NETGEAR®

Nighthawk Pro Gaming SX10 8-Port Gigabit Ethernet Switch with 2-Port 10G/Multi-Gig Ethernet

User Manual

Model GS810EMX

December 2017
202-11833-01

350 E. Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for purchasing this NETGEAR product. You can visit *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.

Conformity

For the current EU Declaration of Conformity, visit *http://kb.netgear.com/app/answers/detail/a_id/11621*.

Compliance

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

See the regulatory compliance document before connecting the power supply.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11833-01	December 2017	First publication.

Contents

Chapter 1 Hardware Overview of the Switch

Chapter 2 Install and Access the Switch in Your Network

Chapter 3 Optimize the Switch Performance

Chapter 4 Use VLANS for Traffic Segmentation

Chapter 5 Manage the Switch in Your Network

Chapter 6 Maintain and Monitor the Switch

Chapter 7 Diagnostics and Troubleshooting

Appendix A Factory Default Settings and Technical Specifications

Hardware Overview of the Switch

1

The NETGEAR Nighthawk® Pro Gaming SX10 8-Port Gigabit Ethernet Switch with 2-Port 10G/Multi-Gig Ethernet (GS810EMX), in this manual referred to as the switch, provides high-speed (up to 10G) and high-performance switching for multiplayer, online, or VR gaming and 4K resolution HD and UHD (ultra-high-definition) television media streaming.

To facilitate traffic segmentation, you can group ports in VLANs using either port-based or 802.1Q criteria. 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. You can view upload and download times for individual gaming devices and block or give high priority to any such devices. The switch supports IGMP snooping for multicast operation and link aggregation for a connection to link aggregation–enabled devices such as ReadyNAS.

The chapter contains the following sections:

- *Related Documentation*
- *Switch Package Contents*
- *Status LEDs*
- *Back Panel*
- *Switch Label*

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 *downloadcenter.netgear.com*. 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 *downloadcenter.netgear.com*:

- 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.

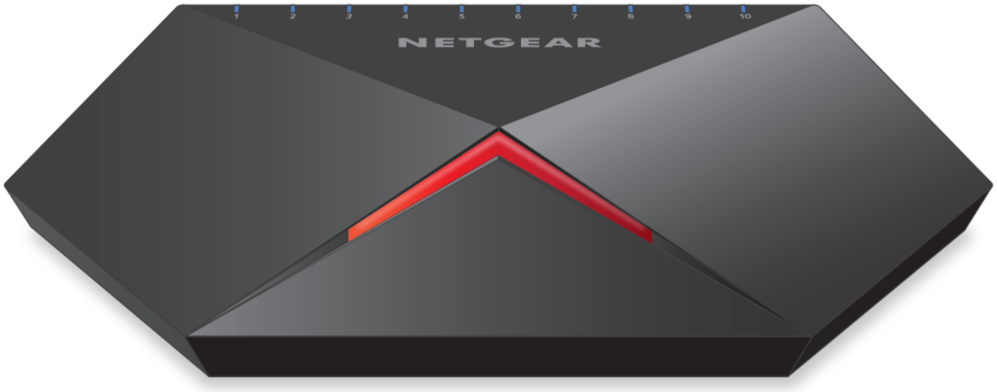


Figure 1. Power LED

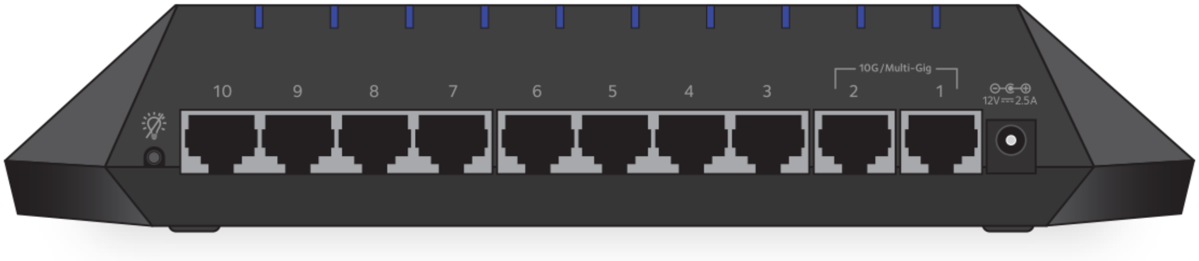


Figure 2. Port LEDs

Table 1. LED descriptions

<table>
<tr><th>LED</th><th colspan="2">Description</th></tr>
<tr><td>Power LED</td><td colspan="2">**Off**. No power is supplied to the switch or the switch functions in Quiet mode with its Power LED disabled (see *Manage the LEDs* on page 69).
Solid orange (default mode). Power is supplied to the switch and the switch is ready for operation.</td></tr>
<tr><td rowspan="6">Port LEDs (1 through 10)</td><td colspan="2">**Off**. No link with a powered-on device is detected or the active ports function in Quiet mode with their port LEDs disabled (see *Manage the LEDs* on page 69).
Solid. A link with a powered-on device is detected. The LED color depends on the color scheme.
Blinking. Traffic is detected. The LED color depends on the color scheme.
Solid Red. The port is part of a network loop. For more information, see *Manage Loop Prevention* on page 76 and *Hardware Troubleshooting Chart* on page 80.</td></tr>
<tr><td colspan="2">In the standard color scheme for the Standard Preset mode, which is the default mode, the port LEDs use the following colors to indicate speed:</td></tr>
<tr><td>●</td><td>**Blue**. 1G or 100M connection (ports 1 through 10).</td></tr>
<tr><td>●</td><td>**Mauve**. 2.5 connection (ports 1 and 2 only).</td></tr>
<tr><td>●</td><td>**Violet**. 5G connection (ports 1 and 2 only).</td></tr>
<tr><td>●</td><td>**Purple**. 10G connection (ports 1 and 2 only).</td></tr>
</table>

The switch functions with the following default color schemes, which you can customize:

- **Standard color scheme**. In the Standard Preset mode (which is the default mode), the switch uses a color scheme with a purple and dark blue color palette. The Power LED is orange.
- **Gaming color scheme**. In the Gaming Preset mode, the switch uses a color scheme with a yellow and green color palette. The Power LED is green.
- **Streaming color scheme**. In the Media Streaming Preset mode, the switch uses a color scheme with a light blue color palette. The Power LED is light blue.

For information about using preset modes, see *Apply a Performance Preset Mode* on page 24.

For information about controlling the LEDs, including the LED colors, see *Manage the LEDs* on page 69.

Back Panel

The back panel of the switch provides the **LED** button, eight Gigabit Ethernet ports, two 10 Gigabit/Multi-Gig Ethernet ports, and the DC power connector. The port LEDs are also located on the back panel.

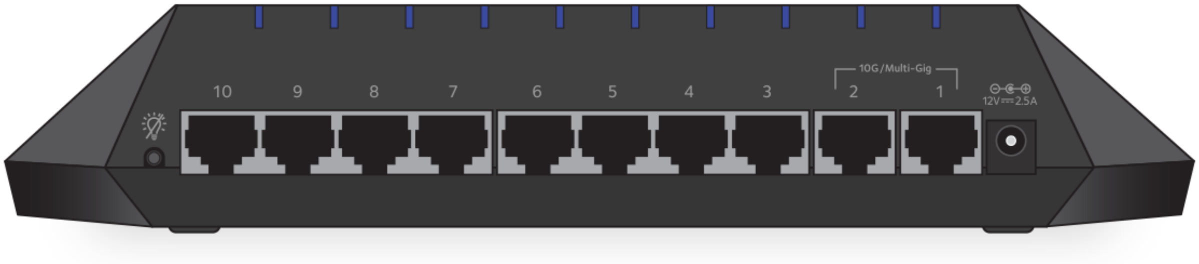


Figure 3. Switch back panel

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

- **DC power connector**. One 12V, 2.5A DC connector for the power adapter.
- **10 Gigabit/Multi-Gig Ethernet ports**. Two 10G ports that also support 5G, 2.5G, 1G, and 100M speeds. These ports are numbered 1 and 2.
  - **Port 1**. We recommend that you use this port as the uplink and connect it to a LAN port on a router that is connected to the Internet.
  - **Port 2**. Connect this port to a high-speed device such as another switch or high-speed NAS.

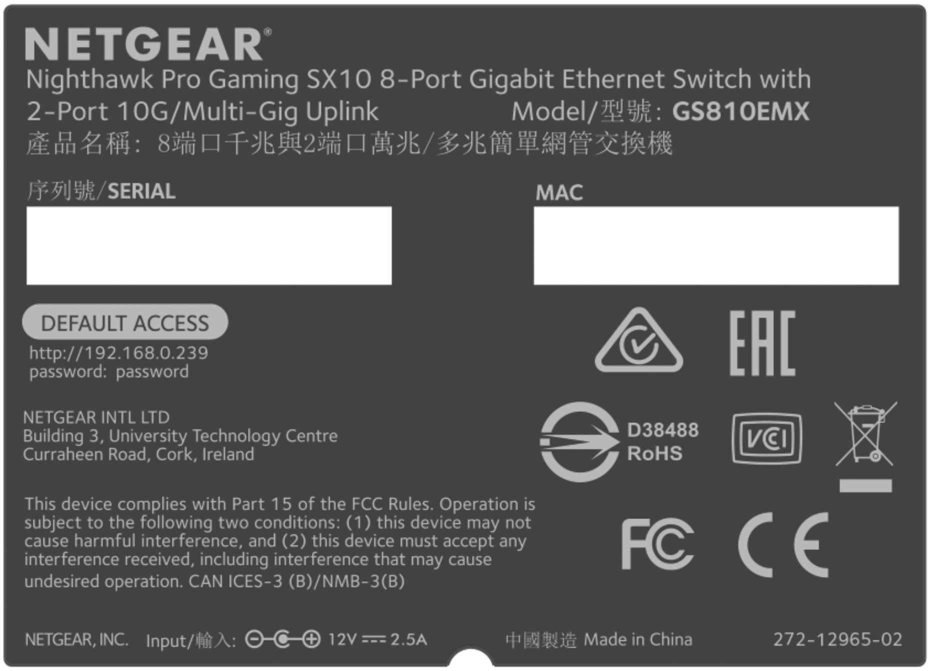
Note Port 1 and port 2 support 10G, 5G, and 2.5G speeds only if your router and Internet connection support these speeds. Otherwise, these ports operate at 1G speed.

- **Gigabit Ethernet ports**. Eight Gigabit Ethernet RJ-45 LAN ports that support 1G and 100M speeds. These ports are numbered 3 through 10.
  - **Ports 3 through 8**. We recommend that you connect these ports to your network devices, other than your main media streaming device (see port 9) and main gaming device (see port 10).
  - **Ports 9**. We recommend that you connect this port to your main media streaming device so that you can use the Media Streaming Preset mode (see *Apply the Media Streaming Preset Mode* on page 25).
  - **Port 10**. We recommend that you connect this port to your main gaming device so that you can use the Gaming Preset mode (see *Apply the Gaming Preset Mode* on page 24).
- **LED button**. One button to turn the port LEDs on and off. When the ports are turned off, we refer to that mode as Quiet mode.

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 *Use the RESET Button to Reset the Switch* on page 66.

Switch Label

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



NETGEAR®

Nighthawk Pro Gaming SX10 8-Port Gigabit Ethernet Switch with 2-Port 10G/Multi-Gig Uplink Model/型號: **GS810EMX**

產品名稱: 8端口千兆與2端口萬兆/多兆簡單網管交換機

序列號/**SERIAL**

MAC

DEFAULT ACCESS

http://192.168.0.239
password: password

NETGEAR INTL LTD
Building 3, University Technology Centre
Curraheen Road, Cork, Ireland

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. CAN ICES-3 (B)/NMB-3(B)

D38488
RoHS

NETGEAR, INC. Input/輸入: ⊖-◐-⊕ 12V ⎓ 2.5A 中國製造 Made in China 272-12965-02

Figure 4. Switch label

Install and Access the Switch in Your Network

2

This chapter describes how to 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. Sample connections

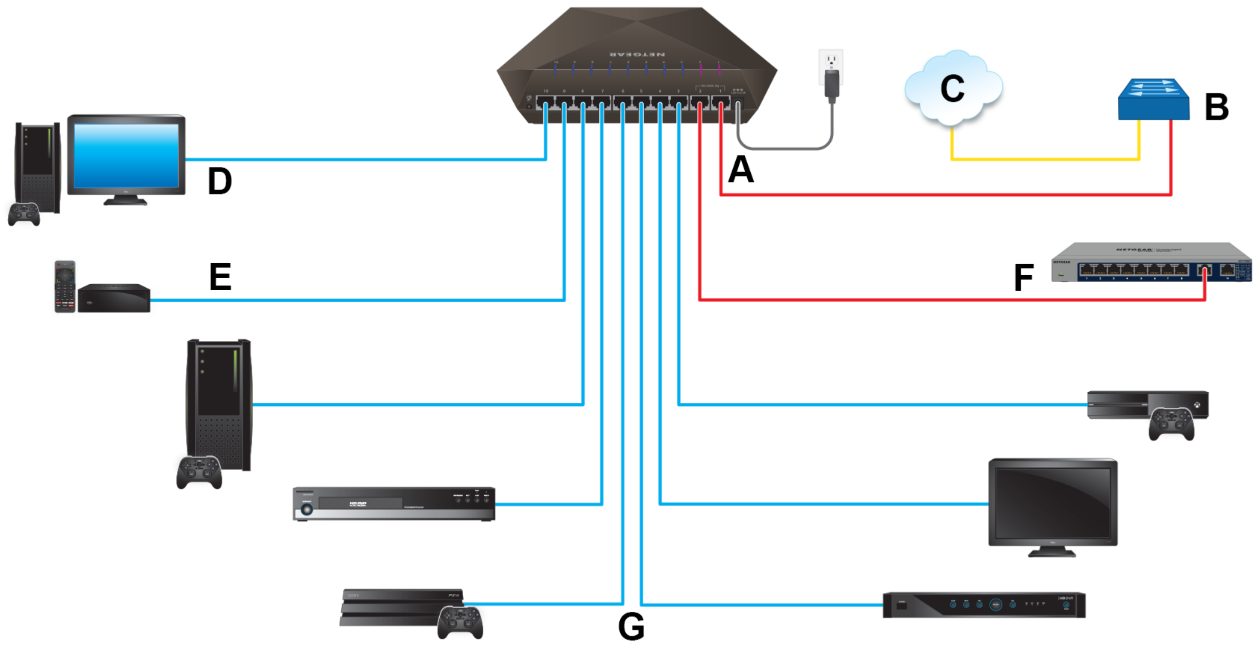


Table 2. Figure components

Letter	Description	Letter	Description
A	GS810EMX switch	E	Main media streaming device
B	Network router	F	High-speed device such as another switch
C	Internet	G	Other network devices
D	Main gaming device		
Red lines indicate 10G (or 5G or 2.5G) connections. Blue lines indicate 1G connections. A yellow line indicates a direct Internet connection.			

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

1. Connect LAN port 1 on the switch (A) to a LAN port on a router (B) that is connected to the Internet (C).

   Port 1 and port 2 support 10G, 5G, and 2.5G speeds only if your router and Internet connection support these speeds. Otherwise, these ports operate at 1G speed.

2. On the switch, connect your devices as follows:

- Connect your main gaming device to port 10 (D). We recommend this port for the one-touch Media Streaming Preset mode (see *Apply the Media Streaming Preset Mode* on page 25).
- Connect your main streaming device to port 9 (E). We recommend this port for the one-touch Gaming Preset mode (see *Apply the Gaming Preset Mode* on page 24).
- Connect a high-speed device such as another switch or a high-speed NAS to port 2 (F).
- Connect all other devices (including additional gaming and streaming devices) to remaining ports 3 through 9 (G).

3. Connect the power adapter to the switch and plug the power adapter into an electrical outlet.

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

Methods to Discover and Access the Switch

You can use any of the following methods to discover the switch in your network and 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 (see *Access the Switch and Discover the IP Address of the Switch* on page 13).
- **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 19).
- **ProSAFE Plus Utility**. Install the NETGEAR ProSAFE® Plus Utility on a Windows-based computer and use the utility to discover the switch in your network (see *Use the NETGEAR ProSAFE Plus Utility to Discover the Switch* on page 20). You cannot perform basic configurations using the ProSAFE Plus Utility. That is, you can only discover the switch in your network. To configure the switch, use the local browser interface of switch.

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 16.

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 SX10 switch.
5. Double-click **Nighthawk SX10 (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 16) 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 15.

► **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 SX10 (xx:xx:xx:xx:xx:xx)**
   - **Bookmarks > Bonjour > Webpages Nighthawk SX10 (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 16) 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/gs810emx.aspx#download*.

   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 **Setup.exe** file (for example, `NetgearSDT-V1.1.115_Win_x64_Setup.exe)`, 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 16) 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 17).
- **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 18).

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.

4. In the SYSTEM INFO pane, select **DHCP**.

   The button 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 displays white, 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.
6. In the SYSTEM INFO pane, select **DHCP**.

   The button 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 displays white, 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 12.
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.

Use the NETGEAR ProSAFE Plus Utility to Discover the Switch

For easiest access, we recommend that you cable the switch to a network with a router or DHCP server that assigns IP addresses, power on the switch, and then use a computer that is connected to the same network as the switch.

The NETGEAR ProSAFE Plus Utility runs on Windows-based computers and lets you discover the switch in your network, after which you can access the local browser interface of the switch.

Note The ProSAFE Plus Utility requires WinPcap and Adobe Air. If WinPcap and Adobe Air are not detected during the ProSAFE Plus Utility installation, you are prompted to allow them to be installed.

To install the ProSAFE Plus Utility, use the utility to discover the switch in your network, and access the local browser interface of the switch:

1. Download the ProSAFE Plus Utility by visiting *netgear.com/support/product/PCU*.

   You must use ProSAFE Plus Utility version 2.5.3 or a later version.

2. Temporarily disable the firewall, Internet security, antivirus programs, or all of these on the computer that you use to configure the switch.

   Note Instead of disabling security services, you can also configure your computer’s security software to allow broadcast UDP packets to go through UDP remote and source (local and destination) ports 63321 through 63324. To allow this traffic, you can create a rule in your computer’s security software.

3. Unzip the ProSAFE Plus Utility files, double-click the **.exe** file (for example, `ProSAFE Plus Utility 2.5.3.exe)`, and install the program on your computer.

   The installation process places a **ProSAFE Plus Utility** icon on your desktop.

4. If you temporarily disabled any security services, reenable those services.

   Note We recommend that you restart your computer after installing the ProSAFE Plus Utility.

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 ProSAFE Plus Utility by double-clicking the **ProSAFE Plus Utility** icon on your desktop.

The discovery process initiates and completes automatically and the configuration home page displays a list of Smart Managed Plus Switches that the utility discovers on the local network.

For each switch, the utility displays the IP address.

8. Open a web browser.
9. Enter the IP address that is assigned to the switch.

   The login page displays.

10. Enter the switch password.

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

    The HOME page displays.

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 **Old 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

Registering the switch allows you to receive email alerts and streamlines the technical support process. For you to register the switch, the switch must be connected to the Internet.

►To register 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 **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.

Optimize the Switch Performance

3

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 28).

A preset mode affects the Quality of Service (QoS), port prioritization, rate limiting, and other features for the ports and 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 the uplink to your router to port 1 and your gaming device to port 10.

Applying the Gaming Preset mode does the following:

- Sets the QoS port priority for ports 1 and 10 to High(P7) (for more information, see *Set the Priority for a Port* on page 35).
- Sets the QoS port priority for ports 2 through 9 to Low(P0) (for more information, see *Set the Priority for a Port* on page 35).
- Enables IGMP snooping for the switch (for more information, see *Manage IGMP Snooping* on page 55).
- Disables flow control for all ports (for more information, *Manage Flow Control for a Port* on page 36).
- Disables power saving for the switch (for more information, see *Manage the Power Saving Mode* on page 68).
- Sets the QoS mode to Port-Based (for more information, see *Use Port-Based Quality of Service and Set Port Priorities* on page 31).
- Disables rate limiting for all ports (for more information, see *Set Rate Limits for a Port* on page 35).
- Sets the LEDs to the gaming color scheme (for more information, see *Manage the LEDs* on page 69).

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 28) 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 **SETTINGS**.

The PRESET MODES page displays.

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 Preset mode, be sure that you connect the uplink to your router to port 1 and your media streaming device to port 9.

Applying the Media Streaming Preset mode does the following:

- Sets the QoS port priority for ports 1 and 9 to High(P7) (for more information, see *Set the Priority for a Port* on page 35).
- Sets the QoS port priority for ports 2 through 8 and port 10 to Low(P0) (for more information, see *Set the Priority for a Port* on page 35).
- Enables IGMP snooping for the switch (for more information, see *Manage IGMP Snooping* on page 55).
- Disables flow control for all ports (for more information, *Manage Flow Control for a Port* on page 36).
- Disables power saving for the switch (for more information, see *Manage the Power Saving Mode* on page 68).
- Sets the QoS mode to Port-Based (for more information, see *Use Port-Based Quality of Service and Set Port Priorities* on page 31).
- Disables rate limiting for all ports (for more information, see *Set Rate Limits for a Port* on page 35).
- Sets the LEDs to the streaming color scheme (for more information, see *Manage the LEDs* on page 69).

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 28) 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 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 priority.

Applying the Standard Preset mode does the following:

- Sets the QoS port priority for all ports to Medium(P4) (for more information, see *Set the Priority for a Port* on page 35.
- Enables IGMP snooping for the switch (for more information, see *Manage IGMP Snooping* on page 55).
- Disables flow control for all ports (for more information, *Manage Flow Control for a Port* on page 36).
- Disables power saving for the switch (for more information, see *Manage the Power Saving Mode* on page 68).
- Sets the QoS mode to Port-Based (for more information, see *Use Port-Based Quality of Service and Set Port Priorities* on page 31).
- Disables rate limiting for all ports (for more information, see *Set Rate Limits for a Port* on page 35).
- Sets the LEDs to the standard color scheme (for more information, see *Manage the LEDs* on page 69).

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

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

5. Select **STANDARD PRESET**.

   The APPLY STANDARD PRESET section shows the settings for the Standard Preset mode.

6. Click the **APPLY** button.

Your settings are saved.

Monitor the Gaming Traffic and Optimize the Gaming Settings

You can monitor the downloaded and uploaded traffic on the ports. The traffic is presented in graphs that show the amount of traffic and achieved traffic speed in Mbps over a period that you can select, from 5 minutes, 30 minutes, 1 hour, to 10 hours. By default, traffic for all ports is displayed, but you can manually exclude ports from the graphs.

While monitoring, with two clicks, you can optimize the gaming settings by assigning the highest priority to an individual port or blocking an individual port.

➤To monitor the gaming traffic and optimize the gaming settings:

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 **GAMING**.

   The page shows the UPLOAD TIMELINE, DOWNLOAD TIMELINE, and DEVICES panes.

   The UPLOAD TIMELINE pane displays a graph that shows the amount of uploaded traffic and achieved traffic speed in Mbps over a period. This traffic is also referred to as outgoing, egress, or transmitted (Tx) traffic.

   The DOWNLOAD TIMELINE pane displays a graph that shows the amount of downloaded traffic and achieved traffic speed in Mbps over a period. This traffic is also referred to as incoming, ingress, or received (Rx) traffic.

   Note For information about the DEVICES pane, see *Set the Priority for a Port* on page 35.

5. To change the period over which traffic is shown, select the Interval **5m** (5 minutes), **30m** (30 minutes), **1h** (1 hour), or **10h** (10 hours) radio button above the graph.
6. To exclude an individual port from a graph, under the Time (seconds) bar of the graph, click the rectangular block for an individual port.

   The port number next to the block is crossed out and the traffic information for the port is exuded from the graph.

7. To optimize the gaming setting by either reprioritizing or blocking an individual port, do the following:

a. Right-click the small square port icon at the bottom of the graph.
This is not the larger rectangular port block under the Time (seconds) bar of the graph, but the smaller square port icon below that.
A pop-up menu opens.

b. Make one of the following selections:

   - **Block**. The port is blocked, that is, shut down. No traffic can go through the port.
     For information about unblocking the port, see *Unblock and Reenable a Port* on page 38.
   - **Set to Highest Priority**. The port is set to the highest priority.
     Whether the switch functions in the Port-Based QoS mode or the 802.1P/DSCP QoS mode, you can set the port to the highest priority. For information about reprioritizing the port to a specific priority, see *Set the Priority for a Port* on page 35.

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, rate limiting, and the priorities of the individual ports.

The switch lets you save two custom preset modes. You can also rename or delete these custom preset modes.

Save Your Quality of Service Settings as a Custom Preset Mode

You can save your current Quality of Service (QoS) settings as a custom preset mode that you can reapply later.

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

   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 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.

Apply a Custom Preset Mode

If you previously saved QoS, port prioritization, multicast, flow control, IGMP snooping, and rate limiting settings as a custom preset mode (see *Save Your Quality of Service Settings as a Custom Preset Mode* on page 28), you can apply the preset mode.

To apply a previously saved 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. From the menu at the top of the page, select **SETTINGS**.

   The PRESET MODES page displays. The **LOAD** tab is automatically selected.
5. Select a custom preset mode.

   The PREVIEW section shows the settings for the custom preset mode.
6. Click the **APPLY** button.

   Your settings are saved.

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

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

5. Click the **SAVE** tab.
6. Select the Slot **1** or **2** button.
7. In the **Preset 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. You cannot delete the default Standard Preset mode.

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

   The PRESET MODES page displays. The **LOAD** tab is automatically selected.
5. Select a custom preset mode.

   The PREVIEW section shows the settings for the custom preset mode.
6. Click the **DELETE** button.

   Your settings are saved. The custom preset mode is removed from the PRESET MODES page.

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 to low with priority 0, low with priority 1, normal with priority 2, normal with priority 3, medium with priority 4, medium with priority 5, high with priority 6, or high with priority 7 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.

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 28.

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 high priority (P7 or P6) before traffic from ports with a medium (P5 or P4), normal (P3 or P2), or low priority (P1 or P0). Similarly, the switch services traffic from ports with a medium priority before traffic from ports with a normal or low priority and traffic from ports with a normal priority before traffic from ports with a 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 (ingress) traffic on that port. The switch transmits traffic from a port at the rate that you set for outgoing (egress) traffic on that port. You can select each rate limit as a predefined data transfer threshold from 1 Mbit/s to 500 Mbit/s.

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 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 34.

6. To set the port priorities, do the following:

   a. Click the **PRIORITY** tab.

   b. Click the edit icon.
      The port priority settings become available.

   c. For each port for which you want to set the priority, select a settings from **Low(P0)** to **High(P7)** from the individual menu for the port.

   d. Click the **APPLY** button.
      Your settings are saved.

7. To set rate limits, do the following:

   a. Click the **RATE LIMITS** tab.

   b. Click the edit icon.
      The rate limit settings become available.

   c. For each port for which you want to set rate limits, select the rate in Mbit/s from the individual **Ingress** and **Egress** menus for the port.
      The default selection is No Limit.

   d. Click the **APPLY** button.
      Your settings are saved.

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 1 Mbit/s to 500 Mbit/s.

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 28.

▶ 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 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 34.

6. To set rate limits, do the following:

   a. Click the **RATE LIMITS** tab.

   b. Click the edit icon.
   The rate limit settings become available.

   c. For each port for which you want to set rate limits, select the rate in Mbit/s from the individual **Ingress** and **Egress** menus for the port.
   The default selection is No Limit.

   d. Click the **APPLY** button.
   Your settings are saved.

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 in a VLAN 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 1 Mbit/s to 500 Mbit/s.

▶ **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 **SWITCHING**.

   The 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, and the **STORM CONTROL RATE** tab displays.
7. To set storm control rate limits, do the following:

   a. Click the **STORM CONTROL RATE** tab.

   b. Click the edit icon.
   The storm control rate settings become available.

   c. For each port for which you want to set storm control rate limits, select the rate in Mbit/s from the individual menu for the port.
   The default selection is No Limit.

   d. Click the **APPLY** button.
   Your settings are saved.

Manage Individual Port Settings

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

Set the Priority for a Port

Port-based priority is the default QoS mode on the switch. In this QoS mode, you can set the priority for a port.

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 31).

The switch services traffic from ports with a high priority (P7 or P6) before traffic from ports with a medium (P5 or P4), normal (P3 or P2), or low priority (P1 or P0). Similarly, the switch services traffic from ports with a medium priority before traffic from ports with a normal or low priority and traffic from ports with a normal priority before traffic from ports with a low priority. If severe network congestion occurs, the switch might drop packets with a low priority.

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

   The page shows the UPLOAD TIME, DOWNLOAD TIME, and DEVICES panes.
5. In the DEVICES pane, click the star icon for the port.

   A pop-up menu displays the priorities.
6. Select a priority by clicking the associated star icon in the pop-up menu.

   The pop-up menu closes and your settings are saved.

   (You do not need to click an **APPLY** button.)

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 30).

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 CONNECTED. A port that is not in use shows as AVAILABLE. A port that is disabled shows as DISABLED.
4. Select the port.

   The pane displays detailed information about the port.
5. Click the **EDIT** button.

   The settings for the selected port become available.
6. From the **Ingress Port Limit** menu, **Egress Port Limit** menu, or both, select the rate in Mbit/s.

   The default selection is No Limit.
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 CONNECTED. A port that is not in use shows as AVAILABLE. A port that is disabled shows as DISABLED.

4. Select the port.

   The pane displays detailed information about the port.

5. Click the **EDIT** button.

   The settings for the selected port become available.

6. Click the **Flow Control** 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 CONNECTED. A port that is not in use shows as AVAILABLE. A port that is disabled shows as DISABLED.

4. Select the port.

   The pane displays detailed information about the port.

5. Click the **EDIT** button.

   The settings for the selected port become available.

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.
  This option is not available for ports 1 and 2.
- **10M Full**. The port is forced to function at 10 Mbps with full-duplex.
  This option is not available for ports 1 and 2.
- **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 For ports 3 through 10, you cannot select Gigabit Ethernet as the port speed. For ports 1 and 2, you cannot select 1G, 2.5G, 5G, or 10G 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, or for ports 1 and 2, a higher speed, if the linked device supports that speed.

7. Click the **APPLY** button.

   Your settings are saved.

Unblock and Reenable a Port

After you block a port or a port becomes disabled, you can unblock and reenable the port.

►To unblock and reenable 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.

   A port that is blocked shows as DISABLED.
4. Select the port.

   The pane displays detailed information about the port.
5. Click the **EDIT** button.

   The settings for the selected port become available.
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.
- **10M Half**. The port is forced to function at 10 Mbps with half-duplex.
  This option is not available for ports 1 and 2.
- **10M Full**. The port is forced to function at 10 Mbps with full-duplex.
  This option is not available for ports 1 and 2.
- **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 For ports 3 through 10, you cannot select Gigabit Ethernet as the port speed. For ports 1 and 2, you cannot select 1G, 2.5G, 5G, or 10G 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, or for ports 1 and 2, a higher speed, if the linked device supports that speed.

7. Click the **APPLY** button.

   Your settings are saved and the port is reenabled.

Add or Change the Name Label for a Port

By default, only ports 1, 9, and 10 contain a port name label:

- **Port 1**. Uplink
- **Port 9**. Media Streaming
- **Port 10**. Gaming

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 CONNECTED. A port that is not in use shows as AVAILABLE. A port that is disabled shows as DISABLED.
4. Select the port.

The pane displays detailed information about the port.

5. Click the **EDIT** button.
   The settings for the selected port become available.
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.

Use VLANS for Traffic Segmentation

4

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

The chapter contains the following sections:

- *VLAN Overview*
- *Manage Port-Based VLANs*
- *Manage 802.1Q-Based VLANs*
- *Deactivate the Port-Based or 802.1Q-Based VLAN Mode and Delete All VLANs*

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.
- **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. You can configure ports to be a part of an 802.1Q VLAN in 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 such as another switch or WiFi access point.

Manage Port-Based VLANs

After you activate the port-based VLAN mode, you can add and manage port-based VLANs.

Activate the Port-Based VLAN Mode

By default, all types of VLANs are disabled on the switch. Before you can add and manage port-based VLANs, you must activate the port-based VLAN mode.

When you activate the port-based VLAN mode, VLAN 1 is added to the switch and all ports (1 through 10) are members of VLAN 1. This is the default VLAN in the port-based VLAN mode.

To activate the 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 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.

Create a Port-Based VLAN

A port-based VLAN configuration lets you assign ports on the switch to a VLAN. The number of VLANs is limited to the number of ports on the switch. In a basic port-based VLAN configuration, ports with the same VLAN ID are placed into the same VLAN. One port can be a member of multiple VLANs.

By default, all ports are members of VLAN 1.

►To create a 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.

   If you did not yet activate the port-based VLAN mode, see *Activate the Port-Based VLAN Mode* on page 42.

6. In the 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 20 characters.
   - **VLAN ID**. Enter a number from 1 to 10.
   - **Ports**. Select the ports that you want to include in the VLAN through a combination of the following actions:

- 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.
- 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.

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 shows in the PORT BASED VLAN section.

Change a Port-Based VLAN

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

To change a 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 PORT BASED VLAN section, click the down arrow for the VLAN that you want to change.
7. Click the **EDIT** button.
8. Change the settings for the VLAN:

   - **VLAN Name**. Enter a name from 1 to 20 characters.
   - **VLAN ID**. Enter a number from 1 to 10.
   - **Ports**. Select the ports that you want to include in the VLAN through a combination of the following actions:

     - 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.

- 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.

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.

9. Click the **APPLY** button.

   Your settings are saved. The modified VLAN shows in the PORT BASED VLAN section.

Delete a Port-Based VLAN

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

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

To delete a 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 PORT BASED VLAN section, click the down arrow for the VLAN that you want to delete.
7. Click the **DELETE** button.

   Your settings are saved. The VLAN is deleted.

Manage 802.1Q-Based VLANs

After you activate the 802.1Q-based VLAN mode, you can add and manage 802.1Q-based VLANs, manage the port modes (access mode or trunk mode), and manage PVIDs.

Activate the 802.1Q-Based VLAN Mode

By default, all types of VLANs are disabled on the switch. Before you can add and manage 802.1Q-based VLANs, port modes, and PVIDs, you must activate the 802.1Q-based VLAN mode.

When you activate the 802.1Q-based VLAN mode, VLAN 1 is added to the switch and all ports (1 through 10) function in access mode (rather than trunk mode) as untagged members of VLAN 1. This is the default VLAN in the 802.1Q-based VLAN mode.

To activate the 802.1Q-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 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.

Create an 802.1Q-Based VLAN and Assign Ports as Members

An 802.1Q-based VLAN configuration lets you assign ports in access mode as untagged members or in trunk mode as tagged members to a VLAN with an ID number in the range of 1–4094. When you activate the 802.1Q-based VLAN mode, VLAN 1 is added to the switch and all ports (1 through 10) function in access mode (rather than trunk mode) as untagged members of VLAN 1.

For information about changing the port mode, VLAN membership, and PVID for a port, see *Manage the Port Mode, VLAN Membership, and PVID for a Port* on page 47.

To create an 802.1Q-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 802.1Q-based VLAN mode, see *Activate the 802.1Q-Based VLAN Mode* on page 46.

   By default, the **Port Configuration** tab is selected and the 802.1Q PORT CONFIGURATIONS pane displays.

6. Click the **VLAN Configuration** tab.

   The 802.1Q VLAN CONFIGURATIONS pane displays.

7. Click the **ADD VLAN** button.

   The 802.1Q VLAN pop-up window opens.

8. Specify the VLAN settings:

   a. In the **VLAN Name** field, enter a name from 1 to 20 characters.

   b. In the **VLAN ID** field, enter a number from 1 to 4094.

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

   c. From the **Priority** menu, select the priority that is assigned to the traffic on the VLAN.

9. Click the **APPLY** button.

   Your settings are saved. The new VLAN shows in the 802.1Q VLAN CONFIGURATIONS pane.

10. Click the **Port Configuration** tab.

    The 802.1Q PORT CONFIGURATIONS pane displays.

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

12. Click the **SAVE** button.

    Your settings are saved.

Manage the Port Mode, VLAN Membership, and PVID for a Port

You can manage the port mode, VLAN membership, and PVID for a port in an 802.1Q-based VLAN.

You can configure ports to be a part of an 802.1Q VLAN in 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. When a port functions in access mode, the port VLAN ID (PVID) is automatically assigned and is identical to the VLAN ID. You cannot change the PVID for a port that functions in access mode.

- **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 such as another switch or WiFi access point.
  When a port functions in trunk mode, you can manually change the port VLAN ID (PVID). For example, if port 3 functions in trunk mode and the switch includes VLAN 1 (the default VLAN) and VLAN 25 (a custom VLAN), you can assign either a PVID of 1 or a PVID of 25 to port 3. If you assign a PVID of 25, all incoming traffic on port 3 is tagged for VLAN 25 and ports that are not members of VLAN 25 do not receive the traffic. This technique is useful for communicating more securely with devices outside your local network as well as receiving data from other ports that are not in the VLAN.

To manage the port mode, VLAN membership, and PVID for a port in an 802.1Q-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.
   If you did not yet activate the 802.1Q-based VLAN mode, see *Activate the 802.1Q-Based VLAN Mode* on page 46.

   By default, the **Port Configuration** tab is selected and the 802.1Q PORT CONFIGURATIONS pane displays.
6. For each individual port that you want to change, specify the following settings:

   - **Port Mode**. From the menu for the port, select either **Trunk** to let the port function in trunk mode or **Access** to let the port function in access mode.
     For more information, see the introduction to this section.
   - **VLAN**. If the port functions in access mode, from the menu for the port, select the ID for the VLAN that the port must be a member of.
     If the port functions in trunk mode, by default, the selection from the menu is **ALL** and the port is a member of all VLANs on the switch.
   - **PVID**. If the port functions in trunk mode, from the menu for the port, select the ID for the VLAN that the port must tag incoming traffic with.
     If the port functions in access mode, by default, the selection from the menu is identical to the VLAN ID that you assigned to the port and you cannot change the PVID.

You change the settings for multiple ports simultaneously.

7. Click the **SAVE** button.

   Your settings are saved.

Change an 802.1Q-Based VLAN

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

To change an 802.1Q-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.
   By default, the **Port Configuration** tab is selected and the 802.1Q PORT CONFIGURATIONS pane displays.
6. Click the **VLAN Configuration** tab.

   The 802.1Q VLAN CONFIGURATIONS pane displays.
7. In the row for the VLAN that you want to change, click the down arrow.
8. Click the **EDIT** button.

   The 802.1Q VLAN pop-up window opens.
9. Change the VLAN settings as needed:

   - In the **VLAN Name** field, enter a name from 1 to 20 characters.
   - From the **Priority** menu, select the priority that is assigned to the traffic on the VLAN.

   You cannot change the VLAN ID.
10. Click the **APPLY** button.

    Your settings are saved. The modified VLAN shows in the 802.1Q VLAN CONFIGURATIONS pane.

Delete an 802.1Q-Based VLAN

You can delete an 802.1Q-based 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 802.1Q-based VLAN mode, all port-based VLANs are deleted.

▶To delete an 802.1Q-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.
   By default, the **Port Configuration** tab is selected and the 802.1Q PORT CONFIGURATIONS pane displays.
6. Click the **VLAN Configuration** tab.

   The 802.1Q VLAN CONFIGURATIONS pane displays.
7. In the row for the VLAN that you want to delete, click the down arrow.
8. Click the **DELETE** button.

   Your settings are saved. The VLAN is deleted.

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

If you activated the port-based VLAN mode or the 802.1Q-based VLAN mode, you can deactivate either VLAN mode and delete all VLANs.

▶To deactivate the port-based VLAN mode or 802.1Q-based 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 and the pop-up window closes.

Manage the Switch in Your Network

5

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.

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 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 the port-based VLAN mode (see *Manage Port-Based VLANs* on page 42) or the 802.1Q-based VLAN mode (see *Manage 802.1Q-Based VLANs* 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 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 the port-based VLAN mode or the 802.1Q-based 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 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 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 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.

Set Up Link Aggregation

The switch supports both static link aggregation groups (also referred to as port trunking groups) and Link Aggregation Control Protocol (LACP) groups through IEEE 802.3ad Link Aggregation. A link aggregation group (LAG) lets 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 four LAGs. If you use ports 1 and 2 with 10G connections, you can set up a LAG that supports up to 20 Gbps. Configure LAG membership before you enable the LAG.

You set up link aggregation on the switch through a LAG in the following order:

1. Set up the LAG on the switch (see *Set Up a Link Aggregation Group* on page 59).
2. Connect the ports that you intend to make members of a LAG on the switch to the ports that are members of a LAG on *another* device in your network (see *Make a Physical Link Aggregation Connection* on page 60).
3. Enable the LAG on the switch (see *Enable a Link Aggregation Group* on page 60).

Set Up a Link Aggregation Group

You set up link aggregation on the switch by adding 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 35 for information about changing these settings on the switch) and you must set up a physical link aggregation connection (see *Make a Physical Link Aggregation Connection* on page 60).

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 60).

►To set up 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 QOS page displays.

5. From the menu on the left, select **LAG**.

   The LAG page displays.

6. Click the tab for the LAG that you want to configure.

   The text in the tab for the selected LAG displays green.

7. To add ports to the LAG, click the icons for the ports that you want to add (from **1** to **10**).

   The icon for a selected port displays purple.

   A LAG must consist of at least two ports.

8. To set up the LAG as a static LAG, click the **Static/LACP** button.

   When the LAG is set up as a static LAG, the button bar displays white. By default, the LAG is set up as an LACP LAG, and the button bar displays green.

9. Click the **APPLY** button.

Your settings are saved.

Make a Physical 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 59). 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 35.

► **To make link aggregation connections between the switch and other network devices:**

Using Ethernet cables, connect each port that you intend to made a member of the LAG on the switch to each port that is member of the same LAG on another network device.

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 59) and make a physical link aggregation connection (see *Make a Physical Link Aggregation Connection* on page 60), you can enable the link aggregation group.

► **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 QOS page displays.
5. From the menu on the left, select **LAG**.

   The LAG page displays.
6. Click the tab for the LAG that you want to enable.

   The text in the tab for the selected LAG displays green.
7. Click the **Disable/Enable** button.

When the LAG is enabled, the button bar displays green.

8. 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. In the SYSTEM INFO pane, select **DHCP**.

   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 white, 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.

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. In the SYSTEM INFO pane, select **DHCP**.

   The IP address fields display but are not editable. The button bar in the DHCP section displays white 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.

Maintain and Monitor the Switch

6

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*
- *Manage the Configuration File*
- *Return the Switch to Its Factory Default Settings*
- *Manage the Power Saving Mode*
- *Manage the LEDs*
- *View System Information*
- *Change the Switch Device Name*
- *View Switch Connections*
- *View the Status of a Port*

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 page shows 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 `GS810EMX_V0.0.1.0.image`.
9. Click the **UPLOAD** 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 FULL CONFIGURATIONS page displays.
6. Click the **BACKUP** tab.

   The BACKUP FULL CONFIGURATIONS page displays.
7. Click the **DOWNLOAD** button.
8. Follow the directions of your browser to save the file.

   The name of the backup file is `GS810EMX.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 FULL CONFIGURATIONS 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 `GS810EMX.cfg`.

   The **UPLOAD** button changes to the **APPLY CONFIGURATION** button.

7. Click the **APPLY CONFIGURATION** 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 82.

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 the Power LED turns off.
3. Release the **RESET** button.

   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.

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 page displays.
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.)

Manage the LEDs

You can customize your visual environment by managing the color and activity of the Power LED and many settings for the port LEDs (also referred to as Activity LEDs). The LED settings do not affect the way in which traffic is switched.

In addition to the Power LED, you can manage either individual port LEDs or a group of port LEDs simultaneously. You can also reset all port LEDs to default settings.

Note To turn off *all* LEDs entirely (referred to as Quiet mode), press the **LED** button to the left of port 10 on the back of the switch (see *Back Panel* on page 9).

The switch functions with the following default color schemes, which you can customize:

- **Standard color scheme**. In the Standard Preset mode (which is the default mode), the switch uses a color scheme with a purple and dark blue color palette. The Power LED is orange.
- **Gaming color scheme**. In the Gaming Preset mode, the switch uses a color scheme with a yellow and green color palette. The Power LED is green.
- **Streaming color scheme**. In the Media Streaming Preset mode, the switch uses a color scheme with a light blue color palette. The Power LED is light blue.

Manage Individual Port LEDs

The switch lets you manage the following settings for individual port LEDs (also referred to as Activity LEDs):

- **Activity**. By default, a port LED lights when you connect a powered-on device to the port. You can disable the LED.
- **Frequency**. By default, the frequency with which a port LED lights is high. You can choose from four other frequency settings.
- **Color**. The LED default color depends on the connection speed. For each connection speed, you can select a predefined color or create your own color.
- **Brightness**. By default, the LED brightness is high. You can lower the brightness.

To manage individual port LEDs:

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. In the SYSTEM INFO pane, select **LED**.

   By default, the **PORT ACTIVITY LEDS** tab is selected and the ACTIVITY LEDs page displays.

5. Click the number for the port LED that you want to manage.

   The LED settings for the port display.

6. Specify the following settings:

   - **Activity**. By default, the port LED lights when you connect a powered-on device to the port. To disable the port LED, click the **ACTIVITY LED** button.
     When the LED activity is enabled, the button bar display green. When it is disabled, the button bar displays white.
   - **Frequency**. By default, the frequency with which a port LED lights is high. To change the frequency, select another setting from the **Frequency** menu.
   - **Color**. The LED default color depends on the connection speed. For each connection speed, select a predefined color or create your own color. To change the color for a port speed, do the following:

     a. For port 1 or 2, click the **10G**, **5G**, **2.5G**, or **1G** icon. For ports 3 through 10, click the **1G** or **100M** icon.
     b. Select one of the predefined colors. Or, to create your own color, click the **Other** menu, and click a color in the color circle.

   - **Brightness**. By default, the LED brightness is high. To change the brightness, move the button on the **Brightness** slider.

   Your settings are saved automatically (that is, the page does not provide an **APPLY** button).

Manage Port LEDs in a Batch

The switch lets you manage the following settings for port LEDs (also referred to as Activity LEDs) in a batch:

- **Activity**. By default, a port LED lights when you connect a powered-on device to the port. You can disable the LED.
- **Frequency**. By default, the frequency with which a port LED lights is high. You can choose from four other frequency settings.
- **Color**. The LED default color depends on the connection speed. For each connection speed, you can select a predefined color or create your own color.
- **Brightness**. By default, the LED brightness is high. You can lower the brightness.

Note Because of different port speed capabilities, you can manage either the LEDs for ports 1 and 2 in a batch or the LEDs for ports 3 through 10 in a batch.

To manage port LEDs in a batch:

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. In the SYSTEM INFO pane, select **LED**.

   By default, the **PORT ACTIVITY LEDS** tab is selected and the ACTIVITY LEDs page displays.

5. At the bottom of the page, click the **BATCH EDIT** link.

   Check boxes for all ports display.

6. Select the check boxes for the port LEDs that you want to manage.

   Either select the check boxes for port 1 and port 2 or select two, several, or all check boxes for other ports (3 through 10).

7. Specify the following settings that will apply to all selected ports:

   - **Activity**. By default, the port LED lights when you connect a powered-on device to the port. To disable the port LED, click the **ACTIVITY LED** button.
     When the LED activity is enabled, the button bar display green. When it is disabled, the button bar displays white.
   - **Frequency**. By default, the frequency with which a port LED lights is high. To change the frequency, select another setting from the **Frequency** menu.
   - **Color**. The LED default color depends on the connection speed. For ports 1 and 2, the page shows four LED color sections (for 10G, 5G, 2.5G, and 1G speeds). For ports 3 through 10, the page shows two LED color sections (for 10G and 100M speeds). For each connection speed, select a predefined color, or create your own color by clicking the **Other** menu and then clicking a color in the color circle.
   - **Brightness**. By default, the LED brightness is high. To change the brightness, move the button on the **Brightness** slider.

8. Click the **SAVE** button.

   Your settings are saved.

Reset the Port LEDs to Default Settings

The switch lets you reset the port LEDs to default settings. The other settings on the switch are not affected. The Power LED is not reset to default settings.

► To reset the port LEDs to default settings:

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. In the SYSTEM INFO pane, select **LED**.

   By default, the **PORT ACTIVITY LEDS** tab is selected and the ACTIVITY LEDs page displays.

5. At the bottom of the page, click the **RESET TO DEFAULT** link.

   A pop-up warning window opens.

6. Click the **CONTINUE** button.

   The pop-up window closes. The port LEDs are reset to default settings.

Manage the Power LED

The switch lets you manage the activity (enabled or disabled) and color of the Power LED on the top of the switch.

► To manage the Power LED:

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. In the SYSTEM INFO pane, select **LED**.

   By default, the **PORT ACTIVITY LEDS** tab is selected and the ACTIVITY LEDs page displays.

5. Click the **POWER LED** tab.

   The POWER LED page displays.

6. Specify the following settings:

   - **Activity**. By default, the Power LED lights when you apply power to the switch. To disable the Power LED, click the **Enable Power LED** button.
     When the LED activity is enabled, the button bar display green. When it is disabled, the button bar displays white.
   - **Color**. By default, the color of the Power LED is orange. To change the color, do the following:

     a. Below Power LED Color, click the color icon.

     b. Select one of the predefined colors. (The default color orange is among the predefined colors.) Or, to create your own color, click the **Other** menu, and click a color in the color circle.

7. Click the **SAVE** 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.

   By default, the SYSTEM INFO pane is expanded and shows the basic system information.

Change the Switch Device Name

By default, the device name of the switch is Nighthawk SX10. 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.

   By default, the SYSTEM INFO pane is expanded and shows the basic system information.
4. In the **Switch Name** field, enter a new name for the switch.
5. Click the **APPLY** button.

   Your settings are saved.

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 CONNECTED. A port that is not in use shows as AVAILABLE. A port that is disabled shows as DISABLED.
4. To view details about a port, select the port.

   The pane displays detailed information about the port.

   For information about setting rate limits for incoming and outgoing traffic, setting the port priority, 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 35.

Diagnostics and Troubleshooting

7

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 to 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 CABLE TEST page displays.
5. Select one or more ports to test by clicking the port icons.

   The icons for 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 section with the test results closes.

Manage Loop Prevention

By default, loop prevention is enabled. If the switch detects a loop, the switch blocks one of the ports that are part of the loop and the port LED for that port blinks at a constant speed. If two ports are part of a loop, the port with the highest port number is blocked. For example, if port 1 and port 2 are part of a loop, port 2 is blocked while port 1 continues to process traffic. The loop status (that is, port blocking and LED blinking) is cleared if the switch does not detect the loop for a period of four seconds.

►To manage loop prevention:

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 CABLE TEST page displays.

5. From the menu on the left, select **LOOP PREVENTION**.

   The LOOP PREVENTION page displays.

6. Disable or enable loop prevention by clicking the button.

   When loop prevention is enabled (which is the default setting), the button bar displays green.

7. Click the **APPLY** button.

   Your settings are saved.

Enable Port Mirroring

Port mirroring lets you mirror the incoming (ingress) and outgoing (egress) traffic on a single source port to a predefined destination port. You might need a network analyzer application to analyze the mirrored network traffic.

Note If you configure a port as a destination port for mirrored traffic, you might not be able to use that port for regular traffic.

► To enable port mirroring:

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 CABLE TEST page displays.

5. From the menu on the left, select **PORT MIRRORING**.

   The PORT MIRRORING page displays.

6. Disable or enable port mirroring by clicking the button.

When port mirroring is enabled, the button bar displays green. By default, port mirroring is disabled and the button bar displays white.

After you enable port mirroring, you must specify the ports.

7. In the upper port section, select one or more source ports by clicking the port icons.

   The icon for a selected port displays purple.

   You cannot select a source port that is a member of a LAG.

8. In the lower port section, select the single destination port by clicking the port icon.

   The icon for a selected port displays purple.

   You cannot select a destination port that is a member of a LAG.

9. Click the **APPLY** button.

   Your settings are saved.

View the Port Statistics

You can view port statistics for each of the 10 ports, including the bytes received, bytes sent, and cyclic redundancy check (CRC) error packets, which are packets with errors or corrupt packets.

► **To view or clear the port statistics.**

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 CABLE TEST page displays.

5. From the menu on the left, select **PORT STATISTICS**.

   The PORT STATISTICS page displays, showing the statistics for each of the ports.

6. To refresh the page with the latest information, click the **REFRESH** button.
7. To reset all counters to 0, click the **CLEAR COUNTERS** button.

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 opens.
5. Click the **REBOOT** button.

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

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 resolve this subnet conflict:**

1. Disconnect the Ethernet cable between the switch and your network.
2. Unplug the power adapter of the switch.
3. Reconnect the Ethernet cable between the switch and your network.
4. Plug the power adapter of the switch 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.

Hardware Troubleshooting Chart

The following table lists symptoms, possible causes, and possible solutions for hardware problems that might occur.

Table 3. Troubleshooting chart

Symptom	Possible Cause	Possible Solution
Power LED is off.	Power is not supplied to the switch or the Power LED is disabled.	Check the power cable connections at the switch and the power source. Make sure that all cables are used correctly and comply with the Ethernet specifications. Make sure that the Power LED is enabled.
A port LED is off when the port is connected to a powered-on device.	The port connection is not working or the port LED is disabled or dimmed.	Check the crimp on the connectors and make sure that the plug is properly inserted and locked into the port at both the switch and the connecting device. Make sure that all cables are used correctly and comply with the Ethernet specifications. Check for a defective port, cable, or module by testing them in an alternate environment where all products are functioning. Make sure that the port LED is enabled and sufficiently bright.
File transfer is slow or performance is degraded.	One possible cause is that a broadcast storm occurred and that a network loop (redundant path) was created.	Break the loop by making sure that only one path exists from any networked device to any other networked device.
A segment or device is not recognized as part of the network.	One or more devices are not properly connected, or cabling does not meet Ethernet guidelines.	Verify that the cabling is correct. Make sure that all connectors are securely positioned in the required ports. It is possible that equipment was accidentally disconnected.
One or more port LEDs are blinking continuously and the network is disabled.	A network loop (redundant path) was created.	Break the loop by making sure that only one path exists from any networked device to any other networked device.

Factory Default Settings and Technical Specifications

A

This appendix includes the following sections:

- *Factory Default Settings*
- *Basic Technical Specifications*

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 more than five seconds. The switch resets and returns to the factory settings that are shown in the following table.

Table 4. 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 mode	Port-Based
Port priority	Medium (P4) (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
VLAN ID enabled for IGMP snooping	None
Blocking of unknown multicast addresses	Disabled
IGMPv3 IP header validation	Disabled
Static router port for IGMP snooping	None
Ports and LEDs	
Port link speed	Autonegotiation
Port LEDs	Enabled

Table 4. Factory default settings (Continued)

Feature	Default Setting
Power LED	Enabled
LED color scheme	Standard color scheme. In the Standard Preset mode (which is the default mode), the switch uses a color scheme with a purple and dark blue color palette. The Power LED is orange.
Other features	
VLANs	No VLANs configured VLANS configurable in access mode or trunk mode
Link aggregation	No LAGs configured, LACP enabled
Power saving mode	Disabled
Loop prevention	Enabled
Port mirroring	Disabled
Jumbo frames	Enabled (nonconfigurable)

Basic Technical Specifications

The following table shows the basic technical specifications of the switch.

For more specifications, see the data sheet that you can download by visiting *downloadcenter.netgear.com*.

Table 5. Basic technical specifications

Feature	Description
Network interfaces	Two RJ-45 ports (ports 1 and 2) supporting 100BASE-TX, 1000BASE-T, 2.5GBASE-T, 5GBASE-T, or 10GBASE-T Eight RJ-45 ports (ports 3 through 10), supporting 10BASE-T, 100BASE-TX, or 1000BASE-T
Network cable	For 100 Mbps, use a Category 5 (Cat 5) or higher-rated cable.
	For 1 Gbps, 2.5 Gbps, or 5 Gbps, use a Category 5e (Cat 5e) or higher-rated cable.
	For 10 Gbps for up to 55 meters (180 feet), use a Category 6 (Cat 6) or higher-rated cable.
	For 10 Gbps for more than 55 meters (180 feet), use a Category 6A (Cat 6A) or higher-rated cable.
Power adapter	Input: 100–240 VAC, 50–60 Hz (The plug is localized to the country of sale.) Output: 12V, 2.5A

Table 5. Basic technical specifications (Continued)

Feature	Description
Power consumption	From 5.54W to 14.19W
Dimensions (W x D x H)	10.55 x 8.0 x 3.66 in. (268 x 203 x 93 mm)
Weight	3.34 lb (1.515 kg)
Operating temperature	32º to 104ºF (0° to 40°C)
Operating humidity	90% maximum relative humidity, noncondensing
Storage temperature	–40° to 158°F (–40º to 70ºC)
Storage humidity	95% maximum relative humidity, noncondensing
IEEE standards	IEEE 802.3 Ethernet IEEE 802.3i 10BASE-T IEEE 802.3x Full-Duplex Flow Control IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3bz 2.5GBASE-T and 5GBASE-T IEEE 802.3an 10GBASE-T IEEE 802.3az Energy Efficient Ethernet (EEE) IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging

Table 5. Basic technical specifications (Continued)

Feature	Description
Electromagnetic certifications	47 CFR FCC Part 15, Subpart B, Class B ICES-003:2016 Issue 6, Class B ANSI C63.4:2014
	EN 55032:2012 + AC:2013 / CISPR 32:2012 EN 55032:2015 + AC:2016 / CISPR 32:2015 + COR1:2016 EN 61000-3-2:2014 EN 61000-3-3:2013 EN 55024:2010 EN 55024:2010 + A1:2015 EN 6100-4-2:2009 EN 6100-4-3:2006 + A1:2008 + A2:2010 EN 6100 -4-4:2012 EN 6100 -4-5:2014 EN 6100 -4-6:2014 EN 6100 -4-8:2010 EN 6100-4-11:2004
	AS/NZS CISPR 32:2013, Class B AS/NZS CISPR 32:2015, Class B
	VCCI-CISPR 32:2016, Class B
	Russia EAC mark
	CNS 13438 CNS 14336-1 : 99
Electromagnetic compliance	Class B
Safety certifications	CE Mark, commercial IEC 60950-1:2005 + A1:2009 + A2:2013
	EN 60950-1: 2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
	AS/NZS 60950.1:2015
	Russia EAC mark