IP Header section.
   When IGMPv3 IP header validation is enabled, the button bar displays green.
7. Click the **APPLY** button.
   Your settings are saved.

Set Up a Static Router Port for IGMP Snooping

If your network does not include a device that sends IGMP queries, the switch cannot discover the router port dynamically. (The router port is a port on a device in the network that performs IGMP snooping in the network.) In this situation, select one port on the switch as the dedicated static router port for IGMP snooping, allowing all IGMP Join and Leave messages in the network to be forwarded to this port.

To set up a static router port for IGMP snooping:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

The login page displays.

3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.
   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **MULTICAST**.
   The MULTICAST page displays.
6. From the menu in the IGMP Snooping Static Router Port section, select a specific port as the router port or select **Any** to let IGMP Join and Leave messages be sent to every port on the switch.
   Typically, the uplink port (that is, the port that is connected to your router or to the device that provides your Internet connection) serves as the router port.
7. Click the **APPLY** button.
   Your settings are saved.

Change the IP Address of the Switch

By default, the switch receives an IP address from a DHCP server (or a router that functions as a DHCP server) in your network.

To disable the DHCP client of the switch and change the IP address of the switch to a fixed IP address:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **IP Address (DHCP On)**.
   The IP address fields display but you cannot change them yet. The button bar in the DHCP section displays green because the DHCP client of the switch is enabled.

5. Click the button in the DHCP section.
   The button bar displays gray, indicating that the DHCP client of the switch is disabled, and you can now change the IP address fields.
6. Enter the fixed (static) IP address that you want to assign to the switch and the associated subnet mask and gateway IP address.
7. Click the **APPLY** button.
   A pop-up window displays a message.
8. Click the **X** in the pop-up window.
   Your settings are saved. Your switch web session might be disconnected when you change the IP address.

Reenable the DHCP Client of the Switch

If you disabled the DHCP client of the switch and changed the IP address of the switch to a fixed (static) IP address, you can reverse the situation. You can also press the **RESET** button for five seconds (not longer) to reenable DHCP (see Use the RESET Button to Renew the DHCP IP Address or Reenable DHCP on page 88).

To reenable the DHCP client on the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **IP Address (Fixed IP)**.
   The button bar in the DHCP section displays gray because the DHCP client of the switch is disabled.
5. Click the button in the DHCP section.
   The button bar displays green, indicating that the DHCP client of the switch is enabled. You can no longer change the IP address fields.
6. Click the **APPLY** button.
   A pop-up window displays a message.

7. Click the **X** in the pop-up window.

   Your settings are saved. The switch receives an IP address from a DHCP server (or a router that functions as a DHCP server) in your network. Your switch web session might be disconnected when you enable the DHCP client of the switch.

6

Maintain and Monitor the Switch

This chapter describes how you can maintain and monitor the switch.

The chapter contains the following sections:

Manually Check for New Switch Firmware and Update the Switch

You can manually check for the latest firmware version through the local browser interface of the switch, download the firmware, and upload the firmware to the switch. If firmware release notes are available with new firmware, read the release notes to find out if you must reconfigure the switch after updating.

To manually check for new switch firmware and update the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **FIRMWARE**.
   The FIRMWARE page displays. The page also shows the UPDATE FIRMWARE section.
   The displays the current firmware version of the switch.
6. To check if new firmware is available, click the link in the FIRMWARE section.
   A NETGEAR web page opens.
7. If new firmware is available, download the firmware file to your computer.
   If the file does not end in `.bin` or `.image`, you might need to unzip the file. For example, if the file ends in `.rar`, you must unzip the file.
8. In the FIRMWARE UPDATE section, click the purple file icon, navigate to the firmware file that you just downloaded, and select the file.
   An example of a firmware file name is `S8000_V1.0.0.1.bin`.
9. Click the **UPDATE** button.
   A pop-up window displays a warning and the firmware update process starts.

Warning: Do not interrupt the network connection or power to the switch during the firmware update process. Do not disconnect any Ethernet cables or power off the switch until the firmware update process and switch reboot are complete.

Your switch web session is disconnected and you must log back in to the local browser interface.

Manage the Configuration File

The configuration settings of the switch are stored within the switch in a configuration file. You can back up (save) this file to your computer or restore it from your computer to the switch.

Back Up the Switch Configuration

You can save a copy of the current configuration settings. If necessary, you can restore the configuration settings later.

To back up the configuration settings switch of the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **CONFIGURATION FILE**.
   The RESTORE CONFIGURATION page displays.
6. Click the **BACKUP** tab.
   The BACKUP CONFIGURATION page displays.
7. Click the **BACKUP** button.
8. Follow the directions of your browser to save the file.
   The name of the backup file is `S8000.cfg`.

Restore the Switch Configuration

If you backed up the configuration file, you can restore the configuration from this file.

To restore the configuration settings of the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **CONFIGURATION FILE**.
   The RESTORE CONFIGURATION page displays.
6. Click the purple file icon and navigate to and select the saved configuration file.
   The name of the saved configuration file is `S8000.cfg`.
   The **RESTORE** button changes to the **APPLY CONFIGURATION** button.
7. Click the **APPLY CONFIGURATION** button.
   A pop-up window displays a warning.
8. Click the **CONTINUE** button.
   The configuration is uploaded to the switch.

   Warning: Do not interrupt the network connection or power to the switch during the restoration process. Do not disconnect any Ethernet cables or power off the switch until the restoration process and switch reboot are complete.

   Your switch web session is disconnected and you must log back in to the local browser interface.

Return the Switch to Its Factory Default Settings

Under some circumstances (for example, if you lost track of the changes that you made to the switch settings or you move the switch to a different network), you might want to erase the configuration and reset the switch to factory default settings.

To reset the switch to factory default settings, you can either use the **RESET** button on the bottom of the switch or use the reset function in the local browser interface. However, if you changed and lost the password and cannot access the switch, you must use the **RESET** button.

After you reset the switch to factory default settings, the password is password and the switch's DHCP client is enabled. For more information, see Factory Default Settings on page 101.

Use the RESET Button to Reset the Switch

You can use the **RESET** button to return the switch to its factory default settings.

Caution: This process erases all settings that you configured on the switch.

To reset the switch to factory default settings:

1. On the bottom of the switch, locate the recessed **RESET** button.
2. Using a straightened paper clip, press and hold the **RESET** button for more than 10 seconds or until all port LEDs start blinking red.
3. Release the **RESET** button.

   All port LEDs blink red five times and the configuration is reset to factory default settings. When the reset is complete, the switch reboots. This process takes about one minute.

   Warning: Do not interrupt the network connection or power to the switch during the reset process. Do not disconnect any Ethernet cables or power off the switch until the reset process and switch reboot are complete.

Use the Local Browser Interface to Reset the Switch

Caution: This process erases all settings that you configured on the switch.

To reset the switch to factory default settings using the local browser interface:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **FACTORY DEFAULT**.
   The FACTORY DEFAULT page displays.
6. Click the **RESTORE DEFAULT SETTINGS** button.
   A warning pop-up window opens.
7. Click the **CONTINUE** button.
   The switch is reset to factory default settings and reboots.

   Warning: Do not interrupt the network connection or power to the switch during the reset process. Do not disconnect any Ethernet cables or power off the switch until the reset process and switch reboot are complete.

Use the RESET Button to Renew the DHCP IP Address or Reenable DHCP

You can use the **RESET** button to renew the DHCP IP address of the switch or, if DHCP is disabled, reenable DHCP.

To renew the DHCP IP address of the switch or reenable DHCP:

1. On the bottom of the switch, locate the recessed **RESET** button.
2. Using a straightened paper clip, press and hold the **RESET** button for about five seconds or until all port LEDs start blinking blue.

   Warning: Do not hold the **RESET** button for more than 10 seconds to prevent the switch from returning to its factory default settings.

3. Release the **RESET** button.

   All port LEDs blink blue three times and the DHCP IP address of the switch is reenabled.

Control Management Access to the Switch

You can control which IP address or IP addresses can access the switch through the local browser interface for management purposes.

To control management access to the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   The login page displays.

3. Enter the switch password.

   The default password is **password**. The password is case-sensitive.

   The HOME page displays.

4. From the menu at the top of the page, select **SETTINGS**.

   The PRESET MODES page displays.

5. From the menu on the left, select **ACCESS CONTROL**.

   The ACCESS CONTROL page displays.

6. Click the **ADD** button.
7. Specify the IP address or IP addresses:
   - **IP Address**. Enter a single IP address or a network IP address.
     Enter a network IP address in the format x.x.x.0, for example, 192.168.100.0.
   - **Mask**. If you enter a single IP address, enter **255.255.255.255** as the mask. If you enter a network IP address, enter **255.255.255.0** as the mask.
8. Click the **APPLY** button.
   Your settings are saved.
9. To enter more IP addresses, repeat the previous three steps.

Change or Lift Access Restrictions to the Switch

If you set up IP addresses that are allowed to access the switch through the local browser interface for management purposes, you can remove one or more IP addresses, or you can remove all IP addresses and in that way lift access restrictions.

If you lift access restrictions, any IP address can access the local browser interface of the switch. (The user still must enter a password to access the local browser interface.)

To change or lift access restrictions to the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **ACCESS CONTROL**.
   The ACCESS CONTROL page displays.
6. Click the IP address that you want to remove.

The DELETE button displays.

7. Click the **DELETE** button.
   The IP address is removed and can no longer access the local browser interface of the switch.
8. To remove more IP addresses, repeat the previous step.
   If you remove all IP addresses, all access restrictions are lifted and any IP address can access the local browser interface of the switch.

Manage the DoS Prevention Mode

You can enable the Denial of Service (DoS) prevention mode so that the switch automatically blocks malicious packets. By default, this mode is disabled.

To manage the DoS prevention mode:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
   The PRESET MODES page displays.
5. From the menu on the left, select **DOS PREVENTION**.
   The DOS PREVENTION page displays.
6. Enable or disable the DoS prevention mode by clicking the button.
   When the DoS prevention mode is enabled, the button bar displays green.
7. Click the **APPLY** button.
   Your settings are saved.

Manage the Power Saving Mode

The power saving mode enables the IEEE 802.3az Energy Efficient Ethernet (EEE) function, cable length power saving, and link-up and link-down power saving:

- **IEEE 802.3az**. Combines the Energy Efficient Ethernet (EEE) 802.3 MAC sublayer with the 100BASE-TX, 1000BASE-T, and 10GBASE-T physical layers to support operation in Low Power Idle (LPI) mode. When LPI mode is enabled, systems on both sides of the link can disable portions of their functionality and save power during periods of low link utilization.
- **Short cable power saving**. Dynamically detects and adjusts power that is required for the detected cable length.
- **Link-down power saving**. Reduces the power consumption considerably when the network cable is disconnected. When the network cable is reconnected, the switch detects an incoming signal and restores normal power.

By default, the power saving mode is disabled.

To manage the power saving mode on the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, to the right of NETGEAR, click the three-dot icon and select **Power Saving**.
   The POWER SAVING pop-up window opens.
5. Enable or disable the power saving mode by clicking the button.
   When the power saving mode is enabled, the button bar displays green.
   (You do not need to click an **APPLY** button.)

Control the Port LEDs

You can turn the blue port LEDs and Power LED on the switch on and off, either by pressing the **LED** button on the back of the switch with the light icon next to port 8, or by using the local browser interface.

By default, a port LED lights when you connect a powered-on device to the port. When the switch functions with its LEDs off, we refer to it as Stealth Mode.

To control the port LEDs through the local browser interface:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **Port LEDs**.
   The **Port LEDs** button displays.
5. Disable or enable the port LEDs by clicking the button.
   When the port LEDs are enabled, the button bar displays green. When the ports LEDs are disabled (Stealth Mode), the button bar displays gray.
6. Click the **APPLY** button.
   Your settings are saved.

Control the Power LED

You can turn the blue Power LED and port LEDs on the switch on and off, either by pressing the **LED** button on the back of the switch with the light icon next to port 8, or by using the local browser interface.

By default, the Power LED lights when you start the switch. When the switch functions with its LEDs off, we refer to it as Stealth Mode.

To control the Power LED through the local browser interface:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **Power LED**.
   The **Power LED** button displays.
5. Disable or enable the Power LED by clicking the button.
   When the Power LEDs is enabled, the button bar displays green. When the Power LEDs is disabled (Stealth Mode), the button bar displays gray.
6. Click the **APPLY** button.
   Your settings are saved.

Change the Switch Device Name

By default, the device name of the switch is Nighthawk S8000. This device name shows in, for example, Windows Explorer and Bonjour. You can change the device name, which can be up to 20 characters.

To change the device name of the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.

3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **System Info**.
   The System Info fields display.
5. In the **Switch Name** field, enter a new name for the switch.
6. Click the **APPLY** button.
   Your settings are saved.

View System Information

You can view basic information about the switch, such as the firmware version, switch name, MAC address, serial number, and model number.

To view basic information about the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. Select **System Info**.
   The system information fields display.

View Switch Connections

You can see the number of connections that are established on the switch.

To see the number of connections on the switch:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

The login page displays.

3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.

   The HOME page displays.

   The switch connections show in the upper left of the page.

View the Status of a Port

You can view the status of and details about a port.

To view the status of a port:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.

   The HOME page displays.

   The PORT STATUS pane displays on the right or the bottom of the HOME page, depending on the size of your browser window.

   A port that is in use shows as UP. A port that is not in use shows as AVAILABLE.
4. To view details about a port, select the port.
   The pane displays detailed information about the port.

   If the QoS mode on the switch is Port-based (the default setting), the **Priority** field displays on the page. If the QoS mode is 802.1P/DSCP, the **Priority** field does not display.

   For information about setting rate limits for incoming and outgoing traffic, setting the port priority (if the QoS mode on the switch is Port-based), setting the port speed (by default, the speed is set automatically), enabling flow control, and changing the port name label, see Manage Individual Port Settings on page 39.

7

Diagnostics and Troubleshooting

This chapter provides information to help you diagnose and solve problems that you might experience with the switch. If you do not find the solution here, check the NETGEAR support site at netgear.com/support for product and contact information.

The chapter contains the following sections:

Test a Cable Connection

You can use the cable diagnostic feature to easily find out the health status of network cables. If any problems exist, this feature helps quickly locate the point where the cabling fails, allowing connectivity issues to be fixed much faster, potentially saving technicians hours of troubleshooting.

If an error is detected, the distance at which the fault is detected is stated in feet. (This is the distance from the port.)

To test one or more cable connections:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, select **DIAGNOSTICS**.
   The SELECT PORTS TO TEST page displays.
5. Select one or more ports to test by clicking the numbers.
   Selected ports display purple.
6. Click the **NEXT** button.
   The switch sends a signal to the cables for the selected ports, causing the ports to be temporarily out of service and traffic on the ports to be temporarily affected.
   When the test is complete, the results are displayed.
   If a fault was detected, the distance (from the switch port) to that fault is displayed in feet.
7. Click the **DONE** button.
   The SELECT PORTS TO TEST page displays again.

Reboot the Switch From the Local Browser Interface

You can reboot the switch remotely from the local browser interface.

To reboot the switch from the local browser interface:

1. Open a web browser from a computer that is connected to the same network as the switch or to the switch directly through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.
   The login page displays.
3. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The HOME page displays.
4. From the menu at the top of the page, to the right of NETGEAR, click the three-dot icon and select **Reboot Switch**.
   A pop-up window displays.
5. Click the **CONTINUE** button.
   The switch reboots. Your switch web session is disconnected and you must log back in to the local browser interface.

Detect a Network Loop

When a network loop occurs, the switch, and possibly the router to which the switch is connected, could become very sluggish or traffic on your network could come to a halt.

By default, loop detection is enabled on the switch. (You cannot disable it.)

If the switch detects a network loop, all port LEDs for the ports that are being used blink blue fast. This visual warning allows you to determine which ports are involved in the loop and remove the loop.

Resolve a Subnet Conflict to Access the Switch

If you power on the switch before you connect it to a network that includes a DHCP server (or a router that functions as a DHCP server), the switch uses its own default IP address of 192.168.0.239. This subnet might be different from the subnet used in your network.

To fix this subnet conflict:

1. Disconnect the Ethernet cable between the switch and your network.
2. Unplug the switch's power adapter.
3. Reconnect the Ethernet cable between the switch and your network.
4. Plug the switch's power adapter into an electrical outlet.
   The switch powers on. The DHCP server in the network discovers the switch and assigns it an IP address that is in the correct subnet for the network.

A

Factory Default Settings and Technical Specifications

This appendix contains the following sections:

Factory Default Settings

You can return the switch to its factory default settings. Use the end of a paper clip or some other similar object to press and hold the **RESET** button on the bottom panel of the switch for at least five seconds. The switch resets and returns to the factory settings that are shown in the following table.

Table 3. Factory default settings

Feature	Default Setting
Access point login and discovery	
IP address	**DHCP client**. Enabled. That is, an IP address is issued to the switch by a DHCP server in the network. **Standalone IP address**. 192.168.0.239 with subnet mask 255.255.255.0.
Login password	password
Switch discovery protocols	All enabled (UPnP, Bonjour, and NSDP)
QoS	
QoS port assignments	**Port 1**. Gaming **Port 2**. Media streaming **Port 8**. Uplink
QoS mode	Port-based
Port priority	High (all ports)
Port rate limits	None (for all ports)
Flow control	Disabled
Broadcast filtering	Disabled
Port storm control rate limits	None (for all ports)
Multicast	
IGMP snooping	Enabled
Blocking of unknown multicast addresses	Disabled
VLAN ID enabled for IGMP snooping	None

Table 3. Factory default settings (Continued)

Feature	Default Setting
IGMPv3 IP header validation	Disabled
Static router port for IGMP snooping	None
Ports and LEDs	
Port link speed	Autonegotiation
Port LEDs	Enabled
Power LED	Enabled
Other features	
Link aggregation	No LAGs configured
Access control	Disabled
DoS prevention	Disabled
Power saving mode	Disabled
Loop detection	Enabled (nonconfigurable)
Jumbo frames	Enabled (nonconfigurable)

Technical Specifications

The following table shows the technical specifications of the switch.

Table 4. Technical specifications

Feature	Description
IEEE standards	IEEE 802.3 Ethernet IEEE 802.3x Full-Duplex Flow Control IEEE 802.3u 100BASE-TX IEEE 802.1p Class of Service IEEE 802.3ab 1000BASE-T IEEE 802.3az Energy Efficient Ethernet (EEE) IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging
Network connectors	RJ-45, supporting 10BASE-T, 100BASE-TX, or 1000BASE-T

Table 4. Technical specifications (Continued)

Feature	Description
Ethernet ports	8
Power adapter	12V, 1.0A (The plug is localized to the country of sale.) Power consumption from 0.8W to 3.8W
Power consumption	From 0.8W to 3.8W
Dimensions (W x D x H)	7.7 x 5.9 x 1.6 in. (195 x 149 x 40 mm)
Weight	1.63 lb (0.74 kg)
Operating temperature	32° to 104°F (0° to 40°C)
Operating humidity	90% maximum relative humidity, noncondensing
Operating altitude	10,000 ft (3,000 m) maximum
Storage temperature	–40° to 158°F (–40° to 70°C)
Storage humidity	95% maximum relative humidity, noncondensing
Storage altitude	10,000 ft (3,000 m) maximum
Safety certifications	UL, CB, CE LVD, EAC

B

Additional Switch Discovery and Access Information

This appendix provides additional information about how you can discover and access the switch in your network.

The appendix contains one section:

- Access the Switch From Any Computer

Access the Switch From Any Computer

This procedure requires you to use an IP scanner application. Such applications are available on the Internet, and some of them are free of charge.

To discover the switch IP address and access the switch from a computer:

1. From a computer that is connected to your network, run the IP scanner application in your network.

   The IP address that is assigned to the switch displays in the IP scanner application.

   Note: You can also access the DHCP server (or the router that functions as a DHCP server) in your network and determine the IP address that is assigned to the switch.

2. Open a web browser, and in the address bar, type the IP address of the switch.

   The login page of the local browser interface opens.

3. Enter the switch password.

   The default password is **password**. The password is case-sensitive.

   The HOME page displays.

   The right pane (or, depending on the size of your browser window, the middle pane) shows the IP address that is assigned to the switch.

   Tip: You can copy and paste the IP address into a new shortcut or bookmark it for quick access on your computer or mobile device. However, if you reboot the switch, a dynamic IP address (assigned by a DHCP server) might change and the bookmark might no longer link to the login page for the switch. In this case, you must repeat Step 1 through Step 3 so that you can discover the new IP address of the switch in the network and update your bookmark accordingly. You can also set up a fixed (static) IP address for the switch (see Set Up a Fixed IP Address for the Switch on page 21) to make sure that the new bookmark always links to the login page for the switch, even after you reboot the switch.