NETGEAR®

User Manual

Gigabit Ethernet Easy Smart Managed Switches

Models

GS116EP

GS116EPP

April 2025
202-12831-01

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

Support and Community

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

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

Regulatory and Legal

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

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

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

See the regulatory compliance document before connecting the power supply.

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

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

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

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
202-12831-01	April 2025	First publication.

Contents

Chapter 1 Get Started

Related documentation..... 9
Hardware..... 9
Switch package contents..... 9
LEDs..... 9
Switch label..... 11
1000BASE-X SFP slots..... 12
Safety instructions and warnings..... 12

Chapter 2 Install and Access the Switch in Your Network

Set up the switch in your network and power on the switch..... 16
Discover the switch's IP address to access its device UI..... 16
Discover the IP address and access the switch..... 17
Use the NETGEAR Discovery Tool to discover the switch's IP address and access the device UI..... 17
Assign a fixed IP address to the switch..... 18
Set a fixed IP address for the switch through a network connection..... 19
Assign a fixed IP address by connecting directly to the switch off-network..... 20
Change the language of the device UI..... 21
Register the switch..... 22

Chapter 3 Optimize the Switch Performance

Set the quality of service mode and port rate limits..... 25
Use port-based quality of service mode and set the priority and rate limits for ports..... 25
Use 802.1P/DSCP quality of service mode and set the rate limits for ports..... 27
Manage broadcast filtering and set port storm control rate limits..... 28
Manage individual port settings..... 29
Set rate limits for a port..... 30
Manage flow control for a port..... 31
Change the speed for a port or disable a port..... 32
Add or change the name label for a port..... 33

Chapter 4 Use VLANS for Traffic Segmentation

Types of supported VLANs..... 35

Manage basic port-based VLANs..... 36
Manage advanced port-based VLANs..... 37
Activate the advanced port-based VLAN mode..... 38
Create an advanced port-based VLAN..... 39
Change an advanced port-based VLAN..... 40
Delete an advanced port-based VLAN..... 41
Manage basic 802.1Q VLANs..... 42
Activate the Basic 802.1Q VLAN mode..... 42
Create a basic 802.1Q VLAN and assign ports as members... 43
Assign the port mode in a basic 802.1Q VLAN configuration. 45
Change a basic 802.1Q VLAN..... 46
Delete a basic 802.1Q VLAN..... 47
Manage advanced 802.1Q VLANs..... 48
Activate the advanced 802.1Q VLAN mode..... 48
Create an advanced 802.1Q VLAN..... 50
Change an advanced 802.1Q VLAN..... 51
Specify a port PVID for an advanced 802.1Q VLAN..... 52
Set an existing advanced 802.1Q VLAN as the voice VLAN and adjust the CoS value..... 53
Edit the OUI table for the voice VLAN..... 55
Set up an auto-camera VLAN on an advanced 802.1Q VLAN and adjust the CoS value..... 56
Edit the OUI table for the auto-camera VLAN..... 58
Set an existing advanced 802.1Q VLAN as the WiFi VLAN and adjust the CoS value..... 59
Edit the OUI table for the auto-WiFi VLAN..... 61
Delete an advanced 802.1Q VLAN..... 62
Deactivate a port-based or 802.1Q VLAN mode and delete configured VLANs..... 63

Chapter 5 Manage the Switch in Your Network

Manage Universal Plug and Play..... 66
Set up link aggregation..... 66
Make a link aggregation connection..... 67
Set up a static link aggregation group..... 67
Set up a dynamic link aggregation group..... 69
Enable a link aggregation group..... 70
View link aggregation group status..... 71
Manage multicast..... 71
Manage IGMP snooping..... 71
Enable a VLAN for IGMP snooping..... 72
Manage blocking of unknown multicast addresses..... 73
Manage IGMPv3 IP header validation..... 74
Set up a static router port for IGMP snooping..... 74

Change the IP address of the switch..... 75
Reenable the DHCP client of the switch..... 76

Chapter 6 Maintain and Monitor the Switch

View system information..... 79
View switch connections..... 79
View the status of a port..... 80
Change the switch device name..... 80
View system uptime..... 81
Control the port LEDs..... 81
Update the firmware on the switch..... 82
Manage the configuration file..... 83
Back up the switch configuration..... 83
Restore the switch configuration..... 84
Use the device UI to reboot the switch..... 85
Return the switch to its factory default settings..... 86
Use the RESET button to reset the switch..... 86
Use the device UI to reset the switch..... 87
Control access to the device UI..... 87
Change or lift access restrictions to the switch..... 88
HTTP and HTTPS management access..... 89
Configure HTTP access settings..... 90
Configure HTTPS access settings..... 90
Browser security message with HTTPS access 92
Manage certificates for HTTPS access..... 92
Update the HTTPS server certificate..... 93
Delete certificates for HTTPS access..... 94
Manage the DoS prevention mode..... 94
Manage the power saving mode..... 95
Change the device management password..... 96
Date and time settings..... 97
Configure the system time manually..... 97
Enable system time to synchronize with an SNTP server 98
Configure the SNTP client mode 99
Configure an SNTP server 100
Configure daylight saving time..... 102
View daylight saving time status..... 103
Power over Ethernet..... 104
PoE considerations for switches that support PoE or PoE+.. 104
PoE+ overview..... 104
Monitor PD health..... 105
Manage uninterrupted PoE..... 106
Power cycle the PoE ports..... 107
Manage an individual PoE port..... 108

Display PoE port status..... 109
Configure a PoE schedule..... 111
Edit or disable a PoE schedule..... 112

Chapter 7 Diagnostics and Troubleshooting

Test cable connections..... 115
Resolve a subnet conflict to access the switch..... 115
PoE troubleshooting suggestions..... 116
Enable or disable loop prevention..... 117
Enable port mirroring..... 117
View or clear the port statistics..... 118

Appendix A Factory Default Settings and Technical Specifications

Factory default settings..... 121
Technical specifications..... 122
Model GS116EP technical specifications..... 122
Model GS116EPP technical specifications..... 122

Appendix B Additional Switch Discovery and Access Information

Access the switch from any computer..... 125

1

Get Started

This user manual describes how you can use the device user interface (UI) to configure and manage NETGEAR Gigabit Ethernet Easy Smart Managed Switches.

The manual describes the software configuration procedures and explains the options that are available within those procedures.

The *Gigabit Ethernet Easy Smart Managed Switches User Manual* describes the switch models listed in the following table.

Table 1. Supported switch models

Model	Name
GS116EP	16-Port PoE+ Gigabit Ethernet Easy Smart Managed Switches
GS116EPP	16-Port High-Power PoE+ Gigabit Ethernet Easy Smart Managed Switches

This chapter covers the following topics:

- Related documentation
- Hardware
- Switch package contents
- LEDs
- Switch label
- 1000BASE-X SFP slots
- Safety instructions and warnings

NOTE:

- This user manual complements the installation guide that came with your switch. You can also download the installation guide by visiting netgear.com/support/download/.
- For more information about the topics covered in this manual, visit the support website at netgear.com/support
- Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. You can manually check for, and download, new firmware. If the features or behavior of your product do not match what is described in this guide, see the latest firmware release notes for your switch model.

Related documentation

Related documentation is available at netgear.com/support/download/:

- Installation guide
- Data sheet

Hardware

The switch provides 15 Gigabit Ethernet copper ports that can support a power of up to 30W PoE+ (802.3at) to devices such as VoIP phones, surveillance IP cameras, and wireless access points.

- Model GS116EP: The maximum PoE power budget of the switch across all active ports is 180W.
- Model GS116EPP: The maximum PoE power budget of the switch across all active ports is 231W.

Each model has an SFP port. To use the SFP port, you must insert an SFP transceiver module, which you can purchase from NETGEAR.

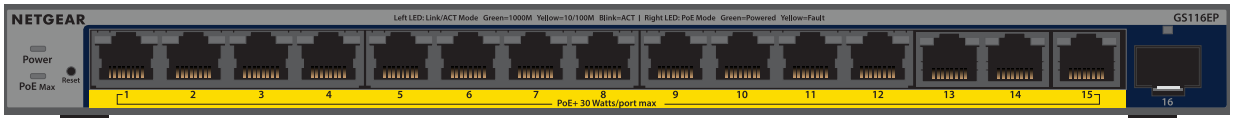
Switch package contents

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

LEDs

This section describes the LED designations. The port LEDs are located above the ports.

Model GS116EP:



Model GS116EP:

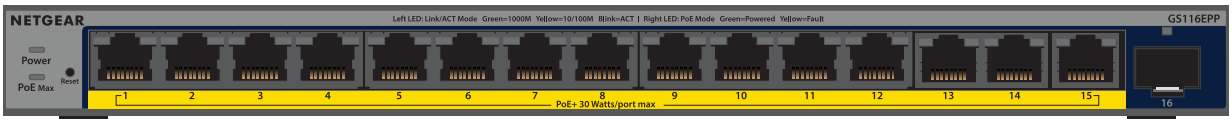
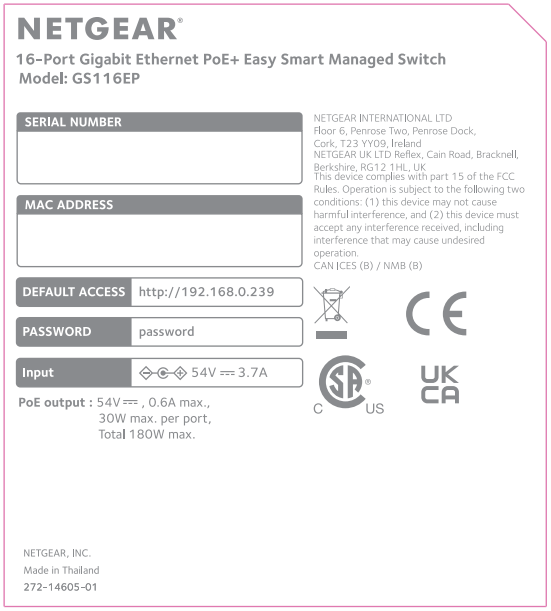


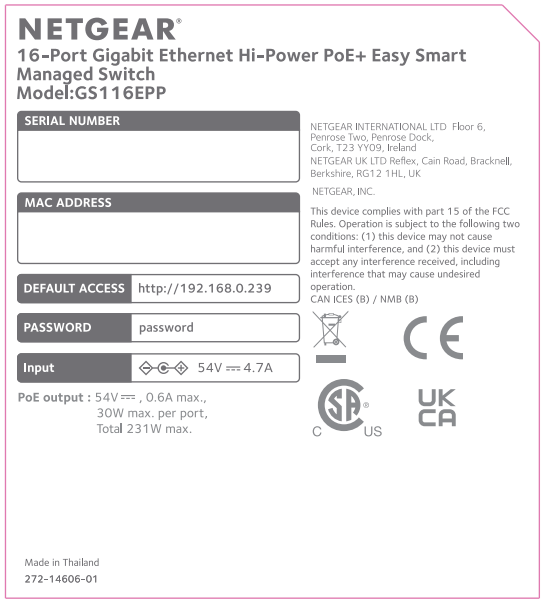
Table 2. Model GS116EP, GS116EPP LEDs on the front panel

LED	Description
Power LED	**Solid green**: The switch is powered on and operating normally. **Off**: Power is not supplied to the switch.
PoE Max LED	**Off**: Sufficient (more than 7W of) PoE power is available. **Solid yellow**: Less than 7W of PoE power is available. **Blinking yellow**: At least once during the previous two minutes, less than 7W of PoE power was available.
Left port LED	**Solid green**: 1000 Mbps link on this port. **Blinking green**: 1000 Mbps activity on this port. **Solid yellow**: A valid 10 Mbps or 100 Mbps port link is established. **Blinking yellow**: 100 Mbps or 10 Mbps activity on this port. **Off**: No link is detected on this port.
Right port LED	**Solid green**: The port is delivering PoE power. **Off**: The port is not delivering PoE power. **Solid yellow**: A PoE fault occurred.
SFP port	**Solid green**: A valid 1 Gbps SFP module link is established. **Blinking green**: The port is transmitting or receiving packets at 1 Gbps. **Off**: No SFP link is detected on this port.

Switch label

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





1000BASE-X SFP slots

To enable fiber, copper, or long-distance connections on the switch, SFP slots accommodate standard 1G SFP transceiver modules, which are sold separately.

For information about specific NETGEAR SFP transceiver modules and cables that are supported for the switch, visit netgear.com/business/wired/switches/ and click the **ACCESSORIES** tab, or see the datasheet for your specific switch.

Table 3. Supported SFP transceiver modules

Speed and Medium	Model	Description
1G Ethernet short-reach fiber	AGM731F	SFP transceiver 1000BASE-SX
1G Ethernet long-reach fiber	AGM732F	SFP transceiver 1000BASE-LX
1G Ethernet copper	AGM734	SFP transceiver 1000BASE-T

Safety instructions and warnings

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

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

- This product is designed for indoor use only in a temperature-controlled and humidity-controlled environment. Note the following:
  - For more information about the environment in which this product must operate, see the environmental specifications in the appendix or the data sheet.
  - If you want to connect the product to a device located outdoors, the outdoor device must be properly grounded and surge protected, and you must install an Ethernet surge protector inline between the indoor product and the outdoor device. Failure to do so can damage the product.
  - Before connecting the product to outdoor cables or devices, see https://kb.netgear.com/000057103 for additional safety and warranty information.

  Failure to follow these guidelines can result in damage to your NETGEAR product, which might not be covered by NETGEAR's warranty, to the extent permissible by applicable law.
- Observe and follow service markings:

  - Do not service any product except as explained in your product documentation. Some devices should never be opened.
  - If applicable to your product, opening or removing covers that are marked with the triangular symbol with a lightning bolt can expose you to electrical shock. We recommend that only a trained technician services components inside these compartments.
- If any of the following conditions occur, unplug the product from the power outlet, and then replace the part or contact your trained service provider:
  - Depending on your product, the power adapter, power adapter cable, power cable, extension cable, or plug is damaged.
  - An object fell into the product.
  - The product was exposed to water.
  - The product was dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep the product away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your product components, and never operate the product in a wet environment. If the product gets wet, see the appropriate section in your troubleshooting guide, or contact your trained service provider.
- Do not push any objects into the openings of your product. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- If applicable to your product, allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To avoid damaging your system, if your product uses a power supply with a voltage selector, be sure that the selector is set to match the power at your location:
  - 115V, 60 Hz in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  - 100V, 50 Hz in eastern Japan and 100V, 60 Hz in western Japan
  - 230V, 50 Hz in most of Europe, the Middle East, and the Far East
- Be sure that attached devices are electrically rated to operate with the power available in your location.

- Depending on your product, use only a supplied power adapter or approved power cable:

  If your product uses a power adapter:

  - If you were not provided with a power adapter, contact your local NETGEAR reseller.
  - The power adapter must be rated for the product and for the voltage and current marked on the product electrical ratings label.

  If your product uses a power cable:

  - If you were not provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable approved for your country.
  - The power cable must be rated for the product and for the voltage and current marked on the product electrical ratings label. The voltage and current rating of the cable must be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded power outlets.
- If applicable to your product, the peripheral power cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a three-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables, power adapter cables, or power cables carefully. Route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power adapters, power adapter cables, power cables or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local and national wiring rules.

2

Install and Access the Switch in Your Network

This chapter describes how you can install the switch in your network, get an IP address for the switch, and use the IP address to access the switch's device UI so you can set up, manage, and monitor the switch.

The chapter contains the following sections:

- Set up the switch in your network and power on the switch
- Discover the switch’s IP address to access its device UI
- Change the language of the device UI
- Register the switch

Set up the switch in your network and power on the switch

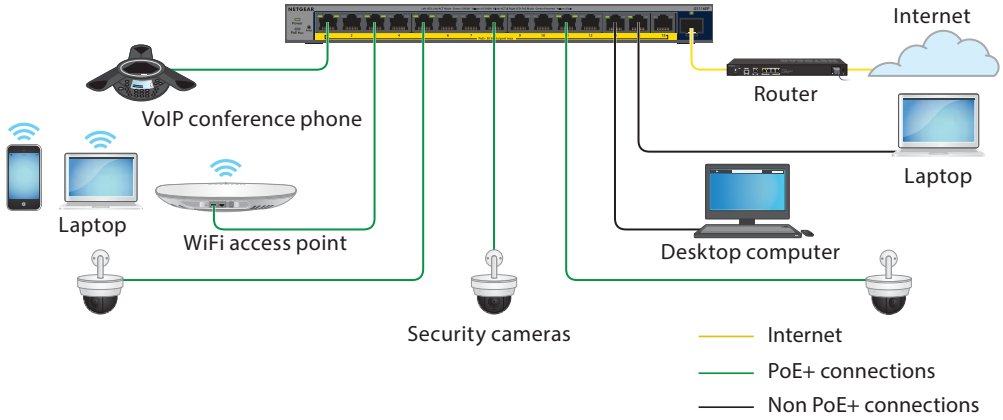


Figure 1. Example connections

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

1. Connect any port on the switch to a LAN port on a router that is connected to the Internet.
2. On the switch, connect your PoE devices to the lowest number ports, starting with port 1, and then connect any non-PoE devices.

   For more information, see PoE considerations for switches that support PoE or PoE+ on page 104.
3. Connect the power adapter to the switch and plug the power adapter into an electrical outlet.

   The power LED lights and the port LEDs for connected devices light.

Discover the switch’s IP address to access its device UI

Use a computer and a web browser to access the device UI so you can configure and manage the switch. Choose one of the following methods to discover the switch's IP address in your network, and then use the IP address to access the device UI of the switch:

- Use the NETGEAR Discovery Tool to discover the switch's IP address and access the device UI on page 17.
- Assign a fixed IP address to the switch on page 18.

Discover the IP address and access the switch

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

If you prefer to set a fixed (static) IP address on the switch, see Assign a fixed IP address to the switch on page 18.

Use the NETGEAR Discovery Tool to discover the switch's IP address and access the device UI

The NETGEAR Discovery Tool (NDT, formerly referred to as NSDT) discovers the switch in your network so you can access the device UI of the switch from a web browser.

To install the NDT, discover the switch in your network, access the switch, and discover the switch IP address:

1. Download the NDT by visiting netgear.com/support/product/netgear-discovery-tool.aspx.

   Download the version for your operating system.
2. Temporarily deactivate the firewall, Internet security, antivirus programs, or all of these on the computer that you are using to configure the switch.
3. Unzip the NDT file, and double-click the **.exe** or **.dmg** file (for example, `NETGEAR+Discovery+Tool+Setup+1.2.103.exe` or `NetgearSDT-V1.2.103.dmg`) to install the program on your computer.

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

   If the **NETGEAR Discovery Tool** icon is in the dock of your Mac or on the desktop of your Windows-based computer, click or double-click the 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 NDT to access the switch.
9. Click the **Start Searching** button.

   The NDT displays a list of switches that it discovers on the selected network.

   For each switch, the tool displays the IP address.

10. To access the device UI of the switch, click the **ADMIN PAGE** button.

    The login page of the device UI opens.

11. Enter the device management password.

    The default password to access the switch is **password**. The first time that you log in to the switch, you must change the default 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.

    NOTE: 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 the IP address, and the bookmark might no longer link to the login page for the switch. When you restart the switch, 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 Assign a fixed IP address to the switch on page 18) to make sure that the new bookmark always links to the login page for the switch, even after you restart the switch.

Assign a fixed IP address to the switch

By default, the switch is configured to automatically receive an IP address from a DHCP server, or a router that functions as a DHCP server, in your network. However, certain events can cause the DHCP server to issue a new IP address to the switch, so if you need

the switch to persistently have the same IP address, you can assign a fixed (static) IP address to the switch. For example, you may want to attach a shared device such as a printer or file server, configure port forwarding, or set up the switch so you can connect remotely from a mobile device.

To change the IP address of the switch, use one of the following methods:

- **Connect to the switch through the network**: If the switch and your computer are connected to the same network, you can change the IP address of the switch through a network connection (see Set a fixed IP address for the switch through a network connection on page 19).
- **Connect directly to the switch**: If you cannot connect to the switch over a network connection, you can change the IP address of the switch by using an Ethernet cable to connect a directly to the switch (see Assign a fixed IP address by connecting directly to the switch off-network on page 20).

Set a fixed IP address for the switch through a network connection

If the switch and your computer are connected to the same network, you can set a fixed IP address on 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.

   A login window opens.
3. Enter the device management password.

   The default password to access the switch is **password**. The first time that you log in to the switch, you must change the default password. The password is case-sensitive.

   The HOME page displays.

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

   The toggle in the DHCP section displays green because the DHCP client of the switch is enabled.
5. In the DHCP section, turn off the toggle.

   The toggle in the DHCP section displays gray because the DHCP client of the switch is disabled. You can now edit 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.

   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, enter the new IP address of the switch in the address field of your web browser.

   The login page displays.
10. For easy access to the device UI, bookmark the page on your computer.

Assign a fixed IP address by connecting directly to the switch off-network

If you cannot connect to the switch over a network connection, you can use an Ethernet cable to connect your computer directly to the switch, and then you can set the IP address of the switch.

To disable the switch's DHCP client and change the IP address of the switch to a fixed IP address through 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 and, to connect to it, your computer's IP address must be on the same subnet (192.168.0.x).

   The method to change your computer's IP address depends on the operating system of your computer.
3. Open a web browser from your computer.
4. Enter **192.168.0.239** as the IP address of the switch.

   The login page displays.
5. Enter the device management password.

   The default password to access the switch is **password**. The first time that you log in to the switch, you must change the default password. The password is case-sensitive.

The HOME page displays.

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

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

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

7. Turn off the toggle in the DHCP section.

   The toggle in the DHCP section displays gray because the DHCP client of the switch is disabled. 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 disconnects when you change the IP address.

11. Disconnect the switch from your computer and install the switch in your network.
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 device management password.

       The password is the one that you specified the first time that you logged in. The password is case-sensitive.

       The HOME page displays.

Change the language of the device UI

By default, the language option of the device UI is set to Auto so that the switch can automatically detect the language. However, you can select a specific language to display in the UI.

To change the language of the device UI:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. Select **System Info**.

   The System Info fields display.
5. From the **Language** menu, select a language.
6. Click the **APPLY** button.

   A pop-up warning window opens.
7. Click the **YES** button.

   Your settings are saved and the language changes.

Register the switch

Registering the switch allows you to receive email alerts and streamlines the technical support process. You can log in to your NETGEAR account at my.netgear.com to register your switch, or you can also register the switch through the device UI, in which case the switch must be connected to the Internet.

To register the switch through the device UI:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **PRODUCT REGISTRATION**.

The PRODUCT REGISTRATION page displays.

6. Click the **REGISTER** button.

   The switch contacts the registration server.

7. Follow the onscreen process to register the switch.

3

Optimize the Switch Performance

This chapter describes how you can optimize the performance of the switch and contains the following sections:

- Set the quality of service mode and port rate limits
- Manage individual port settings

Set the quality of service mode and port rate limits

You can manually set the Quality of Service (QoS) modes to manage traffic:

- **Port-based QoS mode**: Lets you set the priority (low, normal, medium, or high) 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 traffic on a port, including incoming or outgoing traffic, or both, 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 of these QoS modes, simply means that the switch slows down all traffic on the 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 notice degraded video stream quality, sluggish response times during online activity, and other problems.

Use port-based quality of service mode and set the priority and rate limits for ports

802.1P/DSCP is the default QoS mode on the switch, but you can also set port-based QoS. For each port, you can set the priority and the rate limits for both ingress (incoming) and egress (outgoing) traffic:

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

each rate limit as a predefined data transfer threshold from 512 Kbps (Kbit/s) to 512 Mbps (Mbit/s).

You also can set individual port rate limits (the same feature) from the PORT STATUS page (see Set rate limits for a port on page 30).

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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. 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 28.
6. To set the port priorities, do the following:
   a. Click the **PRIORITY** tab.
   b. Click the **Edit** button.

      The EDIT PRIORITY page displays.
   c. For each port for which you want to set the priority, select **Low**, **Normal**, **Medium**, **High (P0-P7)** from the individual menu for the port.

      The default selection is **Medium (P4)**.
   d. Click the **APPLY** button.

Your settings are saved and the EDIT PRIORITY page closes.

7. To set rate limits, do the following:
   a. Click the **RATE LIMITS** tab.
   b. Click the **Edit** button.

      The EDIT RATE LIMITS page displays.
   c. For each port for which you want to set rate limits, select the rate in Kbps (Kbit/s) to Mbps (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 and the EDIT RATE LIMITS page closes.

Use 802.1P/DSCP quality of service mode and set the rate limits for ports

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

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

You also can set individual port rate limits (the same feature) from the PORT STATUS page (see Set rate limits for a port on page 30).

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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. 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 28.
6. To set rate limits, do the following:
   a. In the **RATE LIMITS** tab, click the **Edit** button.

      The EDIT RATE LIMITS page displays.

   b. For each port for which you want to set rate limits, select the rate in Kbps (Kbit/s) to Mbps (Mbit/s) from the individual **Ingress** and **Egress** menus for the port.

      The default selection is **No Limit**.

   c. Click the **APPLY** button.

      Your settings are saved and the EDIT RATE LIMITS page closes.

Manage broadcast filtering and set port storm control rate limits

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

You can also set storm control rate limits for each port. Storm control measures the incoming broadcast, multicast, and unknown unicast frame rates separately on each port, and discards the frames if the rate that you set for the port is exceeded. By default, no storm control rate limit is set for a port. You can select each storm control rate limit as a predefined data transfer threshold from 512 Kbps (Kbit/s) to 512 Mbps (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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.

3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. 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. Turn on the **Broadcast Filtering** toggle.

   When broadcast filtering is enabled, the toggle displays green.
7. Click the **APPLY** button.

   Broadcast filtering is enabled. The **STORM CONTROL RATE** tab displays next to the **RATE LIMITS** tab.
8. To set storm control rate limits, do the following:
   a. Click the **STORM CONTROL RATE** tab.
   b. Click the **EDIT** button.

      The EDIT STORM CONTROL RATE options display.
   c. For each port for which you want to set storm control rate limits, select the rate in Kbps (Kbit/s) to Mbps (Mbit/s) from the individual menu for the port.

      The default selection is **No Limit**.
   d. Click the **APPLY** button.

      Your settings are saved and the EDIT STORM CONTROL RATE tab displays your new settings.

Manage individual port settings

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

Set rate limits for a port

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

You can select each rate limit as a predefined data transfer threshold from 512 Kbps (Kbit/s) to 512 Mbps (Mbit/s).

You also can set port rate limits (the same feature) as part of the QoS configuration on the switch.

- For setting port rate limits in port-based QoS mode, see Use port-based quality of service mode and set the priority and rate limits for ports on page 25.
- For setting port rate limits in 802.1/DSCP QoS mode, see Use 802.1P/DSCP quality of service mode and set the rate limits for ports on page 27.

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 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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. 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.
4. Select the port.

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

   The EDIT PORT page displays for the selected port.
6. From the **Ingress Port Limit** menu, **Egress Port Limit** menu, or both, select the rate in Kbps (Kbit/s) to Mbps (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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The user name and password are 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.
4. Select the port.

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

   The EDIT PORT page displays for the selected port.
6. In the Flow Control section, turn on or off the toggle to enable or disable flow control.

   When flow control is enabled, the toggle 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 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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. 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.
4. Select the port.

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

   The EDIT PORT page displays for the selected port.
6. Select one of the following options from the **Speed** menu:
   - **Auto**: The port speed is set automatically after the switch determines the speed using autonegotiation with the linked device. This is the default setting.
   - **Disable**: The port is shut down (blocked).
   - **10M half**: The port is forced to function at 10 Mbps with half-duplex.
   - **10M full**: The port is forced to function at 10 Mbps with full-duplex.
   - **100M half**: The port is forced to function at 100 Mbps with half-duplex.
   - **100M full**: The port is forced to function at 100 Mbps with full-duplex.

NOTE: You cannot select Gigabit Ethernet as the port speed. However, if the setting from the **Speed** menu is **Auto**, the switch can use autonegotiation to automatically set the port speed to Gigabit Ethernet if the linked device supports that speed.

7. Click the **APPLY** button.

   Your settings are saved.

Add or change the name label for a port

You can add or change a name label for a port. Name labels are for your reference only, and do not affect port behavior.

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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. 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.
4. Select the port.

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

   The EDIT PORT page displays for the selected port.
6. In the **Port Name** field, type a name label for the port.

   The name label can be from 1 to 16 characters.
7. Click the **APPLY** button.

   Your settings are saved.

4

Use VLANS for Traffic Segmentation

This chapter describes how you can use virtual LANS (VLANs) to segment traffic on the switch. It contains these sections:

- Types of supported VLANs
- Manage basic port-based VLANs
- Manage advanced port-based VLANs
- Manage basic 802.1Q VLANs
- Manage advanced 802.1Q VLANs
- Deactivate a port-based or 802.1Q VLAN mode and delete configured VLANs

Types of supported VLANs

VLANs offer many benefits, such as enhanced security, improved load balancing, better use of shared resources, and more efficient network management. You can set up one or more VLANs (virtual local area networks) on your switch to group networked member devices together as an isolated network.

To start, choose which VLAN mode you want to enable for all the VLANs that you want to set up on the switch. Select one of the following port-based or tag-based VLAN modes, listed in order from the simplest to the most advanced:

- **Port-based VLANs**: For each port-based VLAN, you select the switch ports that you want to be members of the VLAN, which creates a virtual network consisting of all the devices connected to the member ports.

  You can use port-based VLANs when this is the only switch in your network that supports VLANs, and the VLAN does not need to function across multiple network devices such as a router, a WiFi AP, or other network device that supports VLANs.

  The switch supports the following port-based VLAN modes:

  - **Basic Port-Based VLAN**: If each port (except the uplink port) only needs to belong to a single VLAN, you can use basic port-based VLANs. The number of basic port-based VLANs can be equal to, or less than, the number of ports on the switch. To set up a basic port-based VLAN, you assign the same VLAN ID to one or more ports.
  - **Advanced Port-Based VLAN**: If you want a port to belong to multiple VLANs, you can use the advanced port-based VLAN mode. To set up an advanced port-based VLAN, you assign the same VLAN ID to one or more ports to make them members of this VLAN. You can also assign other VLAN IDs to these ports to make them members of other VLANs.
- **802.1Q VLANs (tag-based)**: Tagged VLANs are more powerful than port-based VLANs, and the switch can support many more tagged VLANs than port-based VLANs. The switch supports the IEEE 802.1Q standard, and tags Ethernet frames to route VLAN traffic. When a port receives an Ethernet frame tagged for a specific VLAN, the port accepts the data if the port is a member of that VLAN. If not, then it discards the data.

  You can also use 802.1Q VLANs to route traffic from the switch to another network device on your LAN (or even outside your LAN) by configuring 802.1Q VLANs on both network devices and using the same VLAN ID. If you need a VLAN to function across multiple network devices (such as a router, another switch, a WiFi AP), we recommend that you use an 802.1Q VLAN.

  The switch supports the following 802.1Q VLAN modes:

- **Basic 802.1Q VLAN**: If you do not need custom tagging on a port, and you do not need a voice VLAN, auto-camera VLAN, or auto-WiFi VLAN, you can use the basic 802.1Q VLAN mode. When you enable basic 802.1Q VLAN mode, VLAN 1 is added to the switch and all ports are assigned as access members of VLAN 1. A port that functions in access mode can belong to a single VLAN only, and does not tag the traffic that it processes. You can assign access ports to different VLANs, or change a port to trunk mode so that it automatically belongs to all VLANs on the switch and tags the traffic that it processes.
- **Advanced 802.1Q VLAN**: If you need custom tagging on a port, or want to set up a voice VLAN, auto-camera VLAN, or auto-WiFi VLAN, you must use advanced 802.1Q VLAN mode. When you enable advanced 802.1Q VLAN mode, VLAN 1 is added to the switch and all ports are assigned as untagged members of VLAN 1. You can tag or untag ports, remove ports, add more VLANs, assign ports to different VLANs, and manage port PVIDs. You can also set up a voice VLAN, auto-camera VLAN, or auto-WiFi VLAN, .

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

Table 4. Supported VLAN modes for the GS116EP and GS116EPP

VLAN Feature	Basic Port-Based VLAN	Advanced Port-Based VLAN	Basic 802.1Q VLAN	Advanced 802.1Q VLAN
Total number of VLANs	16	16	16	64
Egress tagging	No	No	Yes (trunk port only)	Yes
Multiple VLANs on a single port	No	Yes	Yes (trunk port only)	Yes
Voice VLAN	No	No	No	Yes
Auto-Camera VLAN	No	No	No	Yes
Auto-WiFi VLAN	No	No	No	Yes

Manage basic port-based VLANs

By default, VLANs are disabled on the switch.

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

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

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

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The Quality of Service (QOS) page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.
6. In the Basic Port-Based VLAN section, click the **ACTIVATE MODE** button.

   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **CONTINUE** button.

   Your settings are saved and the pop-up window closes. By default, all VLANs are added and each port is a member of VLAN 1.
8. To assign one or more ports to other VLANs, do the following:
   a. For each port that you want to assign to another VLAN, select a VLAN ID from the **VLAN** menu for the individual port.

      Each port can be assigned to a single VLAN only. However, for the port that you want to use as the uplink port to the Internet connection or a server, select **All** from the **VLAN** menu for the individual port.
   b. Click the **APPLY** button.

      Your settings are saved.

Manage advanced port-based VLANs

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

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

- Activate the advanced port-based VLAN mode
- Create an advanced port-based VLAN
- Change an advanced port-based VLAN
- Delete an advanced port-based VLAN

Activate the advanced port-based VLAN mode

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

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

To activate the Advanced Port-Based VLAN mode:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.
6. In the Advanced Port-Based VLAN section, click the **ACTIVATE MODE** button.

   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **CONTINUE** button.

   Your settings are saved and the pop-up window closes. By default, VLAN 1 is added and all ports are members of VLAN 1.

Create an advanced port-based VLAN

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

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

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

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

   If you did not yet activate the Advanced Port-Based VLAN mode, see Activate the advanced port-based VLAN mode on page 38.
6. In the Advanced Port-Based VLAN section, click the **ADD VLAN** button.
7. Specify the settings for the new VLAN:
   - **VLAN Name**. Enter a name from 1 to 20 characters.
   - **VLAN ID**. Enter a number from 1 to the total number of ports on the switch.
   - **Ports**. Select the ports that you want to include in the VLAN through a combination of the following actions:
     - Click the icon for an unselected port to add the port to the VLAN.
     - Click the icon for a selected port to remove the port from the VLAN.
     - Click the **Select All** link to add all ports to the VLAN.
     - Click the **Remove All** link to remove all selected ports from the VLAN.

     The icon for a selected port displays purple.

NOTE: If ports are members of the same link aggregation group (LAG), you must assign them to the same VLAN. For more information, see Set up link aggregation on page 66.

8. Click the **APPLY** button.

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

Change an advanced port-based VLAN

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

To change an advanced port-based VLAN:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.
6. In the Advanced Port-Based VLAN section, click the VLAN that you want to change (you can click anywhere in the row for the VLAN) and click the **EDIT** button.

   The Advanced Port-Based VLAN pane displays.
7. Change the settings for the VLAN:
   - **VLAN Name**. Enter a name from 1 to 20 characters.

     You cannot change the VLAN ID. If you need to change the VLAN ID, delete the VLAN and create a new VLAN with another VLAN ID.
   - **Ports**. Select the ports that you want to include in the VLAN through a combination of the following actions:
     - Click the icon for an unselected port to add the port to the VLAN.
     - Click the icon for a selected port to remove the port from the VLAN.

- Click the **Select All** link to add all ports to the VLAN.
- Click the **Remove All** link to remove all selected ports from the VLAN.

  The icon for a selected port displays purple.

The icon for a selected port displays purple.

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

8. Click the **APPLY** button.

   Your settings are saved. The modified VLAN shows in the VLAN table.

Delete an advanced port-based VLAN

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

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

To delete an advanced port-based VLAN:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.
6. In the Advanced Port-Based VLAN section, click the VLAN that you want to delete (you can click anywhere in the row for the VLAN).
7. Click the **DELETE** button.

   Your settings are saved. The VLAN is deleted.

Manage basic 802.1Q VLANs

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

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

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

- Activate the Basic 802.1Q VLAN mode
- Create a basic 802.1Q VLAN and assign ports as members
- Assign the port mode in a basic 802.1Q VLAN configuration
- Change a basic 802.1Q VLAN
- Delete a basic 802.1Q VLAN

Activate the Basic 802.1Q VLAN mode

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

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

To activate the Basic 802.1Q VLAN mode:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

6. In the Basic 802.1Q VLAN section, click the **ACTIVATE MODE** button.

   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **CONTINUE** button.

   Your settings are saved and the pop-up window closes. By default, VLAN 1 is added.

   For information about adding VLANs, see Create a basic 802.1Q VLAN and assign ports as members on page 43.

   For all ports, the default selection from the **Mode** menu is **Access**. For more information about access mode and trunk mode, see Assign the port mode in a basic 802.1Q VLAN configuration on page 45.
8. If you already determined which ports must function in trunk mode, for those ports, select **Trunk (uplink)** from the **Mode** menu.
9. Click the **SAVE** button.

   Your settings are saved.

Create a basic 802.1Q VLAN and assign ports as members

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

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

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

If you did not yet activate the Basic 802.1Q VLAN mode, see Activate the Basic 802.1Q VLAN mode on page 42.

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

6. To add a VLAN and then assign ports as members of the VLAN, do the following:
   a. Click the **Edit VLAN** tab.

      The 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane displays.
   b. Click the **ADD VLAN** button.

      The BASIC 802.1Q VLAN pop-up window opens.
   c. In the **VLAN Name** field, enter a name from 1 to 20 characters.
   d. In the **VLAN ID** field, enter a number from 1 to 4093.
   e. Click the **APPLY** button.

      Your settings are saved. The new VLAN shows in the 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane.
   f. Click the **Port Configuration** tab.

      The 802.1Q PORT CONFIGURATIONS pane displays
   g. For each port that you want to make a member of the new VLAN, select the VLAN from the **VLAN** menu for the individual port.

      NOTE: If ports are members of the same LAG, you must assign them to the same VLAN.
7. For a port that functions in access mode, to add a VLAN by using the **VLAN** menu for the individual port, do the following:
   a. From the **VLAN** menu for the individual port, select **Add VLAN**.

      The BASIC 802.1Q VLAN pop-up window opens.
   b. In the **VLAN Name** field, enter a name from 1 to 20 characters.
   c. In the **VLAN ID** field, enter a number from 1 to 4093.
   d. Click the **APPLY** button.

      The pop-up window closes. The VLAN is added as a possible selection in the **VLAN** menu for each individual port.
   e. For each port that you want to make a member of the new VLAN, select the VLAN from the **VLAN** menu for the individual port.

      NOTE: If ports are members of the same LAG, you must assign them to the same VLAN.
8. Click the **SAVE** button.

Your settings are saved.

NOTE: For information about assigning the port mode, see Assign the port mode in a basic 802.1Q VLAN configuration on page 45.

Assign the port mode in a basic 802.1Q VLAN configuration

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

- **Access mode**. A port that functions in access mode can belong to a single VLAN only, and does not tag the traffic that it processes. You would typically use access mode for a port that is connected to an end device such as a gaming device, media device, or computer. When a port that functions in access mode receives data that is untagged, the data is delivered normally. When a port that functions in access mode receives data that is tagged for a VLAN other than the one the port belongs to, the data is discarded.
- **Trunk mode**. A port that functions in trunk mode automatically belongs to all VLANs on the switch and tags the traffic that it processes. You would typically use trunk mode for a port that is connected to another network device. For example, you would assign trunk mode for an uplink to another switch or router and for a downlink to a WiFi access point.

To assign the port mode:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

   If you did not yet activate the Basic 802.1Q VLAN mode, see Activate the Basic 802.1Q VLAN mode on page 42.

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

6. For each individual port that you want to change, from the **Mode** menu, select either **Trunk (uplink)** to let the port function in trunk mode or **Access** to let the port function in access mode.

   If you place a port in trunk mode, the selection from the **VLAN** menu changes to **All** because all VLANs must be supported on a trunk port.

7. Click the **SAVE** button.

   Your settings are saved.

Change a basic 802.1Q VLAN

You can change an existing basic 802.1Q VLAN.

To change a basic 802.1Q VLAN:

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

   A login window opens.

3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.

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

   The QOS page displays.

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

   The VLAN page displays.

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

6. To change the name for the VLAN, do the following:
   a. Click the **Edit VLAN** tab.

      The 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane displays.

   b. Click the VLAN that you want to change.

      You can click anywhere in the row for the VLAN.

   c. Click the **EDIT** button.

      The BASIC 802.1Q VLAN pop-up window opens.

d. Change the VLAN name.

   You cannot change the VLAN ID. If you need to change the VLAN ID, delete the VLAN and create a new VLAN with another VLAN ID.

e. Click the **APPLY** button.

   Your settings are saved. The modified VLAN shows in the 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane.

7. To change the membership of the VLAN, for each port that you want to make a member, select the VLAN from the **VLAN** menu for the individual port in the 802.1Q-BASED PORT CONFIGURATION pane.
8. Click the **SAVE** button.

   Your settings are saved.

Delete a basic 802.1Q VLAN

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

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

To delete a basic 802.1Q VLAN:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.
6. Click the **Edit VLAN** tab.

   The 802.1Q-BASED VLAN CONFIGURATIONS (BASIC MODE) pane displays.
7. Click the VLAN that you want to delete.

You can click anywhere in the row for the VLAN

8. Click the **DELETE** button.

   Your settings are saved. The VLAN is deleted.

Manage advanced 802.1Q VLANs

Advanced 802.1Q VLANs provide many options. You can tag ports, untag ports, exclude ports, add more VLANs, assign a different VLAN to a port, manage port PVIDs. When you enable advanced 802.1Q VLAN, VLAN 1 is created on the switch, and all ports become untagged members of VLAN 1.

You can set up special-purpose VLANs like a voice VLAN, auto-camera VLAN, and auto-WiFi VLAN. When you create a special-purpose VLAN, the default Organizationally Unique Identifiers (OUI) table lists OUI values associated with devices from specific manufacturers. When the switch detects a known OUI in network traffic traffic on a port that belongs to a special-purpose VLAN, it routes traffic coming from the device to the appropriate VLAN.

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

- Activate the advanced 802.1Q VLAN mode
- Create an advanced 802.1Q VLAN
- Change an advanced 802.1Q VLAN
- Specify a port PVID for an advanced 802.1Q VLAN
- Set an existing advanced 802.1Q VLAN as the voice VLAN and adjust the CoS value
- Edit the OUI table for the voice VLAN
- Set up an auto-camera VLAN on an advanced 802.1Q VLAN and adjust the CoS value
- Edit the OUI table for the auto-camera VLAN
- Set an existing advanced 802.1Q VLAN as the WiFi VLAN and adjust the CoS value
- Edit the OUI table for the auto-WiFi VLAN
- Delete an advanced 802.1Q VLAN

Activate the advanced 802.1Q VLAN mode

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

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

In an advanced 802.1Q VLAN configuration, you can set up VLANs to which you can add tagged or untagged ports. Port tagging allows a port to be associated with a particular VLAN and allows the VLAN ID tag to be added to data packets that are sent through the port. The tag identifies the VLAN that must receive the data. You can also manage the VLAN IDs (PVIDs) of the ports (see Specify a port PVID for an advanced 802.1Q VLAN on page 52).

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

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.
6. In the Advanced 802.1Q VLAN section, click the **ACTIVATE MODE** button.

   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **CONTINUE** button.

   Your settings are saved and the pop-up window closes. By default, VLAN 1 is added and all ports are made untagged members of VLAN 1.

   For information about adding VLANs, see Create an advanced 802.1Q VLAN on page 50.

   For all ports, the default selection from the **Mode** menu is **Access**. For more information about access mode and trunk mode, see Assign the port mode in a basic 802.1Q VLAN configuration on page 45.
8. To change the port tagging for a VLAN, do the following:
   a. In the Advanced 802.1Q VLAN table, click the VLAN that you want to edit.

      You can click anywhere in the row.
   b. Click the **EDIT** button.

c. Select the port tags and whether ports are members of the VLAN through a combination of the following actions:
   - **T**: Make the port a tagged member of the VLAN.
   - **U**: Make the port an untagged member of the VLAN.
   - **E**: Exclude the port from the VLAN.
   - **Tag All**: Make all ports tagged members of the VLAN.
   - **Untag All**: Make all ports untagged members of the VLAN.
   - **Exclude All**: Exclude ports from the VLAN.

d. Click the **APPLY** button.

   Your settings are saved.

Create an advanced 802.1Q VLAN

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

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

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the advanced 802.1Q VLAN mode on page 48.
6. In the right pane, click the **ADD VLAN** button.

   The Advanced 802.1Q VLAN pane displays.

7. Specify the VLAN settings and assign ports as tagged or untagged members:
   a. In the **VLAN Name** field, enter a name from 1 to 20 characters.
   b. In the **VLAN ID** field, enter a number from 1 to 4094.
   c. Use a combination of the following options to select port tags and set whether ports are members of the VLAN:
      - **T**: Make the port a tagged member of the VLAN.
      - **U**: Make the port an untagged member of the VLAN.
      - **E**: Exclude the port from the VLAN.
      - **Tag All**: Make all ports tagged members of the VLAN.
      - **Untag All**: Make all ports untagged members of the VLAN.
      - **Exclude All**: Exclude ports from the VLAN.

      NOTE: If ports are members of the same LAG, you must assign them to the same VLAN.
8. Click the **APPLY** button.

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

Change an advanced 802.1Q VLAN

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

To change an advanced 802.1Q VLAN:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.
6. In the table in the right pane, click the VLAN that you want to change.

You can click anywhere in the row for the VLAN.

7. Click the **EDIT** button.
8. Change the VLAN settings as needed:
   - In the **VLAN Name** field, enter a name from 1 to 20 characters.

     You cannot change the VLAN ID. If you need to change the VLAN ID, delete the VLAN and create a new VLAN with another VLAN ID.
   - Use a combination of the following options to select port tags and set whether ports are members of the VLAN:
     - **T**: Make the port a tagged member of the VLAN.
     - **U**: Make the port an untagged member of the VLAN.
     - **E**: Exclude the port from the VLAN.
     - **Tag All**: Make all ports tagged members of the VLAN.
     - **Untag All**: Make all ports untagged members of the VLAN.
     - **Exclude All**: Exclude ports from the VLAN.
9. Click the **APPLY** button.

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

Specify a port PVID for an advanced 802.1Q VLAN

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

NOTE: If you did not yet create an advanced 802.1Q VLAN, all ports are assigned PVID 1 and you cannot assign another PVID to a port. In this situation, first create an advanced 802.1Q VLAN (see Create an advanced 802.1Q VLAN on page 50).

To assign a PVID to a port:

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

A login window opens.

3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.

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

   The QOS page displays.

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

   The VLAN page displays.

   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the advanced 802.1Q VLAN mode on page 48.

6. In PVID Table section in the right pane, click the **PVID Table** link.

   The Port and VLAN IDs pane displays.

7. Click the icon for a port.

   A menu displays. The menu lets you select a PVID for the port.

8. From the menu, select a VLAN ID and name.

   You can select only a VLAN that the selected port is a member of.

9. Click the **APPLY** button.

   Your settings are saved. The Port and VLAN IDs pane displays again. The VLAN ID that is assigned as the PVID displays with an asterisk (*) next to the port.

10. Click the **BACK** button.

    The Advanced 802.1Q VLAN pane displays.

Set an existing advanced 802.1Q VLAN as the voice VLAN and adjust the CoS value

The switch can support a single advanced 802.1Q VLAN as the voice VLAN to facilitate voice over IP (VoIP) traffic. Because a voice VLAN might require a single port to join to multiple VLANs as an untagged member, you can set up a voice VLAN only as an advanced 802.1Q VLAN.

For information about creating an advanced 802.1Q VLAN, see Create an advanced 802.1Q VLAN on page 50.

A port that is a member of the voice VLAN sends any packet with the first 3 bytes of the MAC addresses listed in the OUI table through the voice VLAN. Other types of packets

(for example, data packets) that enter the port are forwarded according to the 802.1Q VLAN ID in the packet and the PVID setting on the port.

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

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

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the advanced 802.1Q VLAN mode on page 48.
6. In the **Advanced 802.1Q VLAN** table in the right pane, click the VLAN that you want to make the voice VLAN.

   You can click anywhere in the row to select the VLAN.
7. Click the **EDIT** button.
8. In the Voice VLAN section, turn on the **voice VLAN** toggle.

   When the voice VLAN is enabled, the toggle displays green and is positioned on the right.
9. From the **Class of Service** menu, select a CoS value.

   A value of 0 is the lowest priority and a value of 7 is the highest priority. The default value is 6.
10. View the OUI values to verify that your voice over IP (VoIP) device manufacturers are listed.

For information about viewing and changing the OUI settings, see Edit the OUI table for the voice VLAN on page 55.

11. Click the **APPLY** button.

    Your settings are saved. The voice VLAN shows in the Advanced 802.1Q VLAN pane with a telephone icon.

Edit the OUI table for the voice VLAN

The voice VLAN is a specialized advanced 802.1Q VLAN that uses a configurable list of Organizationally Unique Identifiers (OUI) to recognize VoIP phones from specific manufacturers. When a switch port that is a member of the voice VLAN receives a packet, it searches the voice VLAN's OUI table to see whether the originating device is listed, and if so, the port forwards the packet to the voice VLAN. In this way, the OUI table helps voice VLAN member ports forward all voice traffic from VoIP phones to the voice VLAN.

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

To edit the OUI table for the voice VLAN:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the advanced 802.1Q VLAN mode on page 48.
6. In the **Advanced 802.1Q VLAN** table in the right pane, click the VLAN that you set as the voice VLAN.

   You can click anywhere in the row to select the VLAN.

If you did not yet set a voice VLAN mode, see Set an existing advanced 802.1Q VLAN as the voice VLAN and adjust the CoS value on page 53.

7. Click the **EDIT** button.
8. In the OUI Table section, click the **OUI Settings** link.

   The Voice VLAN pane displays and shows the OUI table.
9. To add a new OUI, do the following:
   a. Click the **ADD OUI** button.

      The OUI Entry page displays.
   b. Enter the new OUI and description.
   c. Click the **APPLY** button.

      Your settings are saved.
10. To change an existing OUI, do the following:
    a. Select the OUI that you want to change and click the **EDIT** button.
    b. Change the OUI, the description, or both.
    c. Click the **APPLY** button.

       Your settings are saved.
11. To delete an OUI that you no longer need, select the OUI and click the **DELETE** button.

    Your settings are saved and the OUI is deleted.
12. Click the **BACK** button.

    The Advanced 802.1Q VLAN pane displays and shows the voice VLAN settings.
13. Click the **APPLY** button.

    Your settings are saved.

Set up an auto-camera VLAN on an advanced 802.1Q VLAN and adjust the CoS value

You can set up an auto-camera VLAN to provide a better quality of service for network traffic originating from IP surveillance cameras and automatically enable multicast for those devices, as required by many IP camera systems. Before proceeding, you must enable advanced 802.1Q VLAN mode and set up an advanced 802.1Q VLAN to serve as the auto-camera VLAN. For information on how to set up an advanced 802.1Q VLAN, see Create an advanced 802.1Q VLAN on page 50.

If you set up an auto-camera VLAN on your network, each port that is a member searches the OUI table for the first 3 bytes of the client device's MAC address listed in a received packet, and if found, it forwards the packet to the auto-camera VLAN. The port forwards other packets according to the PVID setting on the port and the packet's 802.1Q VLAN ID.

The default Class of Service (CoS) value for the auto-camera VLAN is 6, which you can adjust to any value from 0 (lowest priority) to 7 (highest priority). The auto-camera VLAN CoS only applies to traffic routed to the auto-camera VLAN.

NOTE: Although the default VLAN (VLAN 1) has features designed to support network administration, you can configure it as the auto-camera VLAN if there is no need to reserve VLAN 1 for administrative purposes. If you decide to do this, be sure to preserve access from the computing device that you're using to configure the switch

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

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the advanced 802.1Q VLAN mode on page 48.
6. In the **Advanced 802.1Q VLAN** table in the right pane, click the VLAN that you want to make the auto-camera VLAN.

   You can click anywhere in the row to select the VLAN.
7. Click the **EDIT** button.
8. In the Auto-Camera VLAN section, turn on the **Auto-Camera VLAN** toggle.

   When the auto-camera VLAN is enabled, the button displays green and is positioned on the right.
9. From the **Class of Service** menu, select a CoS value.

A value of 0 is the lowest priority and a value of 7 is the highest priority. The default value is 6.

10. View the **OUI Table** to verify that your IP camera manufacturer is listed.

    For information about viewing and changing the OUI settings, see Edit the OUI table for the auto-camera VLAN on page 58.

11. Click the **APPLY** button.

    Your settings are saved. The auto-camera VLAN shows in the Advanced 802.1Q VLAN pane with a camera icon.

Edit the OUI table for the auto-camera VLAN

For the auto-camera VLAN, the switch supports default Organizationally Unique Identifiers (OUI), which are associated with cameras from specific manufacturers. All traffic received on auto-camera VLAN ports from surveillance cameras with a listed OUI is forwarded on the auto-camera VLAN.

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

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

To edit the OUI table for the auto-camera VLAN:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the advanced 802.1Q VLAN mode on page 48.

6. In the **Advanced 802.1Q VLAN** table in the right pane, click the VLAN that you set as the auto-camera VLAN.

   You can click anywhere in the row to select the VLAN.

   If you did not yet set an auto-camera VLAN mode, see Set up an auto-camera VLAN on an advanced 802.1Q VLAN and adjust the CoS value on page 56.
7. Click the **EDIT** button.
8. In the OUI Table section, click the **OUI Settings** link.

   The Auto-Camera VLAN pane displays and shows the OUI table.
9. To add a new OUI, do the following:
   a. Click the **ADD OUI** button.

      The OUI Entry page displays.
   b. Enter the new OUI and description.
   c. Click the **APPLY** button.

      Your settings are saved.
10. To change an existing OUI, do the following:
    a. Select the OUI that you want to change and click the **EDIT** button.
    b. Change the OUI, the description, or both.
    c. Click the **APPLY** button.

       Your settings are saved.
11. To delete an OUI that you no longer need, select the OUI and click the **DELETE** button.

    Your settings are saved and the OUI is deleted.
12. Click the **BACK** button.

    The Advanced 802.1Q VLAN pane displays and shows the auto-camera VLAN settings.
13. Click the **APPLY** button.

    Your settings are saved.

Set an existing advanced 802.1Q VLAN as the WiFi VLAN and adjust the CoS value

The switch can support a single advanced 802.1Q VLAN as the auto-WiFi VLAN to facilitate traffic to WiFi devices. You can set up a auto-WiFi VLAN only as an advanced 802.1Q VLAN. For information about creating an advanced 802.1Q VLAN, see Create an advanced 802.1Q VLAN on page 50.

A port that is a member of the auto-WiFi VLAN sends any packet with the first 3 bytes of the MAC addresses listed in the OUI table through the auto-WiFi VLAN. Other types of packets (for example, data packets) that enter the port are forwarded according to the 802.1Q VLAN ID in the packet and the PVID setting on the port.

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

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

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the advanced 802.1Q VLAN mode on page 48.
6. In the **Advanced 802.1Q VLAN** table in the right pane, click the VLAN that you want to make the auto-WiFi VLAN.

   You can click anywhere in the row to select the VLAN.
7. Click the **EDIT** button.
8. In the auto-WiFi VLAN section, turn on the **Auto-WiFi VLAN** toggle.

   When the auto-WiFi VLAN is enabled, the bar displays green and is positioned on the right.
9. From the **Class of Service** menu, select a CoS value.

   A value of 0 is the lowest priority and a value of 7 is the highest priority. The default value is 6.
10. View the OUI values to verify that your WiFi devices manufacturers are listed.

For information about viewing and changing the OUI settings, see Edit the OUI table for the auto-WiFi VLAN on page 61.

11. Click the **APPLY** button.

    Your settings are saved. The auto-WiFi VLAN shows in the Advanced 802.1Q VLAN pane with a WiFi icon.

Edit the OUI table for the auto-WiFi VLAN

For the auto-WiFi VLAN, the switch supports default Organizationally Unique Identifiers (OUI), which are associated with WiFi devices from specific manufacturers. All traffic received on auto-WiFi VLAN ports from WiFi devices with a listed OUI is forwarded on the auto-WiFi VLAN.

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

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

To edit the OUI table for the auto-WiFi VLAN:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.

   If you did not yet activate the Advanced 802.1Q VLAN mode, see Activate the advanced 802.1Q VLAN mode on page 48.
6. In the **Advanced 802.1Q VLAN** table in the right pane, click the VLAN that you set as the auto-WiFi VLAN.

   You can click anywhere in the row to select the VLAN.

If you did not yet set an auto-WiFi VLAN mode, see Set an existing advanced 802.1Q VLAN as the WiFi VLAN and adjust the CoS value on page 59.

7. Click the **EDIT** button.
8. In the OUI Table section, click the **OUI Settings** link.

   The Auto-WiFi VLAN pane displays and shows the OUI table.
9. To add a new OUI, do the following:
   a. Click the **ADD OUI** button.

      The OUI Entry page displays.
   b. Enter the new OUI and description.
   c. Click the **APPLY** button.

      Your settings are saved.
10. To change an existing OUI, do the following:
    a. Select the OUI that you want to change and click the **EDIT** button.
    b. Change the OUI, the description, or both.
    c. Click the **APPLY** button.

       Your settings are saved.
11. To delete an OUI that you no longer need, select the OUI and click the **DELETE** button.

    Your settings are saved and the OUI is deleted.
12. Click the **BACK** button.

    The Advanced 802.1Q VLAN pane displays and shows the auto-WiFi VLAN settings.
13. Click the **APPLY** button.

    Your settings are saved.

Delete an advanced 802.1Q VLAN

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

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

To delete an advanced 802.1Q VLAN:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The QOS page displays.
5. From the menu on the left, select **VLAN**.

   The VLAN page displays.
6. In the table in the right pane, click the VLAN that you want to delete.

   You can click anywhere in the row for the VLAN.
7. Click the **DELETE** button.

   Your settings are saved. The VLAN is deleted.

Deactivate a port-based or 802.1Q VLAN mode and delete configured VLANs

If you activated any of the VLAN modes, such as the Basic Port-Based VLAN mode, Advanced Port-Based VLAN mode, Basic 802.1Q VLAN mode, or Advanced 802.1Q VLAN mode, you can deactivate the VLAN mode and delete all VLANs.

To deactivate 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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

The password is the one that you specified the first time that you logged in. 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 configuration settings will be lost.

7. Click the **CONTINUE** button.

   Your settings are saved, the pop-up window closes, and all VLANs are deleted.

5

Manage the Switch in Your Network

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

The chapter contains the following sections:

- Manage Universal Plug and Play
- Set up link aggregation
- Manage multicast
- Change the IP address of the switch
- Reenable the DHCP client of the switch

Manage Universal Plug and Play

A NETGEAR device or application 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 device UI 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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **SWITCH DISCOVERY**.

   The SWITCH DISCOVERY page displays.
6. In the UPnP section, turn on or off the toggle to enable or disable UPnP.

   When UPnP is enabled, the toggle displays green.
7. Click the **APPLY** button.

   Your settings are saved.

Set up link aggregation

Link aggregation on the switch allows you to combine multiple Ethernet ports into a single logical link. Network devices treat the link aggregation group (LAG) as a single link, which increases throughput, fault tolerance, or both, between devices. 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 GS116EP and GS116EPP switches each support 8 LAGs with up to 16 ports each, which means that one LAG can support a link of up to 8 Gbps.

Set up a link aggregation on the switch by performing this series of tasks:

1. Set up the LAG on the switch.

- For a static LAG see: Set up a static link aggregation group on page 67.
- For a dynamic LAG, see: Set up a dynamic link aggregation group on page 69.

2. Connect the ports that must be members of the LAG on the switch to the ports that must be members of the LAG on *another* device in your network (see Make a link aggregation connection on page 67).
3. Enable the LAG on the switch (see Enable a link aggregation group on page 70) and on the other device.

Make a link aggregation connection

Before you make a physical link aggregation connection to another network device (usually a router or another switch) that also supports link aggregation, you must first set up a LAG on the switch. 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 29.

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

Using Ethernet cables, connect each port that must be a member of the LAG on the switch to each port that must be a member of the same LAG on another network device.
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.
- The ports use the same speed, full duplex mode, and flow control setting as the ports in the LAG on the switch.

Set up a static link aggregation group

Set up a static link aggregation group (LAG) to combine multiple Ethernet links into a single logical link between two networked devices.
For a LAG to function, you must:

- Set up the LAG on the switch, as described in this task.
- Connect the ports that must be members of the LAG on the switch to the ports that must be members of the LAG on *another* device in your network (see Make a link aggregation connection on page 67).
- Enable the LAG on the switch (see Enable a link aggregation group on page 70) and on the connected device.

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 device management password.

   The password is the one that you specified the first time that you logged in. 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 **16**.

   The icon for a selected port displays purple.

   A LAG must consist of at least two ports.
8. Verify that the **Static/LACP** toggle is turned off.

   By default, static LAG is enabled, so that the toggle displays white and is positioned on the left.
9. Click the **APPLY** button.

   Your settings are saved.

Set up a dynamic link aggregation group

Set up a dynamic link aggregation group (LAG) to combine multiple Ethernet links into a single logical link between two networked devices. Dynamic LAGs use Link Aggregation Control Protocol (LACP), which helps to prevent errors in the LAG setup.

For a LAG to function you 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 29 for information about changing these settings on the switch).
- Set up a physical link aggregation connection (see Make a link aggregation connection on page 67).
- Select the ports on the switch that must participate in the LAG, as described in this task.
- Enable the LAG on the switch and on the connected network device.

To set up a dynamic LAG on the switch:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. 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 **16**.

   The icon for a selected port displays purple.

   A LAG must consist of at least two ports.
8. To enable a dynamic LAG, turn on the **Static/LACP** toggle.

When the LAG is set up as a dynamic LAG, the toggle displays green and is positioned on the right.

9. Click the **APPLY** button.

   Your settings are saved.

   Now that the LAG ports are selected, you must set up the physical link aggregation connection. For more information, see Make a link aggregation connection on page 67.

Enable a link aggregation group

After you set up a link aggregation group (see Set up a static link aggregation group on page 67 or Set up a dynamic link aggregation group on page 69) and make a physical link aggregation connection (see Make a link aggregation connection on page 67), you can enable the link aggregation group.

NOTE: You must also enable the LAG on the other network device.

To enable a LAG on the switch:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. 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 LAG that you want to enable.

   A green check mark displays for the selected LAG.
7. To enable the LAG, turn on the **Disable/Enable** toggle.

   When the LAG is enabled, the toggle displays green and is positioned on the right.
8. To enable LACP, turn on the **Static/LACP** toggle.

   When LACP is enabled, the toggle displays green and is positioned on the right.

9. Click the LAG ports that you want to select.

   A selected port displays purple.
10. Click the **APPLY** button.

    Your settings are saved.

View link aggregation group status

You can view the status of all link aggregation groups on the switch at a glance.

To view all LAGs on the switch:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.

   The LAG section displays the link status and ports that participate in the link aggregation group.

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 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

IGMP snooping is disabled by default.

To manage IGMP snooping:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **MULTICAST**.

   The MULTICAST page displays.
6. In the IGMP Snooping section, turn on or off the toggle to enable or disable IGMP snooping.

   When IGMP snooping is enabled, the toggle displays green.
7. Click the **APPLY** button.

   Your settings are saved.

Enable a VLAN for IGMP snooping

You can enable IGMP for a VLAN only if you enabled a port-based VLAN mode or an 802.1Q VLAN mode (see Use VLANS for Traffic Segmentation on page 34).

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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **MULTICAST**.

The MULTICAST page displays.

6. In the VLAN ID Enabled for IGMP Snooping section, enter a VLAN ID in the field.

   If you enabled either a port-based VLAN mode or an 802.1Q VLAN mode, the default VLAN for IGMP snooping is VLAN 1.

7. Click the **APPLY** button.

   Your settings are saved.

Manage blocking of unknown multicast addresses

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

To manage blocking of unknown multicast addresses:

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

   A login window opens.

3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.

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

   The Quality of Service (QoS) page displays.

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

   The MULTICAST page displays.

6. In the Block Unknown Multicast Address section, turn on or off the toggle to enable or disable blocking of unknown multicast traffic.

   When blocking of unknown multicast traffic is enabled, the toggle 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 type of service (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, the 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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **MULTICAST**.

   The MULTICAST page displays.
6. In the Validate IGMPv3 IP Header section, turn on or off the toggle to enable or disable IGMPv3 IP header validation.

   When IGMPv3 IP header validation is enabled, the toggle 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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SWITCHING**.

   The Quality of Service (QoS) page displays.
5. From the menu on the left, select **MULTICAST**.

   The MULTICAST page displays.
6. From the menu in the IGMP Snooping Static Router Port section, select a specific port as the router port or select **Any** to let IGMP Join and Leave messages be sent to every port on the switch.

   Typically, the uplink port (that is, the port that is connected to your router or to the device that provides your Internet connection) serves as the router port.
7. Click the **APPLY** button.

   Your settings are saved.

Change the IP address of the switch

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

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

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.

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

   The IP address fields display, but you cannot change them yet. The toggle in the DHCP section displays green because the DHCP client of the switch is enabled.
5. Turn off the toggle in the DHCP section.

   The toggle displays gray, indicating that the DHCP client of the switch is disabled, and you can now change the IP address fields.
6. Enter the fixed (static) IP address that you want to assign to the switch and the associated subnet mask and gateway IP address.
7. Click the **APPLY** button.

   A message displays to confirm that the IP address changed.

   If the IP address of the switch changes, your web session disconnects, and you must log back in to the device UI.

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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. Select **IP Address (Fixed IP)**.

   The toggle in the DHCP section displays gray because the DHCP client of the switch is disabled.
5. Turn on the toggle in the DHCP section.

   The toggle 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 message displays to confirm that the IP address settings changed.

The switch receives an IP address from a DHCP server (or a router that functions as a DHCP server) in your network. If the IP address of the switch changes, your web session disconnects, and you must log back in to the device UI.

6

Maintain and Monitor the Switch

This chapter describes how you can maintain and monitor the switch, and contains these sections:

- View system information
- View switch connections
- View the status of a port
- Change the switch device name
- View system uptime
- Control the port LEDs
- Update the firmware on the switch
- Manage the configuration file
- Use the device UI to reboot the switch
- Return the switch to its factory default settings
- Control access to the device UI
- Change or lift access restrictions to the switch
- HTTP and HTTPS management access
- Manage the DoS prevention mode
- Manage the power saving mode
- Change the device management password
- Date and time settings
- Power over Ethernet

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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. Select **System Info**.

   The system information fields display.

View switch connections

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

To see the number of connections on the switch:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The user name and password are 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 port status and drill down for details about the 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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. 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.
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 (if the QoS mode on the switch is port-based), setting the port speed (by default, the speed is set automatically), enabling flow control, and changing the port name label, see Manage individual port settings on page 29.

Change the switch device name

By default, the device name of the switch is the same as the model number. This device name shows in, for example, in 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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

The password is the one that you specified the first time that you logged in. The password is case-sensitive.

The HOME page displays.

4. Select **System Info**.

   The System Info fields display.

5. In the **Switch Name** field, enter a new name for the switch.
6. Click the **APPLY** button.

   Your settings are saved.

View system uptime

You can view the length of time that the switch has been up and running in hours, minutes, and seconds.

To view uptime for the switch:

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

   A login window opens.

3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.

4. In the SYSTEM TIME section, click the down arrow to expand the menu.

   The System Uptime section displays the amount of time that the switch has been up and running.

Control the port LEDs

You can turn the port LEDs on the switch on and off by using the device UI.

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

To control the port LEDs through the device UI:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. Select **Port LEDs**.

   The Port LEDs button displays.

   NOTE: You can also access the port LEDs controls through **SETTINGS > LEDS > PORT LEDS**.
5. Turn on or off the toggle to enable or disable the port LEDs.

   When the port LEDs are ON (LEDs active), the toggle displays green. When the ports LEDs are OFF (Stealth Mode), the toggle displays gray.
6. Click the **APPLY** button.

   Your settings are saved.

Update the firmware on the switch

The switch firmware does not update automatically, so you must update it manually. You can manually check for the latest firmware version, download the firmware, and upload it to the switch.

CAUTION: We recommend that you read the release notes before updating the switch's firmware.

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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

The HOME page displays.

4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **FIRMWARE**.

   The FIRMWARE page displays. The page also shows the UPDATE FIRMWARE section.

   The FIRMWARE VERSION displays the current firmware version of the switch.
6. To check if new firmware is available, click the **netgear.com** link in the FIRMWARE section.

   A NETGEAR web page opens.
7. Click the **Downloads** button.
8. 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.
9. 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 `GS116EPP_V1.0.0.1.bin`.
10. Click the **UPDATE** button.

    A pop-up window displays a warning and the firmware update process starts.

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

    Your switch web session is disconnected and you must log back in to the device UI.

Manage the configuration file

The switch stores its configuration settings in a configuration file. You can back up your switch's configuration settings by saving the configuration file to your computer. Later, if you need to restore your settings, you can load the saved configuration file from your computer to the switch.

Back up the switch configuration

You can save a copy of the switch's current configuration settings to your computer so that you can restore the configuration settings from this backup file later if needed.

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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **CONFIGURATION FILE**.

   The RESTORE CONFIGURATION page displays.
6. Click the **BACKUP** tab.

   The BACKUP CONFIGURATION page displays.
7. Click the **BACKUP** button.
8. Follow the directions in your browser to save the file.

   The default name of the backup file is based on the switch model, for example: `GS116EPP.cfg`.

Restore the switch configuration

If you saved a back up of the switch's configuration file, you can load this file from your computer on to the switch to restore the configuration.

To restore the configuration settings of the switch from a back up file:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **CONFIGURATION FILE**.

   The RESTORE CONFIGURATION page displays.

6. Click the purple file icon, navigate to the saved configuration file, and select it.

   The name of the saved configuration file is based on the switch model, for example: `GS116EPP.cfg`.

   The **RESTORE** button changes to the **APPLY CONFIGURATION** button.
7. Click the **APPLY CONFIGURATION** button.

   A pop-up window displays a warning.
8. Click the **CONTINUE** button.

   The configuration is uploaded to the switch.

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

   Your switch web session is disconnected and you must log back in to the device UI.

Use the device UI to reboot the switch

To reboot the switch using the device UI:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **REBOOT SWITCH**.

   The REBOOT SWITCH page displays.
6. Click the **REBOOT** button.

   A warning pop-up window opens.
7. Click the **CONTINUE** button.

   The switch reboots.

WARNING: Do not interrupt the network connection or power to the switch during the reboot process. Do not disconnect any Ethernet cables or power off the switch until the switch reboot is complete. Doing so can damage the switch.

Return the switch to its factory default settings

You can reset the switch to return it to factory default settings, using either the **RESET** button on the front of the switch, or the reset function in the device UI. If you have 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 121.

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

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

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

Use the device UI 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 device UI:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
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. Doing so can damage the switch.

Control access to the device UI

You can control which IP address or IP addresses are allowed to access the switch through the device UI for management purposes.

To control management access to the device UI:

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

   A login window opens.

3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **ACCESS CONTROL**.

   The ACCESS CONTROL page displays any allowed IP addresses.
6. Click the **ADD** button.
7. Specify the IP address or IP addresses to allow:
   - **IP Address**. Enter a single IP address or a network IP address.

     Enter a network IP address in the format x.x.x.0, for example, 192.168.100.0.
   - **Mask**. If you enter a single IP address, enter **255.255.255.255** as the mask. If you enter a network IP address, enter **255.255.255.0** as the mask.

   NOTE: First add the IP address of the computing device that you are using to configure the switch so you can ensure your own access to the switch UI.
8. Click the **APPLY** button.

   Your settings are saved.
9. To enter more IP addresses, repeat the previous three steps.

Change or lift access restrictions to the switch

If you set up IP addresses that are allowed to access the switch through the device UI for management purposes, you can remove one or more IP addresses, or you can remove all IP addresses to lift the access restrictions.

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

To change or lift access restrictions to the switch:

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

   A login window opens.
3. Enter the device management password.

The password is the one that you specified the first time that you logged in. The password is case-sensitive.

The HOME page displays.

4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **ACCESS CONTROL**.

   The ACCESS CONTROL page displays.
6. Click the IP address that you want to remove.

   The DELETE button displays.
7. Click the **DELETE** button.

   The IP address is removed from the list, and access to the switch's device UI from the IP address is blocked.
8. To remove more IP addresses, repeat steps 6 and 7.

   CAUTION: If you remove all IP addresses, all access restrictions are removed and any IP address can access the device UI of the switch.

HTTP and HTTPS management access

You can configure HTTP and HTTPS to allow management access to the switch's device UI on a web browser. You can enable one or both options.

- HTTP is the default, and is simpler to use. You can use HTTP to log in to the device UI from within the same network subnet.
- HTTPS is more secure, but requires a dedicated HTTPS port. You can enable this option when you want to provide network administrators with remote management access to the switch. You might want to generate an SSL certificate before you enable HTTPS so that you can avoid seeing a browser security message every time you use HTTPS to log into the device UI.

For each option, you can set the maximum time that a management login session can remain idle before it times out, and set the maximum number of concurrent management sessions.

Configure HTTP access settings

You can choose to enable or disable web access to the switch's device UI through HTTP, set the session timeout, and maximum number of HTTP sessions. HTTP is enabled by default.

To configure the HTTP access settings:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **GUI ACCESS**.

   The HTTP Configuration page displays. Set one or more of the following options.
6. Turn on or off the **Admin Mode** toggle to enable or disable remote access through HTTP.

   When the setting is enabled, the toggle displays green and is positioned on the right.
7. In the **HTTP Session Timeout (Minutes)** field, type the number of minutes that a session can be idle before the session times out.

   The default is 30. The range is 0 to 60.
8. In the **Maximum Number of HTTP Sessions** field, set the number of concurrent sessions allowed.

   You can set a number from 1 to 4. For example, if you manage your home office or small business network yourself, you might set this to 1. The default is 4.
9. When your settings are complete, click the **APPLY** button.

   Your settings are applied.

Configure HTTPS access settings

You can choose to enable or disable web access to the switch's device UI through HTTPS for remote network administration. You must select the HTTPS port you want to use for

remote access, set the session timeout, and maximum number of HTTPS sessions. HTTPS is disabled by default.

NOTE: Secure HTTP (HTTPS) enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. When you manage the switch over the device UI, HTTPS can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks. The hash algorithms that SSL uses are MD5 and SHA-1.

NOTE: You can download SSL certificates only when HTTPS is disabled.

To configure the HTTPS access settings:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **GUI ACCESS**.

   The HTTPS Configuration page displays.
6. Click the **HTTPS Configuration** tab.
7. Click the **Admin Mode** button to enable or disable remote access through HTTPS.

   When this setting is enabled, the button displays on the right side of the slide, and the slide turns green.
8. In the **HTTPS Port field**, type in the number of the port.

   The default is port 443, or you can set a number in the range from 1025 to 65535.
9. In the **HTTPS Session Timeout (Minutes)** field, type the number of minutes that a session can be inactive before it times out.

   The default is 30. The range is 0 to 60.
10. In the **Maximum Number of HTTPS Sessions** field, set the number of concurrent sessions allowed.

    The default is 4. The range is 1 to 4.
11. When your settings are complete, click the **APPLY** button.

    Your settings are applied.

Browser security message with HTTPS access

After you enable HTTPS access and you attempt to access the device UI, your browser might display a security warning because of the self-signed certificate on the switch. This is expected behavior. You can proceed, or add an exception for the security warning.

NOTE: To avoid encountering a security message again, you can configure an SSL certificate. For more information, see Manage certificates for HTTPS access on page 92.

To proceed with a security warning or add an exception for a security warning::

- **Google Chrome**: Click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the domain name or IP address of the device.
- **Apple Safari**: Click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window displays, click the **Visit Website** button. If another pop-up window displays to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
- **Mozilla Firefox**: Click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
- **Microsoft Edge**: Select **Details > Go on to the webpage**.
- **Microsoft Internet Explorer**: Click the **Continue to this website (not recommended)** link.

NOTE: To prevent a security warning, you can configure and install an SSL certificate on the switch. For more information, see Manage certificates for HTTPS access on page 92 and Update the HTTPS server certificate on page 93.

Manage certificates for HTTPS access

You can manage certificates for HTTPS access. After you generate and install a valid certificate, browser security messages no longer display.

NOTE: HTTPS must be disabled before you can generate a certificate. For more information, see Configure HTTPS access settings on page 90.

To generate an SSL certificate:

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

   A login window opens.
3. Enter the device management password.

The password is the one that you specified the first time that you logged in. The password is case-sensitive.

The HOME page displays.

4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **GUI ACCESS**.

   The HTTP Configuration page displays.
6. Click the **Certificate Configuration** tab.
7. In the Certificate Management section, click the **Generate Certificates** radio button.
8. Click the **APPLY** button.

   The Certificate Generation Status field displays **Certificate generation in progress**.

   When the certificate is generated, the Certificate Present field displays **Yes**.

   You can now enable HTTPS.

Update the HTTPS server certificate

You can update the HTTPS server certificate PEM file. After you generate and install a valid certificate, browser security messages no longer display.

NOTE: HTTPS must be disabled before you can update a HTTPS server certificate PEM file. For more information, see Configure HTTPS access settings on page 90.

To update the HTTPS server certificate PEM file:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **GUI ACCESS**.

   The HTTP Configuration page displays.
6. Click the **Certificate Configuration** tab.
7. In the Certificate Update section, click the purple file icon.

8. In the **File name** field, select the PEM file or type in the PEM file name, including the .pem extension, and click **Open**.
9. Click the **UPDATE** button.

Delete certificates for HTTPS access

You can delete previously created certificates for HTTPS access.

NOTE: You must disable HTTPS before you can delete a certificate. For more information, see Configure HTTPS access settings on page 90.

To delete an SSL certificate:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **GUI ACCESS**.

   The HTTP Configuration page displays.
6. Click the **Certificate Configuration** tab.
7. Click the **Delete Certificates** radio button.
8. Click the **APPLY** button.

   The Certificate Generation Status field displays No certificate generation in progress.

   When the certificate is deleted, the Certificate Present field displays No.

Manage the DoS prevention mode

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

To manage the DoS prevention mode:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **DOS PREVENTION**.

   The DOS PREVENTION page displays.
6. Turn on or off the toggle to enable or disable the DoS prevention mode.

   When the DoS prevention mode is enabled, the toggle displays green.
7. Click the **APPLY** button.

   Your settings are saved.

Manage the power saving mode

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

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

By default, the power saving mode is disabled.

To manage the power saving mode on the switch:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **POWER SAVINGS MODE**.

   The POWER SAVING page opens.
6. Turn on or off the toggle to enable or disable the power saving mode.

   When the power saving mode is enabled, the toggle displays green.
7. Click the **APPLY** button.

   Your settings are saved.

Change the device management password

The default password to access the device UI of the switch is **password**. The first time that you log in to the switch, you must change the default password. In this manual, we call the password to access the device UI the *device management password*.

You can change the password again. 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 device management password:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

The HOME page displays.

4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **CHANGE PASSWORD**.

   The CHANGE PASSWORD page displays.
6. In the **Current Password** field, type the current password for the switch.
7. Type the new password in the **New Password** field and in the **Retype New Password** field.
8. Click the **APPLY** button.

   Your settings are saved. Keep the new password in a secure location so that you can access the switch in the future.

Date and time settings

You can set the system time manually, or enable Simple Network Time Protocol (SNTP) to allow the switch to automatically synchronize its internal clock with the time provided by an SNTP server.

If you want to automate SNTP time syncing, you must configure the SNTP client mode, configure one or more SNTP servers, and then enable system time syncing.

Configure the system time manually

To set the system time manually:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. In the SYSTEM TIME section, click the down arrow to expand the menu.

   The system time options display.
5. Select **Local**.

   The toggle displays gray and is positioned on the left.

6. Click in the **Date** field and select the date from the pop-up menu.

   The date field displays the date that you set.
7. Click in the **Time** field and select the time from the pop-up menu.

   The time field displays the time that you set.
8. Click the **APPLY** button.

   Your settings are saved.

   The current system date and time display next to the menu icon.

Enable system time to synchronize with an SNTP server

The local system time on the switch can be set to sync with an SNTP server when the following conditions are met:

- The SNTP client mode is configured.
- The switch can contact a configured SNTP server.

NOTE: If you did not configure an SNTP server before enabling SNTP on the switch, the switch sets the SNTP Server Configuration fields to a NETGEAR time server, such as time-a.netgear.com.

For more information on configuring SNTP servers, see Configure an SNTP server on page 100.

To enable system time to synchronize with SNTP server time:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. In the SYSTEM TIME section, click the down arrow to expand the menu.

   The system time options display.
5. Click the **SNTP** toggle to turn it green.
6. From the **Time Zone** menu, select the time zone in which the switch operates.
7. Click the **APPLY** button.

Your settings are saved.

The current system date and time display next to the menu icon.

Configure the SNTP client mode

You can configure the SNTP client mode as unicast or broadcast.

NOTE: Automated time syncing depends on the switch knowing how to contact your SNTP servers, and then activating automated time syncing. For more information, see Configure an SNTP server on page 100 and Enable system time to synchronize with an SNTP server on page 98.

To enable SNTP client mode and configure it for unicast or broadcast:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **TIME**.

   The SNTP options display.
6. Click the **SNTP Configuration** tab.

   The SNTP Configuration options display.
7. Under Client Mode, select the mode of operation of the SNTP client:
   - **Broadcast**: If there is a time server on your network, then you can enable broadcast. The SNTP client on the switch listens for time packets that the server broadcasts to the network.

     If you enable this option, skip to Step 13.

     NOTE: We recommend that the broadcast client mode be enabled only by professional network admins or installers with an advanced understanding of network security.
   - **Unicast**: The SNTP client sends a request to a external public SNTP server, or a pool of time servers, such as an SNTP server provided by your ISP. The SNTP server responds with the time, and the switch calculates and sets the local system time by factoring in the round-trip and local time zone offset relative to the SNTP

server time, which is usually in UTC (equivalent to Greenwich Meridian Time). The default value is Unicast.

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

   For more information, see Configure an SNTP server on page 100.

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

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

10. In the **Unicast Poll Interval** field, specify the number of seconds between unicast poll requests expressed as a power of 2. The allowed range is 6 to 10. The default value is 6.

11. In the **Unicast Poll Timeout** field, specify the number of seconds to wait for an SNTP response to a unicast poll request.

    The allowed range is 1 to 30. The default value is 5.

12. In the **Unicast Poll Retry** field, specify the number of times to retry a unicast poll request to an SNTP server after the first time-out before the switch attempts to use the next configured server.

    The allowed range is 0 to 10. The default value is 2.

13. Click the **APPLY** button.

    Your settings are saved.

Configure an SNTP server

You can enable automatic syncing of system time after you configure at least one SNTP server providing you also:

- Configure the SNTP client mode to use either a public SNTP server, or a clock and SNTP server within your own network. For more information, see Configure the SNTP client mode on page 99.
- Activate automated time management. For more information, see Enable system time to synchronize with an SNTP server on page 98.

NOTE: If you did not configure an SNTP server before enabling SNTP on the switch, the switch sets the SNTP Server Configuration fields to a NETGEAR time server, such as time-a.netgear.com.

To configure an SNTP server:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **TIME**.

   The SNTP options display.
6. Click the **SNTP Server Configuration** tab.
7. Click the **Add** button.

   The SNTP server configuration menu options display.
8. From the **Server Type** menu, select either IPv4 or DNS.
9. In the **Address** field, enter the address in the format compatible with Server Type.
10. In the **Port** field, enter the number of the port to use for UDP transmissions: 123, or 1025 to 36465.

    For unicast transmissions between the SNTP client and an external SNTP server, this port must be open in the firewall to allow access.

    When the SNTP client mode is broadcast, only allow the internal SNTP server to access the port.
11. In the **Priority** field, set a priority from 1 to 3, with the lowest number assigned to the preferred SNTP server.
12. In the **Version** field, set the SNTP version from 1 to 4.
13. Click the **APPLY** button.

    Your settings are saved.

    The SNTP server information displays in a table.

Configure daylight saving time

To configure the daylight saving time manually:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **TIME**.

   The SNTP options display.
6. Click the **Daylight Saving (DST) Configuration** tab.

   The Daylight Saving configuration options display.
7. In the **Daylight Saving (DST) Configuration** section, click the radio button for your preferred option.

   a. **Disable**: Daylight Saving is disabled by default.

   b. **Recurring**: Manually configure the yearly recurrence of the daylight savings schedule for your location, including the start and end of the recurrence, the amount of time offset, and the time zone.

      - Week: Select the week that daylight savings begins or ends.
      - Day: Select the day of the week that daylight savings begins or ends.
      - Month: Select the month in which daylight savings begins or ends.
      - Hours: Select the daylight savings time offset in hours.
      - Minutes: Select the daylight savings time offset in hours, for example, 30 minutes.
      - Zone: Select the time zone for your location.

   c. **Recurring EU**: Set the time zone to your EU location.

      Fields display the start and end days and offset times for your zone.

   d. **Recurring USA**: Set the time zone to your US location.

      Fields display the start and end days and offset times for your zone.

   e. **Nonrecurring**:

- Month: Select the month in which daylight savings begins or ends.
- Date: Select the date in which daylight savings begins or ends.
- Year: Select the year for which you want to add a daylight savings time schedule.
- Hours: Select the daylight savings time offset in hours.
- Minutes: Select the daylight savings time offset in hours, for example, 30 minutes.
- Zone: Select the time zone for your location.

8. Click the **APPLY** button.

   Your settings are saved.

   The current system date and time display next to the menu icon.

View daylight saving time status

To view the daylight saving time status:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **SETTINGS**.
5. From the menu on the left, select **TIME**.

   The SNTP options display.
6. Click the **Daylight Saving (DST) Status** tab.

   The following fields display:

   - **Daylight Saving (DST)**: Displays the type of daylight setting enabled.
   - **Begins At**: Displays the scheduled settings for the start of the daylight savings period.
   - **Ends At**: Displays the scheduled settings for the end of the daylight savings period.
   - **Offset (in Minutes)**: Displays the daylight savings time offset in minutes.

- **Zone**: Select the time zone for your location.
- **Daylight Saving (DST) in Effect**: Indicates whether the daylight savings offset is currently being applied to system time.

Power over Ethernet

You can manage Power over Ethernet (PoE) on the switch by turning the uninterrupted PoE feature on or off, and perform power cycling to reset one or more PSE ports. You can also view port status, and manage PoE settings for each Ethernet port.

PoE considerations for switches that support PoE or PoE+

A switch that supports Power over Ethernet (PoE) or PoE+ prioritizes the PoE power that it supplies in ascending port order (that is, from the lowest-numbered port to the highest-numbered port), up to its total power budget.

If the power requirements for the attached powered devices (PDs) exceed the total power budget of the switch, the PD on the highest-numbered port is disabled to make sure that the PDs that are connected to the higher-priority, lower numbered ports are supported first.

Just because a PD is listed as an 802.3af PoE or 802.3at PoE+ powered device does not necessarily mean that it requires the maximum power limit of the specification. Many PDs require less power, allowing all PoE ports to be active simultaneously.

PoE+ overview

The PoE+ ports on model GS116EP (port 1–15) and model GS116EPP (port 1–15) support PoE+ (IEEE 802.3at) and PoE (IEEE 802.3af), and can support non-PoE devices.

The maximum PoE power budget on the switch depends on the model:

- **Model GS116EP**: The maximum PoE power budget across all active PoE+ ports is 180W.

  The maximum PoE power that an individual PoE+ port can supply is 30W.
- **Model GS116EPP**: The maximum PoE power budget across all active PoE+ ports is 231W.

  The maximum PoE power that an individual PoE+ port can supply is 30W.

The PoE+ power supplied by the switch is prioritized in ascending port order (from port 1 to port 15), with a total power budget of 180W (model GS116EP) or 231W (model GS116EPP) across all active PoE+ ports.

The following table shows the standard power ranges, calculated with the maximum cable length of 328 feet (100 meters). If a device receives insufficient PoE power from the switch, consider using a shorter cable.

Table 5. PoE classes and PoE power allocations

Device Class	Compatible PoE Standard	Class Description	Maximum Power Supplied by the Switch	Power Delivered to the Device
0	PoE and PoE+	Default power (full)	15.4W	0.44W–13.0W
1	PoE and PoE+	Very low power	4.0W	0.44W–3.84W
2	PoE and PoE+	Low power	7.0W	3.84W–6.49W
3	PoE and PoE+	Mid power	15.4W	6.49W–13.0W
4	PoE+	High power	30.0W	13.0W–25.5W

Monitor PD health

You can use powered device (PD) health monitoring to test the health of a PD that is connected to a PoE port. You can enable automated ping tests that check for connection faults, and you can restart PoE power to the PD.

NOTE: Wait a few minutes after attaching the PD before you start the PD health monitor.

WARNING: To prevent corrupting firmware on a PD, be sure to disable PD health monitoring on the switch before you update the PD's firmware. During a firmware update, the PD might not reply to a ping test, so disabling PD health monitoring ensures that the switch doesn't restart the PD while a firmware update is in progress.

To display the status of the PD:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.

4. From the menu at the top of the page, select **POE**.
5. From the menu on the left, select **PD HEALTH MONITORING**.

   The PD Health Monitoring page displays.
6. Click the port where the PD that you want to test is connected.

   When the port is selected, the port button displays solid purple.
7. Turn on the **PD Health Monitoring** toggle.

   When PD health monitoring is enabled, the toggle displays green.

   A status message displays to confirm whether the PD Health Monitor is ready.

   The PD IP Address field displays the IP address of the PD.
8. In the **Ping Time Interval** field, enter the time interval in seconds for the ping test.

   The default value is 60 seconds.
9. Turn on or off the **If an error occurs while the PD Health Monitor is running, restart the PoE** toggle.

   When enabled, the toggle displays green and is positioned on the right.
10. Click to enable or disable the **If the Restart Count is over 5 then disable PoE** option. If you want to use a different count value, select **10** or **20** from the menu.

    The option is disabled by default, with the count set to 5.
11. When your settings are complete, click the **APPLY** button.

    The ping test on the PD begins.

Total Count: The number of ping tests conducted.

Failure Count: The number of tests where the ping failed to complete.

Restart Count: The number of times that the PoE port was reset.

Manage uninterrupted PoE

If you enable the uninterrupted PoE feature, the switch continues to provide PoE power to any attached PDs while the switch is rebooting, even if it is rebooting after a regular firmware update. By default, the uninterrupted PoE feature is disabled, so that the switch stops providing PoE power while it is rebooting.

Even with the feature enabled, the switch temporarily stops providing PoE in the following situations:

- The switch reboots because you reset it to factory default settings.
- The switch reboots because you installed updated firmware that changed configuration options, the chip driver, or the default PoE settings.

To managed the uninterrupted PoE feature:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **POE**.

   The PoE page displays.
5. Turn on or off the **Uninterrupted PoE** toggle:
   - **Disabled**: The toggle displays gray and is positioned on the left.
   - **Enabled**: The toggle displays green and is positioned on the right.
6. Click the **APPLY** button.
7. Your settings are saved.

Power cycle the PoE ports

You can use the Power Cycle Ports feature to forcibly reset one or more PoE ports.

To power cycle PoE ports through the device UI:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **POE**.

   The PoE page displays.
5. In the **Power Cycle Ports** section, click the port number icon for every port that you want to reset.

When a port is selected, the port number icon displays solid purple.

6. When all the ports that you want to power cycle are selected, click the **APPLY** button.

   PoE on the selected ports is forcibly reset.

Manage an individual PoE port

You can manage the settings on an individual PoE port.

To select a PoE port and configure the settings:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **POE**.

   The PoE page displays.
5. On the **SETTING** menu, click the port number you want to open.

   You can click anywhere on the row for the port number.

   The port settings display.
6. Click the **EDIT** button.

   The PoE port options display.
7. Choose any of the following options to manage the PoE settings on the port:

   a. **Port Power**.

      - **Enable**: The port's ability to deliver PoE power is enabled. This is the default setting.
      - **Disable**: The port’s ability to deliver PoE power is disabled.

   b. **Power Mode** .

      - **802.3af**: The port is powered in, and limited to, the IEEE 802.3af mode. A PD that requires IEEE 802.3at or IEEE 802.3bt power will not receive power when IEEE 802.3af mode is selected.
      - **Legacy**: The port is powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.

- **Pre-802.3at**: The port is initially powered in the IEEE 802.3af mode and, before 75 msec pass, changes to high power IEEE 802.3at mode. Select this mode for a PD that does not perform Layer 2 classification, or if the switch performs 2-event Layer 1 classification.
- **802.3at**: The port is powered in the IEEE 802.3at mode and is backward compatible with IEEE 802.3af. In this mode, if the switch detects that the attached PD requests more power than IEEE 802.3af, but is not an IEEE 802.3at Class 4 device, the PD does not receive power from the port.

c. **Power Limit (W)**: Manually set a value from 3.0W to 30.0W, with step increments of 0.2W.

   Power limit can be set only when the Power Limit Type option is set to **User**.

   The default is 30.0W.

d. **Port Priority**: Select the priority for the port in relation to other ports if the total power that the switch is capable of delivering exceeds the total power budget.
   - **Low**: Low priority. This is the default setting.
   - **High**: High priority.
   - **Critical**: Critical priority.

e. **Power Limit Type**.
   - **None**: No power limit is applied.
   - **Class**: The power limit automatically adjusts based on the class of PD.
   - **User**: When this setting is selected, you can manually set the Power Limit (W). This is the default setting.

f. **Detection Type**.
   - **Legacy**: The port performs legacy detection.
   - **IEEE802**: The port performs a 4-point resistive detection. This is the default setting.
   - **4pt 802.3af + Legacy**: The port performs a 4-point resistive detection, and if required, continues with legacy detection.

8. When your settings are complete, click the **APPLY** button.

   Your settings are applied to the PoE port.

Display PoE port status

You can display the PoE port status, including the amount of power delivered to the PD, and the fault status.

To display the PoE port status through the device UI:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **POE**.

   The PoE page displays.
5. Click the **STATUS** tab.

   The port numbers display, including the Class and Status of each PoE port.
6. Select the port that you want to view.

   You can click anywhere on the row.

   The port status information displays:

   - **Output Voltage (V)**: The voltage that is delivered to the PD in volts.
   - **Output Current (mA)**: The current that is delivered to the PD in milliamps.
   - **Temperature**: The temperature in degrees Celcius.
   - **Fault Status**: The error description when the PoE port is in a fault state:
     - **No Error**: The port is not in any error state and can provide power.
     - **MPS Absent**: The port detected the absence of the main power supply, preventing the port from providing power.
     - **Short**: The port detected a short circuit condition, preventing the port from providing power.
     - **Overload**: The PD that is connected to the port attempts to draw more power than allowed by the port's settings, preventing the port from providing power at all.
     - **Power Denied**: The port was denied power because of a shortage of power or because of an administrative condition. In this condition, the port cannot provide power.
     - **Startup Failure**: The PD that is connected to the port failed to start up. In this condition, the port does not provide power.
     - **Over Voltage**: The port was denied power because of a over-voltage lockout.

  - **Under Voltage**: The port was denied power because of an under-voltage lockout.
  - **Thermal Shutdown**: The port detected a thermal temperature fault, preventing the port from providing power.
- **Output Power (W)**: The power that is delivered to the PD in watts.

Configure a PoE schedule

You can create a PoE schedule for a single port, or for multiple ports.

- PoE schedules are repeated weekly during the selected time range.
- On dates that are not included in a PoE schedule range, individual port settings apply. For more information see Manage an individual PoE port on page 108.

To set up and enable a PoE schedule for one or multiple ports:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **POE**.

   The PoE page displays.
5. From the menu on the left, select **POE SCHEDULE**.

   The POE SCHEDULE page displays.
6. Click the toggle to select **Apply to a single port** or **Apply to multiple ports**.

   The default is a single port where the toggle displays gray and positioned on the left.
7. Click one or more ports.

   When a port is selected, the port button displays solid purple.
8. Click the **Start Date** field and select the date from the pop-up menu.

   Your start date displays.
9. Click the **End Date** field and select the date from the pop-up menu.

   Your end date displays.

10. For each day of the week that you want to schedule PoE, use the sliders to set the ranges.

    Green indicates that PoE is enabled.

11. When your settings are complete, click the **APPLY** button.

    The schedule is enabled.

Edit or disable a PoE schedule

To edit the or disable a PoE schedule:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **POE**.

   The PoE page displays.
5. From the menu on the left, select **POE SCHEDULE**.

   The POE SCHEDULE page displays.
6. If your configured schedule applied to a single port and you want to apply it to more than one port, click the toggle to select **Apply to multiple ports**.

   The toggle displays green and is positioned on the right.
7. To change which PoE ports are scheduled, click one or more ports.

   When a port is selected, the port button displays solid purple.
8. To change the start date, click the **Start Date** field and select the date from the pop-up menu.

   Your new start date displays.
9. To change the end date, click the **End Date** field and select the date from the pop-up menu.

   Your new end date displays.
10. To change the PoE schedule for a specific day of the week, use the sliders to edit one or both ranges.

    Green indicates the ranges for which PoE is enabled.

11. To disable a PoE schedule range for a specific day of the week, pull the end points of the range together so that they overlap.

    The start and end times for the range slider display identical time values.

    For example, if the RANGE1 sliders are pulled all the way to the left, the range displays 0:00 AM - 0:00 AM, indicating that the range is disabled.

12. When your settings are complete, click the **APPLY** button.

    Your settings are saved.

7

Diagnostics and Troubleshooting

This chapter covers the following topics:

- Test cable connections
- Resolve a subnet conflict to access the switch
- PoE troubleshooting suggestions
- Enable or disable loop prevention
- Enable port mirroring
- View or clear the port statistics

Test cable connections

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

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

To test cable connections:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **DIAGNOSTICS**.
5. From the menu on the left, select **CABLE TEST**.
6. Select one or more ports where you want to test the cable that is attached to the port.
7. Click the **NEXT** button.

   The switch tests cable connections for the selected ports and displays the results. This process might take up to a few minutes.
8. Click the **DONE** button to dismiss the test results.

   You can run another cable test if desired.

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, 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. You might see the following message if you try to access the switch:

`The switch and manager IP address are not in the same subnet.`

To resolve this subnet conflict:

1. Disconnect the Ethernet cable between the switch and your network.
2. Shut down power to the switch.
3. Reconnect the Ethernet cable between the switch and your network.
4. Reapply power to the switch.

   The switch powers on. The network DHCP server discovers the switch and assigns it an IP address that is in the correct subnet for the network.

PoE troubleshooting suggestions

Here are some tips for correcting Power over Ethernet (PoE) problems that might occur on switches that support PoE:

- Make sure that the PoE Max LED is off. If the PoE Max LED is solid amber, disconnect one or more PoE devices to prevent PoE oversubscription.
- Make sure that the Ethernet cables are plugged in correctly. For each powered device (PD) that is connected to the switch, the associated PoE port LED on the switch lights solid green. If the associated PoE port LED lights solid amber, a PoE fault occurred and PoE halted because of one of the conditions listed in the following table.

Table 6. PoE fault conditions and possible solutions

PoE Fault Condition	Possible Solution
A PoE-related short circuit occurred on the port.	The problem is most likely with the attached PD. Check the condition of the PD or restart the PD by disconnecting and reconnecting the PD.
The PoE power demand of the PD exceeded the maximum level that the switch permits. The maximum level is 15.4W for a PoE connection or 30W for a PoE+ connection.	
The PoE current on the port exceeded the classification limit of the PD.	
The PoE voltage of the port is outside the range that the switch permits.	Restart the switch to see if the condition resolves itself.

Enable or disable loop prevention

Loop prevention is enabled by default. When enabled and the switch detects a loop, the LED or both LEDs of a port blink at a constant speed.

To enable or disable loop prevention:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **DIAGNOSTICS**.
5. From the menu on the left, select **LOOP PREVENTION**.

   The LOOP PREVENTION page displays.
6. Turn on or off the toggle to enable or disable loop prevention.

   When enabled, the toggle 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 of one or more ports (the source ports) to a single predefined destination port. Port mirroring is disabled by default.

To enable or disable port mirroring:

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

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

The HOME page displays.

4. From the menu at the top of the page, select **DIAGNOSTICS**.
5. From the menu on the left, select **PORT MIRRORING**.

   The PORT MIRRORING page displays.
6. Turn on the toggle to enable port mirroring.

   The toggle displays green and is positioned on the right.
7. In the source port section, click to select the source port.

   The selected port displays purple.

   You can select one source port only.
8. In the destination port section, select the destination port.

   You can select only one destination port. You cannot select a destination port that is a member of a LAG.
9. Click the **APPLY** button.

   Your settings are saved.

View or clear the port statistics

For each switch port, you can view the bytes received, bytes sent, and cyclic redundancy check (CRC) error 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 connected directly to the switch through an Ethernet cable.
2. Enter the IP address that is assigned to the switch.

   A login window opens.
3. Enter the device management password.

   The password is the one that you specified the first time that you logged in. The password is case-sensitive.

   The HOME page displays.
4. From the menu at the top of the page, select **DIAGNOSTICS**.
5. From the menu on the left, select **PORT STATISTICS**.

   The PORT STATISTICS page displays.

   For each port, the page lists the bytes received, bytes sent, and cyclic redundancy check (CRC) error packets, which are packets with errors or corrupt packets.
6. To clear the port statistics, click the **CLEAR COUNTERS** button.

All statistics counters change to 0.

7. To refresh the port statistics, click the **REFRESH** button.
   All statistics counters are updated.

A

Factory Default Settings and Technical Specifications

This appendix contains the following sections:

- Factory default settings
- Technical specifications

Factory default settings

You can return the switch to its factory settings. For more information, see Return the switch to its factory default settings on page 86.

The switch resets and returns to the factory settings shown in the following table.

Table 7. Factory default settings

Feature	Setting
Device management password	password
IP address	192.168.0.239 (if the switch is not connected to a network with a DHCP server)
Subnet mask	255.255.255.0
DHCP mode	Enabled
IGMP snooping	Disabled
LAGs	None configured
VLANs	Disabled. If enabled, by default, all ports are members of VLAN 1.
802.1p/DSCP-based QoS	Enabled
Port-based QoS	Disabled
Rate limiting	Disabled
Broadcast filtering	Disabled
Loop prevention	Enabled
Port speed	Autonegotiation
Flow control	Disabled
Port mirroring	Disabled
DoS prevention	Enabled

Technical specifications

This section describes the technical specifications for each switch model.

Model GS116EP technical specifications

The following table shows the technical specifications for model GS116EP.

Table 8. Models GS116EP technical specifications

Feature	Description
Network interface	RJ-45 connector for 10BASE-T, 100BASE-TX, or 1000BASE-T
Network cable	Category 5e (Cat 5e) or higher-rated Ethernet cable
Ethernet ports	15
SFP	1
Power input	54V, 3.7A DC input
Power consumption	GS116EP: 10.1W (no PoE), 198.7W (with PoE max)
Dimensions (W x D x H)	6.2 x 4.0 x 1.1 in (158 x 101 x 27 mm)
Weight	GS116EP: 0.86 lb (0.39 kg)
Operating temperature	32° to 104°F (0° to 40°C)
Operating humidity	10–90% maximum relative humidity, noncondensing
Electromagnetic compliance	FCC part 15 Class B, CAN ICES (B)/NMB (B), CE Class B, RCM Class B, VCCI Class B, BSMI, KC Class B
Safety agency approvals	CB, CE LVD, CSA, BSMI, RCM

Model GS116EPP technical specifications

The following table shows the technical specifications for model GS116EPP.

Table 9. Models GS116EPP technical specifications

Feature	Description
Network interface	RJ-45 connector for 10BASE-T, 100BASE-TX, or 1000BASE-T
Network cable	Category 5e (Cat 5e) or higher-rated Ethernet cable
Ethernet ports	15

Table 9. Models GS116EPP technical specifications (Continued)

Feature	Description
SFP port	1
Power input	54V, 4.7A DC input
Power consumption	GS116EPP: 10.2W (no PoE), 250.6W (with PoE max)
Dimensions (W x D x H)	11.3 x 4.0 x 1.1 in (286 x 102 x 27 mm)
Weight	GS116EPP: 2.0 lb (0.88 kg)
Operating temperature	32° to 104°F (0° to 40°C)
Operating humidity	10–90% maximum relative humidity, noncondensing
Electromagnetic compliance	FCC part 15 Class B, CAN ICES (B)/NMB (B), CE Class B, RCM Class B, VCCI Class B, BSMI, KC Class B
Safety agency approvals	CB, CE LVD, CSA, BSMI, RCM

B

Additional Switch Discovery and Access Information

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

The appendix contains the following section:

- Access the switch from any computer

Access the switch from any computer

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

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

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

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

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

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

   The login page of the device UI opens.

3. Enter the device management password.

   The default password to access the switch is **password**. The first time that you log in to the switch, you must change the default 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.

   NOTE: You can copy and paste the IP address into a new shortcut or bookmark it for quick access on your computer or mobile device. However, if you reboot the switch, a dynamic IP address (assigned by a DHCP server) might change and the bookmark might no longer link to the login page for the switch. In this case, you must repeat these steps 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 Assign a fixed IP address to the switch on page 18) to make sure that the new bookmark always links to the login page for the switch, even after you reboot the switch.