NETGEAR®

User Manual

Gigabit Ethernet Smart Managed Plus Switches

Models

GS105Ev2

GS105PE

GS108Ev3

GS108PEv3

GS116Ev2

JGS516PE

JGS524Ev2

JGS524PE

October 2018
202-11700-04

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

Support

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

Compliance and Conformity

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

See the regulatory compliance document before connecting the power supply.

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

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11700-04	October 2018	Added a note to Manage Access Control on page 58 to state that models GS108Ev3 and GS108PEv3 do not support access control.
202-11700-03	October 2018	• Changed the manual name from *ProSAFE Gigabit Web Managed (Plus) Switches User Manual* to *Gigabit Ethernet Smart Managed Plus Switches User Manual*. • Added Safety Instructions and Warnings on page 7. • Revised Configure the Switch on page 9. • Revised Access a Switch That Is Connected to a Network on page 10. • Revised Install the ProSAFE Plus Utility on page 13. • Added Use the NETGEAR Switch Discovery Tool to Access the Switch on page 15. • Added Use the NETGEAR Insight Mobile App to Discover the Switch on page 16. • Added Change the Language on page 17, including Change the Language of the Local Browser Interface on page 18 and Change the Language for the Local Browser Interface by Installing Another Firmware Version on page 18. • Added Manage Access Control on page 58 including Add Devices to the Access Control Table on page 58 and Remove Devices From the Access Control Table on page 59. • Added PoE Considerations for Switches That Support PoE on page 63. • Added PoE Troubleshooting Suggestions on page 67. • Removed references to the resource CD. • Made multiple minor changes.
202-11700-02	March 2017	Made corrections to Specify a Port PVID for an 802.1Q-Based VLAN on page 30.
202-11700-01	August 2016	First publication.

Contents

Chapter 4 Manage Network Settings

Chapter 5 Manage and Monitor the Switch

Chapter 6 Diagnostics and Troubleshooting

Appendix A Factory Default Settings

1

Get Started

This chapter covers the following topics:

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/.

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

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

Supported Switches

The *Gigabit Ethernet Smart Managed Plus Switches User Manual* describes the following switch models:

- GS105Ev2
- GS105PE
- GS108Ev3
- GS108PEv3
- GS116Ev2
- JGS516PE
- JGS524Ev2
- JGS524PE

Note: Smart Managed Plus Switches used to be called Web Managed (Plus) Switches.

Safety Instructions and Warnings

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

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

- This product is designed for indoor use only in a temperature-controlled and humidity-controlled environment. For more information, see the environmental specifications in the appendix or the data sheet.
  Any device that is located outdoors and connected to this product must be properly grounded and surge protected.
  Failure to follow these guidelines can result in damage to your NETGEAR product, which might not be covered by NETGEAR's warranty, to the extent permissible by applicable law.
- Observe and follow service markings:
  - Do not service any product except as explained in your system documentation. Some devices should never be opened.
  - If applicable to your device, opening or removing covers that are marked with the triangular symbol with a lightning bolt can expose you to electrical shock.

We recommend that only a trained technician services components inside these compartments.

- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
  - Depending on your device, the power adapter, power adapter cable, power cable, extension cable, or plug is damaged.
  - An object fell into the product.
  - The product was exposed to water.
  - The product was dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.

- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide, or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- If applicable to your device, allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To avoid damaging your system, if your device uses a power supply with a voltage selector, be sure that the selector is set to match the power at your location:
  - 115V, 60 Hz in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  - 100V, 50 Hz in eastern Japan and 100V, 60 Hz in western Japan
  - 230V, 50 Hz in most of Europe, the Middle East, and the Far East

- Be sure that attached devices are electrically rated to operate with the power available in your location.
- Depending on your device, use only a supplied power adapter or approved power cable:

If your device uses a power adapter:

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

If your device uses a power cable:

- If you were not provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable approved for your country.
- The power cable must be rated for the product and for the voltage and current marked on the product electrical ratings label. The voltage and current rating of the cable must be greater than the ratings marked on the product.

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

Configure the Switch

Gigabit Ethernet Smart Managed Plus Switches are plug-and-play, so they can be used without any configuration. Just connect power, connect to your network and to your other devices, and you’re done.

For easiest access, we recommend that you cable the switch to a network with a router or DHCP server that assigns IP addresses and power on the switch. However, it is also possible to configure the switch connected directly only to the computer that you are using to configure it, and not connected to the network (off-network).

You can configure and manage advanced features of the switch either by using your computer's web browser and accessing the switch at its IP address or by installing the ProSAFE® Plus Utility on your Windows-based computer.

If you use a Mac or a 64-bit Windows-based computer, you can use the NETGEAR Switch Discovery Tool to discover the switch in your network and access the local browser–based management interface of the switch.

You can also use the NETGEAR Insight mobile app on your smartphone to discover the switch in your network.

For more information, see the following sections:

- Access the Switch Using a Web Browser on page 10
- Access the Switch With the ProSAFE Plus Utility on page 12
- Use the NETGEAR Switch Discovery Tool to Access the Switch on page 15
- Use the NETGEAR Insight Mobile App to Discover the Switch on page 16

Access the Switch Using a Web Browser

This manual describes the local browser–based management interface, referred to as the local browser interface.

You can access and configure the switch directly through its local browser interface by entering the IP address of the switch in the address bar of a browser. When you use the local browser interface, the simplest way to configure the switch is not connected to your network (off-network). You can also configure the switch with it connected to your network, router, or modem, (on-network) but you must be able to determine the IP address of the switch if your network uses DHCP.

Access a Switch That Is Connected to a Network

By default, the DHCP client of the switch is enabled. To access the switch, use the IP address that the DHCP server assigned to the switch.

To determine the IP address of the switch, do one of the following:

- If you use a Windows-based computer, use the ProSAFE® Plus Utility to detect the IP address (see Access the Switch With the ProSAFE Plus Utility on page 12). You can also access and configure the switch from the utility.

- If you use a Mac or a 64-bit Windows-based computer, use the NETGEAR Switch Discovery Tool to detect the IP address (see Use the NETGEAR Switch Discovery Tool to Access the Switch on page 15).
- If you use an iOS or Android smartphone, use the NETGEAR Insight mobile app to detect the IP address (see Use the NETGEAR Insight Mobile App to Discover the Switch on page 16).
- Access the DHCP server.
- Use an IP scanner utility.

To use your web browser to configure a switch that is connected to a network:

1. Cable the switch to a network with a router or DHCP server that manages IP addresses.
2. Power on the switch.
   The DHCP server assigns the switch an IP address.
3. Connect your computer to the same network as the switch.
4. Determine the IP address of the switch.
   By default, the DHCP client of the switch is enabled. Use the IP address that the DHCP server assigned to the switch.
5. Open a web browser, and enter the IP address of the switch.
   The login window opens.
6. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
7. Click the **Login** button.
   You can now configure additional options for the switch through the local browser interface.

   For information about setting up a fixed (static) IP address for the switch, see Specify IP Address Settings for the Switch on page 40.

Access a Switch That Is Off-Network

To use your web browser to configure a switch that is not connected to a network:

1. Record your computer's TCP/IP configuration settings, and then configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 as the subnet mask.

   Note: If you are unsure how to do this, visit the support website at netgear.com/support and search for Static IP address on computer.

2. Plug the switch into a power outlet and then connect your computer to the switch using an Ethernet cable.

   You can connect the Ethernet cable to any port on the switch.

3. Open a web browser, and enter **http://192.168.0.239**.

   This is the default address of the switch.

   The login window opens.

4. Enter the switch password.

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

5. Click the **Login** button.

   You can now configure additional options for the switch through the local browser interface.

   For information about setting up a fixed (static) IP address for the switch, see Specify IP Address Settings for the Switch on page 40.

6. After you complete the configuration of the switch, reconfigure the computer that you used for this process to its original TCP/IP settings.

   You can now connect your switch to your network using an Ethernet cable.

Access the Switch With the ProSAFE Plus Utility

The ProSAFE Plus Utility runs on Windows-based computers. You can install the latest utility to select additional options to manage and customize the switch for your network. Visit netgear.com/support/product/PCU to download the latest utility.

Install the ProSAFE Plus Utility

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

To install the ProSAFE Plus Utility:

1. Visit netgear.com/support/product/PCU.
2. Select and download the latest version of the utility to your computer.
3. Unzip the downloaded file to extract the utility installation file.
4. Install the utility on your computer.
5. If prompted, allow WinPcap and Adobe Air to be installed.

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

Access and Configure the Switch Using the ProSAFE Plus Utility

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

Note: You can also access and configure the switch directly using a web browser. See Access the Switch Using a Web Browser on page 10.

To access and configure the switch using the ProSAFE Plus Utility:

1. Cable the switch to a network with a router or DHCP server that manages IP addresses.
2. Power on the switch.

   The DHCP server assigns the switch an IP address.
3. 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.

Note: You can use the ProSAFE Plus Utility to upgrade the firmware on the switch. In that situation, do not use a WiFi connection to the switch but use only a direct wired connection over an Ethernet cable. That is, configure a computer with an IP address in the same subnet as the switch and connect directly to the switch using an Ethernet cable before you start the firmware upgrade using the ProSAFE Plus Utility.

4. Double-click the **ProSAFE Plus Utility** icon.
   The configuration home page displays a list of Smart Managed Plus switches that the utility discovers on the local network.

   Note: To use the ProSAFE Plus Utility, you must configure your computer's security software to allow broadcast UDP packets to go through UDP remote and source (local and destination) ports 63321 through 63324. To allow this traffic, you can create a rule in your computer's security software, or temporarily disable the firewall, Internet security, antivirus programs, or all of these on the computer that you use to configure the switch. If you temporarily disable any security services, be sure to reenable those services once configuration is complete.

5. Select the Smart Managed Plus switch that you want to configure.
   If you do not see the switch, click the **REFRESH** button.
6. Click the **APPLY** button.
   The login window displays.
7. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
8. Use the utility to configure the switch settings.
9. When you are finished with the configuration, return the computer's firewall, Internet security, and antivirus programs to their usual settings.

For a description of ProSAFE Plus Utility features, see the *ProSAFE Plus Utility User Manual*.

You can access the user manual through a link on the **Help** tab of the utility or you can download it by visiting netgear.com/support/download/.

Use the NETGEAR Switch Discovery Tool to Access the Switch

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

Depending on your model switch, the NETGEAR Switch Discovery Tool lets you discover the switch in your network and access the local browser interface of the switch from a Mac or a 64-bit Windows-based computer.

To install the NETGEAR Switch Discovery Tool, discover the switch in your network, and access the local browser interface of the switch:

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

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

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

   The installation process places a **NETGEAR Switch Discovery Tool** icon on your desktop.

4. Reenable the security services on your computer.
5. Power on the switch.

   The DHCP server assigns the switch an IP address.

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

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

7. Open the Switch Discovery Tool.

   To open the program, double-click the **NETGEAR Switch Discovery Tool** icon on your desktop.

   The initial page displays a menu and a button.

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

9. Click the **Start Searching** button.

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

   For each switch, the tool displays the IP address.

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

    The login page of the local browser interface opens.

11. Enter the switch password.

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

    The Switch Information page displays.

Use the NETGEAR Insight Mobile App to Discover the Switch

If the switch is connected to a WiFi router or access point, the NETGEAR Insight mobile app lets you discover the switch in your network.

To use the NETGEAR Insight mobile app to discover the switch in your network:

1. On your iOS or Android mobile device, go to the app store, search for NETGEAR Insight, and download and install the app.
2. Connect your mobile device to the WiFi network of the WiFi router or access point to which the switch is connected.
3. Open the NETGEAR Insight mobile app.
4. Select **LOG IN** to log in to your existing NETGEAR account or tap the **CREATE NETGEAR ACCOUNT** button to create a new account.

   After you log in to your account, the IP address of the switch displays in the device list.

5. Write down the IP address for future use.

Change the Password

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

To change the password:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **Maintenance > Change Password**.
   The Change Password page displays.
6. In the **Old Password** field, type the current password for the switch.
7. Type the new password in the **New Password** field and in the **Re-type 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.

Change the Language

For most switches, you can select the language for the local browser interface by selecting another language from the language menu at the upper right of the page in the local browser interface.

However, for models GS108Ev3 and GS108PEv3, you must download and install a firmware version in the desired language.

Change the Language of the Local Browser Interface

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

To change the language of the local browser interface:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
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.

Change the Language for the Local Browser Interface by Installing Another Firmware Version

For models GS108Ev3 and GS108PEv3, you must download and install a firmware version in the desired language.

To change the language for the local browser interface of model GS108Ev3 or GS108PEv3:

1. Visit netgear.com/support/download/.
2. In the **Enter a Product Name/Model Number** field, start typing the model number, and select the model from the menu that displays after you start typing.
   The available firmware versions displays. The language is included in the firmware name.

3. Select and download the desired firmware version to your computer.
4. Unzip the downloaded file to extract the firmware image.
5. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
6. Launch a web browser.
7. In the address field of your web browser, enter the IP address of the switch.
   The login window opens.
8. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
9. Select **System > Maintenance > Firmware Upgrade**.
   The Firmware Upgrade page displays.
   The firmware upgrade method depends on the current firmware and boot loader versions on your switch.
10. If the page displays the **Enter Loader Mode** button, click the **Enter Loader Mode** button.
    The switch reboots and enters into the loader mode. The Firmware Upgrade page that displays varies, depending on the firmware boot loader version that is already on your switch.
11. Click the **Browse** button and locate and select the firmware image that you downloaded and unzipped.
12. Click the **Apply** button.

    Warning: To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not turn off the switch or disconnect it.

    When the upgrade is complete, your switch restarts, and the local browser interface uses the language of the firmware that you installed. The upgrade process typically takes about three minutes.

Register Your Product

We recommend that you use the NETGEAR Insight mobile app to register your product (see Use the NETGEAR Insight Mobile App to Discover the Switch on page 16).

Registering your product allows you to receive email alerts and streamlines the technical support process. However, you can also register your product through the local browser interface.

To register your product through the local browser interface:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection.

   Note: You must access the switch while connected to the network (on-network) to register the switch.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **Help > Registration**.
   The Product Registration page displays.
6. Click the **Register** button.
7. Follow the onscreen process to register your product.

2

Use VLANS for Traffic Segmentation

This chapter covers the following topics:

VLAN Overview

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

Ports can be grouped in VLANs using port-based or 802.1Q criteria:

- **Port-based VLANs**. Assign ports to virtual networks. Ports with the same VLAN ID are placed in the same VLAN. This feature provides an easy way to partition a network into private subnetworks.
- **802.1Q VLANs**. Create virtual networks using the IEEE 802.1Q standard. 802.1Q uses a VLAN tagging system to determine which VLAN an Ethernet frame belongs to. You can configure ports to be a part of a VLAN. When a port receives data tagged for a VLAN, the data is discarded unless the port is a member of that VLAN. This technique is useful for communicating with devices outside your local network as well as receiving data from other ports that are not in the VLAN. However, for you to be able to use an 802.1Q VLAN, you must know the VLAN ID.

Create Basic Port-Based VLANs

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

You can also assign ports to multiple VLANs (see Assign Ports to Multiple Port-Based VLANs on page 24).

By default, all ports are members of VLAN 1.

To create basic port-based VLANs:

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

   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

   The login window opens.

4. Enter the switch password.

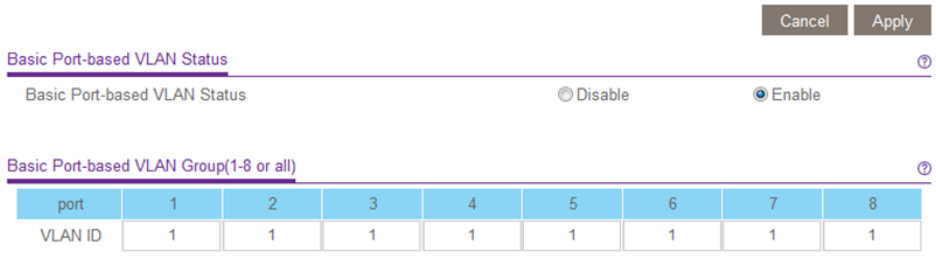
The default password is **password**. The password is case-sensitive.

The Switch Information page displays.

5. Select **VLAN**.
   The Basic Port-based VLAN Status page displays.
6. If this is the first time that you are accessing this page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with Step 7.
   Otherwise, see Step 9.

   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **OK** button.
   The pop-up window closes.
8. Click the **Apply** button.
   Your settings are saved.

   The Basic Port-based VLAN Group table displays.



   The previous figure is an example. Your switch might provide more or fewer ports.
9. Under each port to be added to a VLAN, enter the ID of the VLAN.
   You can enter a VLAN ID from 1 to the maximum number of ports that your switch supports. If all the VLANs share an uplink to the Internet or servers, enter **all** in the **VLAN ID** field for the port that you want to use for the uplink.

   Note: If ports are members of the same LAG, you must assign them to the same VLAN.
10. Click the **Apply** button.
    Your settings are saved.

Assign Ports to Multiple Port-Based VLANs

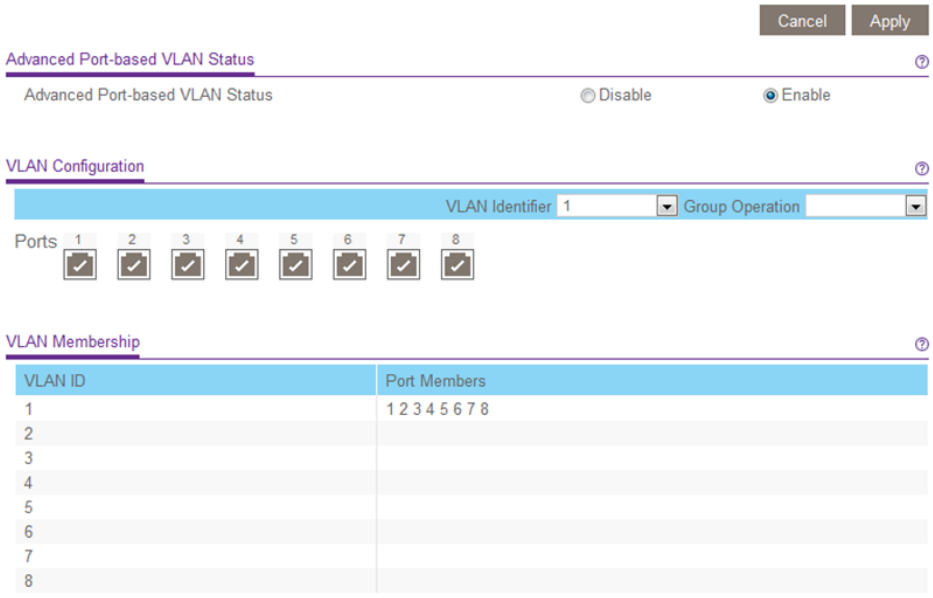
A port-based VLAN configuration lets you assign ports on the switch to a VLAN. The number of VLANs is limited to the number of ports on the switch. In an advanced port-based VLAN configuration, you can assign a single port to multiple VLANs.

By default, all ports are members of VLAN 1.

To assign ports to multiple port-based VLANs:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **VLAN**.
   The Basic Port-based VLAN Status page displays.
6. If this is the first time that you are accessing this page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with Step 7.
   Otherwise, see Step 9.
   A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **OK** button.
   The pop-up window closes.
8. Click the **Apply** button.
   Your settings are saved.

The VLAN Configuration and VLAN Membership sections display.



The previous figure is an example. Your switch might provide more or fewer ports.

9. In the **VLAN Identifier** menu, select the VLAN.
10. Select the ports that you want to add to the VLAN by doing the following:
    a. (Optional) In the **Group Operation** menu, select either **Select All** or **Remove All**.
    All ports are either added to the VLAN or removed from the VLAN.
    b. Select or remove individual ports by selecting the check boxes that are associated with the port numbers.

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

    c. Click the **Apply** button.
    Your settings are saved. In the VLAN Membership table, the ports display as members of the VLAN.
11. To select ports for another VLAN, repeat Step 9 and Step 10.

Create 802.1Q-Based VLANs in a Basic Configuration

A 802.1Q-based VLAN configuration lets you assign ports on the switch to a VLAN with an ID number in the range of 1–4093. By default, all ports are members of VLAN 1.

In an advanced 802.1Q-based VLAN configuration, you can set up VLANs to which you can add tagged or untagged ports and you can use port VLAN ID (PVID). For more information, Create 802.1Q-Based VLANs in an Advanced Configuration on page 27.

To create 802.1Q-based VLANs in a basic configuration:

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

   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

   The login window opens.

4. Enter the switch password.

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

   The Switch Information page displays.

5. Select **VLAN > 802.1Q**.

   The Basic 802.1Q VLAN Status page displays.

6. If this is the first time that you are accessing the Basic 802.1Q VLAN Status page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with Step 7.

   Otherwise, see Step 9.

   A pop-up window opens, informing you that the current VLAN settings will be lost.

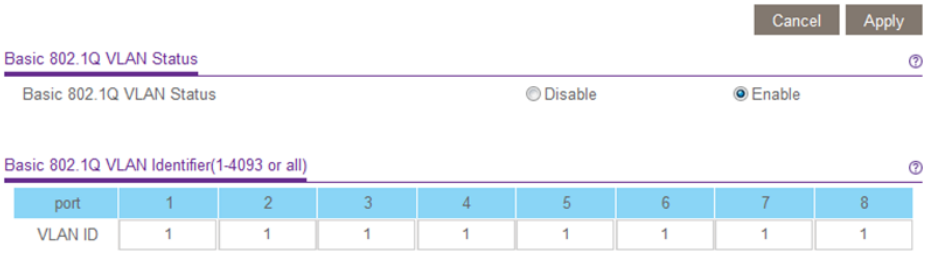
7. Click the **OK** button.

   The pop-up window closes.

8. Click the **Apply** button.

   Your settings are saved.

The Basic 802.1Q VLAN Identifier table displays.



The previous figure is an example. Your switch might provide more or fewer ports.

9. Under each port to be added to a VLAN, enter the ID of the VLAN.
   You can enter a VLAN ID from 1 to 4093. If all the VLANs share an uplink to the Internet or servers, enter **all** in the **VLAN ID** field for the port that you want to use for the uplink.

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

10. Click the **Apply** button.
    Your settings are saved.

Create 802.1Q-Based VLANs in an Advanced Configuration

In an advanced 802.1Q-based VLAN configuration, you can assign ports on the switch to a VLAN with an ID number in the range of 1–4093 and you can add tagged or untagged ports to a VLAN. In addition, you can use port VLAN IDs (PVIDs). By default, all ports are untagged members of VLAN 1.

To create 802.1Q-based VLANs in an advanced configuration:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

The login window opens.

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

   The Switch Information page displays.

5. Select **VLAN > 802.1Q > Advanced > VLAN Configuration**.
   The Advanced 802.1Q VLAN Status page displays.

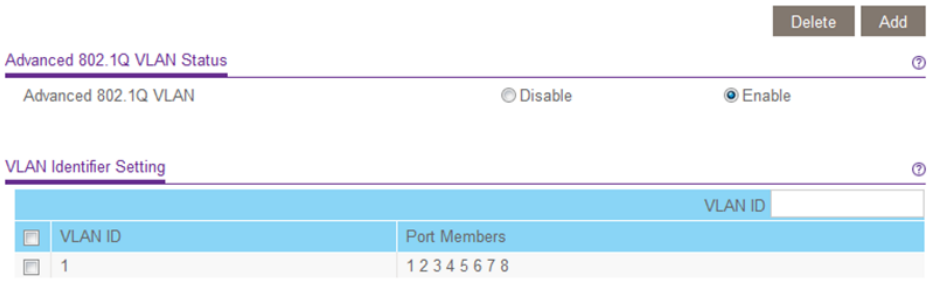
6. If this is the first time that you are accessing the Advanced 802.1Q VLAN Status page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with Step 7.
   Otherwise, see Step 9.

   A pop-up window opens, informing you that the current VLAN settings will be lost.

7. Click the **OK** button.
   The pop-up window closes.

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

   The VLAN Identifier Setting table displays.



   The previous figure is an example. Your switch might provide more or fewer ports, all of which are members of VLAN 1 by default.

9. In the **VLAN ID** field, enter a VLAN ID.
   You can enter a VLAN ID from 1 to 4093.

10. Click the **Add** button.
    The new VLAN is added to the VLAN Identifier Setting table.

    After you create a new VLAN ID, use the VLAN membership option to add ports to the VLAN. (Select **VLAN > 802.1Q > Advanced > VLAN Membership**. See also Add Tagged or Untagged Ports to an 802.1Q-Based VLAN on page 29.)

Note: To delete a VLAN, select the check box for the VLAN and click the **Delete** button.

Add Tagged or Untagged Ports to an 802.1Q-Based VLAN

After you define a VLAN ID using the advanced 802.1Q VLAN option (see Create 802.1Q-Based VLANs in an Advanced Configuration on page 27), you must add ports to the VLAN.

While you add ports to a VLAN, you can specify whether the ports must be tagged or untagged. 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.

By default, all ports are untagged.

To add tagged or untagged ports to an 802.1Q-based VLAN:

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

   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

   The login window opens.

4. Enter the switch password.

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

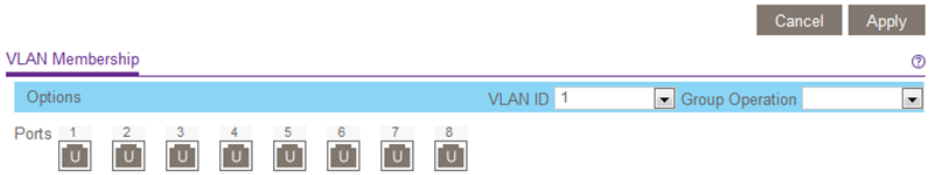
   The Switch Information page displays.

5. Select **VLAN > 802.1Q > Advanced > VLAN Configuration**.

   The Advanced 802.1Q VLAN Status page displays. The menu on the left displays more options.

6. Select **VLAN Membership**.

You can select **VLAN Membership** only if you already enabled the advanced 802.1Q VLAN option (see Create 802.1Q-Based VLANs in an Advanced Configuration on page 27).



The previous figure is an example. Your switch might provide more or fewer ports.

7. In the **VLAN ID** menu, select the VLAN.
8. Select the ports that you want to add to the VLAN by doing the following:
   a. (Optional) In the **Group Operation** menu, select **Untag All**, **Tag all**, or **Remove all**.
      All ports are either added to the VLAN (tagged or untagged) or removed from the VLAN.
   b. Select individual ports and assign them as tagged (T) or untagged (U) ports or remove individual ports by selecting the check boxes that are associated with the port numbers.
      By default, all ports are untagged.
   c. Click the **Apply** button.
      Your settings are saved. In the VLAN Membership table, the ports display as members of the VLAN.
9. To select ports for another VLAN, repeat Step 7 and Step 8.
10. To verify your selections, select **VLAN > 802.1Q > Advanced > VLAN Configuration**.
    The Advanced 802.1Q VLAN Status page displays. In the VLAN Identifier Setting table, the ports display next to the VLAN or VLANs to which they were added.

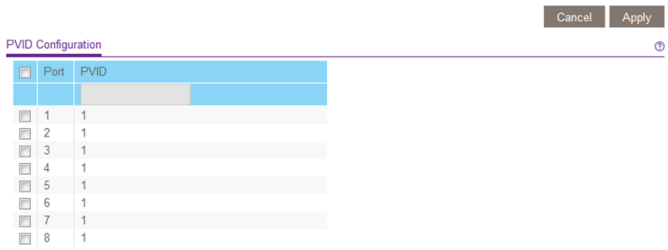
Specify a Port PVID for an 802.1Q-Based VLAN

A default port VLAN ID (PVID) is a VLAN ID tag that the switch assigns to data packets it receives that are not already addressed (tagged) for a particular VLAN. For example, if you connected a computer on port 6 and you want it to be a part of VLAN 2, configure port 6 to automatically add a PVID of 2 to all data received from the computer. This step

ensures 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.

To assign a PVID to one or more ports:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **VLAN > 802.1Q > Advanced > VLAN Configuration**.
   The Advanced 802.1Q VLAN Status page displays. The menu on the left displays more options.
6. Select **Port PVID**.
   You can select **Port PVID** only if you already enabled the advanced 802.1Q VLAN option (see Create 802.1Q-Based VLANs in an Advanced Configuration on page 27).



   The previous figure is an example. Your switch might provide more or fewer ports.
7. Select one or more ports.
8. Enter the PVID.
   You can enter a PVID only for a VLAN that already exists.
9. Click the **Apply** button.
   Your settings are saved.

3

Optimize Performance With Quality of Service

This chapter covers the following topics:

- Enable 802.1p/DSCP-Based Quality of Service
- Configure Port-Based Quality of Service
- Set Up Rate Limiting
- Set Up Broadcast Filtering

Enable 802.1p/DSCP-Based Quality of Service

Note: 802.1p-based QoS is available on all models. DSCP-based QoS is available on models GS105Ev2, GS105PEv2, GS108Ev3, and GS108PEv3 only.

802.1p/DSCP-based priority uses a field in the data packet header that identifies the class of data in the packet (for example, voice or video). When 802.1p/DSCP-based priority is used, the switch reads information in the packet header to determine the priority to assign to the packet. The switch reads both 802.1p tag information and DSCP/ToS tag information. If an ingress packet contains both an 802.1p tag and a DSCP/ToS tag, the switch gives precedence to the 802.1p tag.

All ports on the switch check the packet header and transmit the packet with a priority determined by the packet content.

To enable 802.1p/DSCP-based QoS:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **QoS**.
   The Quality of Service page displays.
6. Select the **802.1p/DSCP-based** radio button.
   A pop-up window opens, informing you that the current QoS settings will be lost.
7. Click the **OK** button.
   The pop-up window closes.
8. Click the **Apply** button.

Your settings are saved.

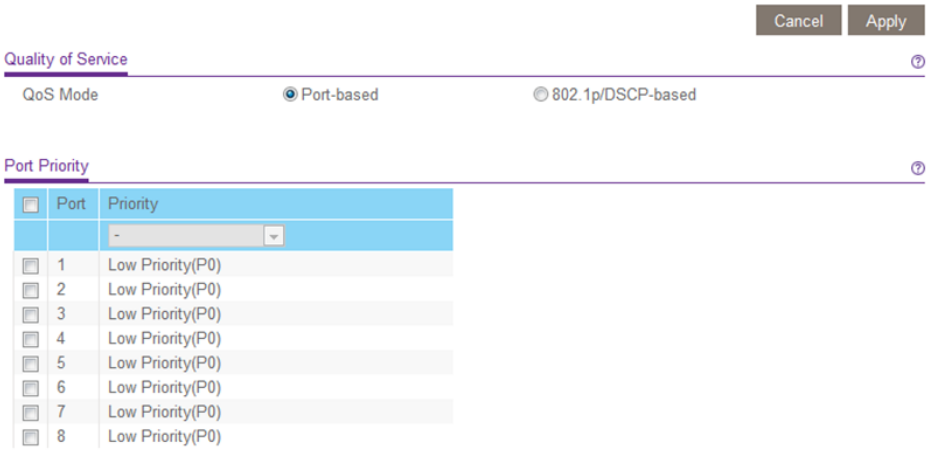
Configure Port-Based Quality of Service

You can assign a priority to all data passing through a particular port. Data with a higher priority is transmitted faster. If packets arrive at several ports at the same time, the ports configured as higher priority transmit their packets first. You must determine which ports will carry delay-sensitive data.

To configure port-based QoS:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **QoS**.
   The Quality of Service page displays.
6. If this is the first time that you are setting up port-based QoS, select the **Port-based** radio button and continue with the next step.
   Otherwise, see Step 9.
   A pop-up window opens, informing you that the current QoS settings will be lost.
7. Click the **OK** button.
   The pop-up window closes.
8. Click the **Apply** button.

Your settings are saved and the Port Priority table displays.



The previous figure is an example. Your switch might provide more or fewer ports. The **802.1p/DSCP-based** radio button is not supported on all models and therefore might not show on the page.

9. To set the port priority for one or more ports, do the following:
   a. Select one or more ports.
   b. In the **Priority** menu, select the priority.
   c. Click the **Apply** button.
      Your settings are saved. The same priority is applied to all ports that you selected.
10. To set a different port priority for one or more other ports, repeat Step 9.

Set Up Rate Limiting

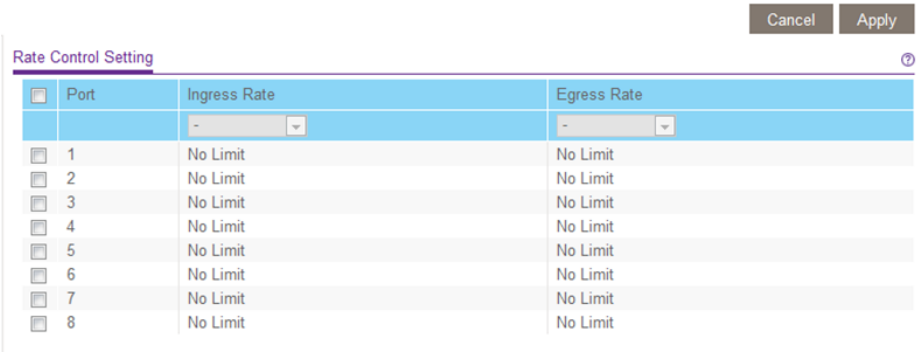
You can limit the rate at which the switch accepts incoming data and the rate that it retransmits outgoing data. The rate choices vary depending on the switch model.

Rate limiting can be set for a port in addition to other QoS settings. If the port rate limit is set, the switch restricts the acceptance or retransmission of data to the values configured.

To set up rate limiting:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **QoS > Rate Limit**.



   The previous figure is an example. Your switch might provide more or fewer ports.
6. Set the ingress (incoming) and egress (outgoing) traffic rates by doing the following:
   a. Select one or more ports.
   b. In the **Ingress Rate** menu, select the maximum rate.
      You can set a rate from 512 Kbit/s to 512 Mbit/s. By default, no limit is set.
   c. In the **Egress Rate** menu, select the maximum rate.
      You can set a rate from 512 Kbit/s to 512 Mbit/s. By default, no limit is set.
   d. Click the **Apply** button.
      Your settings are saved.
7. To set different rates for one or more other ports, repeat Step 6.

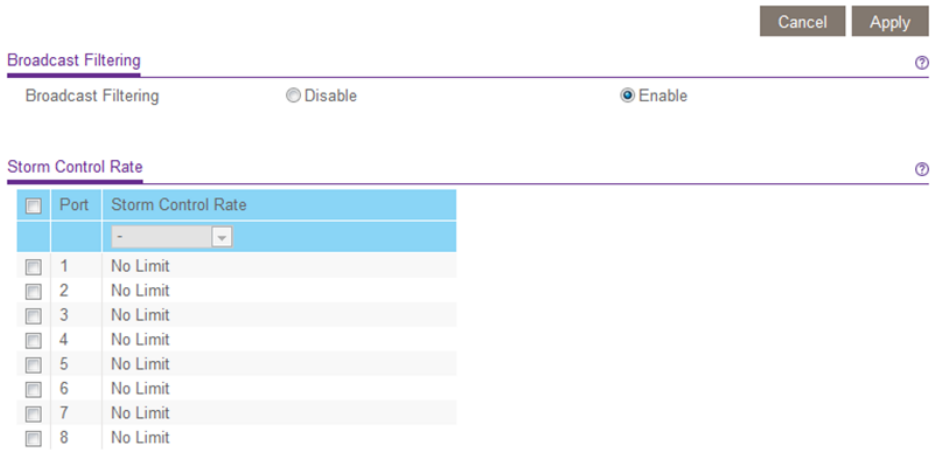
Set Up Broadcast Filtering

You can configure the switch to block broadcast storms (massive transmission of broadcast packets forwarded to every port on the same VLAN). If they are not blocked, broadcast storm packets can delay or halt the transmission of other data. Some switches allow you to select a storm control rate for each port. Others assign a predetermined storm control rate for all ports on the switch.

If broadcast traffic on any port exceeds the threshold that you set, the switch temporarily blocks (discards) the broadcast traffic.

To set up broadcast filtering:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **QoS > Broadcast Filtering**.
   The Broadcast Filtering page displays.
6. If this is the first time that you are setting up broadcast filtering, select the **Enable** radio button and continue with the next step.
   Otherwise, see Step 8.
7. Click the **Apply** button.
   Your settings are saved and the Storm Control Rate table displays.



The previous figure is an example. Your switch might provide more or fewer ports.

8. Set the storm control rate by doing the following:
   a. Select one or more ports.
   b. In the **Storm Control Rate** menu, select the maximum rate.
      You can set a rate from 512 Kbit/s to 512 Mbit/s. By default, no limit is set.
   c. Click the **Apply** button.
      Your settings are saved.

9. To set a different rate for one or more other ports, repeat Step 8.

4

Manage Network Settings

This chapter covers the following topics:

Specify IP Address Settings for the Switch

By default, the switch IP address works as follows:

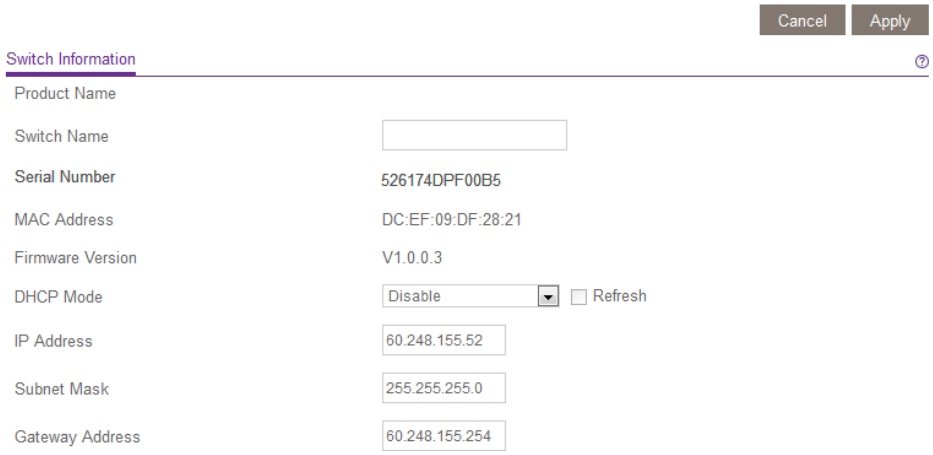
- If you cable the switch to a network with a DHCP server before you power on the switch, the DHCP server assigns an IP address to the switch when the switch is powered on.
- If you power on the switch when it is not connected to a network with a DHCP server, the switch uses its default IP address, which is 192.168.0.239.
  You can disable the DHCP mode in the switch and enter static IP address and subnet mask values for the switch as well as the address of the gateway device used by the switch.

Use Browser-Based Access to Specify the Switch IP Address

To specify IP address settings for the switch:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.

5. In the **DHCP Mode** menu, select **Disable**.



   The **IP Address**, **Subnet Mask**, and **Gateway Address** fields are enabled.

6. Enter the IP address, subnet mask, and gateway address.
7. Click the **Apply** button.
   Your settings are saved.

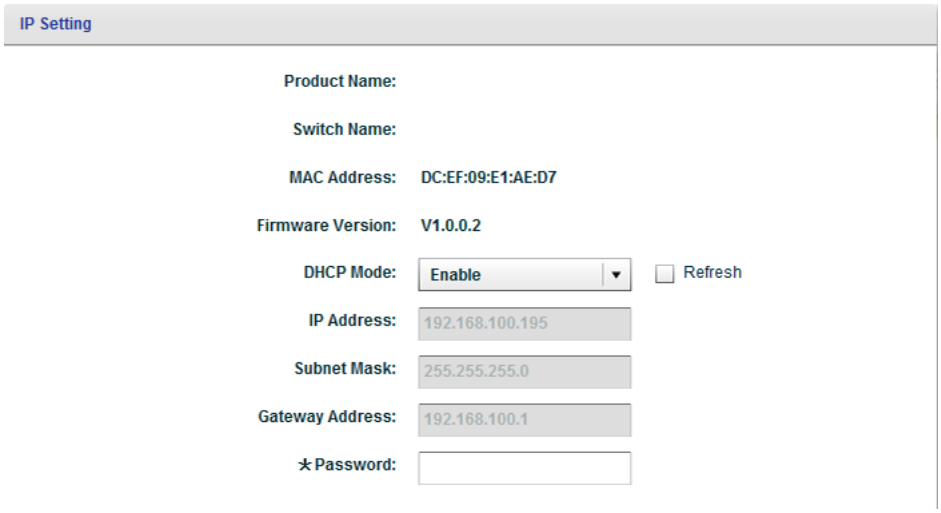
Use the ProSAFE Plus Utility to Specify the Switch IP Address

The ProSAFE Plus Utility runs on Windows-based computers. You can install the utility to select additional options to manage and customize the switch for your network. Visit netgear.com/support/product/PCU to download the utility.

To specify IP address settings for the switch:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Double-click the **ProSAFE Plus Utility** icon.
   The Switch Selection page displays a list of Smart Managed Plus Switches that the utility discovers on the local network.
3. Select the switch.
   If you do not see the switch, click the **REFRESH** button.

4. Click the **IP SETTING** button.



Note: To navigate to this page, select **Network**, select the switch, and click the **IP SETTING** button.

5. In the **DHCP Mode** menu, select **Disable**.
   The **IP Address**, **Subnet Mask**, and **Gateway Address** fields are enabled.
6. Enter the IP address, subnet mask, and if available, the gateway address.
7. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
8. Click the **APPLY** button.
   Your settings are saved.

Manage Multicast Traffic With IGMP Snooping

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

The switch maintains a map that shows which links need which IP multicast streams. The switch forwards multicast traffic only to the links that requested them and cuts multicast traffic from links that do not contain a multicast listener. Essentially, IGMP snooping helps optimize multicast performance at Layer 2 and is especially useful for bandwidth-intensive IP multicast applications such as IPTV.

Customize IGMP Snooping

By default, IGMP snooping is enabled. You can customize the settings for your network.

To customize IGMP snooping:

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

   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

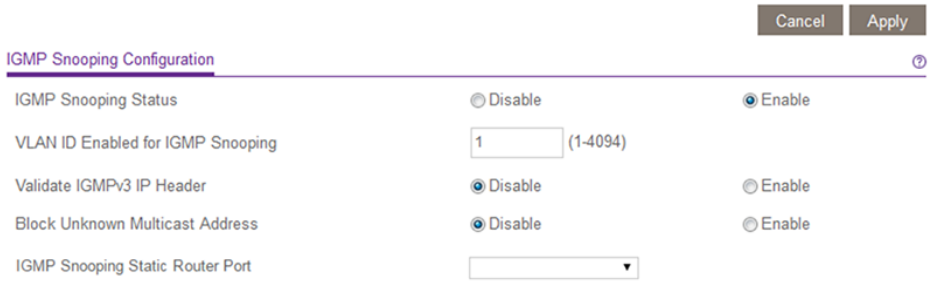
   The login window opens.

4. Enter the switch password.

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

   The Switch Information page displays.

5. Select **System > Multicast**.



6. Make sure that the IGMP Snooping Status **Enable** radio button is selected.

   By default, the **Enable** radio button is selected.

7. In the **VLAN ID Enabled for IGMP Snooping** field, enter a VLAN ID between 1 and 4094.

   By default, the VLAN ID is 1.

You can specify a VLAN for IGMP snooping only if you enabled port-based or 802.1Q-based VLANs (see Use VLANS for Traffic Segmentation on page 21).

IGMP snooping functions only on the VLAN that is specified in the **VLAN ID Enabled for IGMP Snooping** field.

8. (Optional) Select the Validate IGMPv3 IP header **Enable** radio button.

   Some network devices might not conform to the IGMPv3 standard. When the Validate IGMPv3 IP header option is enabled, IGMP messages are required to include TTL = 1, ToS Byte = 0xC0 (Internetwork Control), and the router alert IP option (9404) must be set. Otherwise, the packets are ignored.

9. (Optional) Select the Block Unknown MultiCast Address **Enable** radio button.

   When this feature is enabled, multicast packets are forwarded only to the ports that are in the multicast group learned from IGMP snooping. All unknown multicast packets are dropped.

10. (Optional, for some models only) Select an option from the **IGMP Snooping Static Router Port** menu.

    You can select a port to be the dedicated IGMP snooping static router port if no IGMP query exists in the network for the switch to discover the router port dynamically. After a port is selected as the static router port, all IGMP Join and Leave reports are forwarded to the port.

11. Click the **Apply** button.

    Your settings are saved.

Specify a VLAN for IGMP Snooping

You can specify a VLAN for IGMP snooping only if you enabled port-based or 802.1Q-based VLANs (see Use VLANS for Traffic Segmentation on page 21).

To specify a VLAN for IGMP snooping:

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

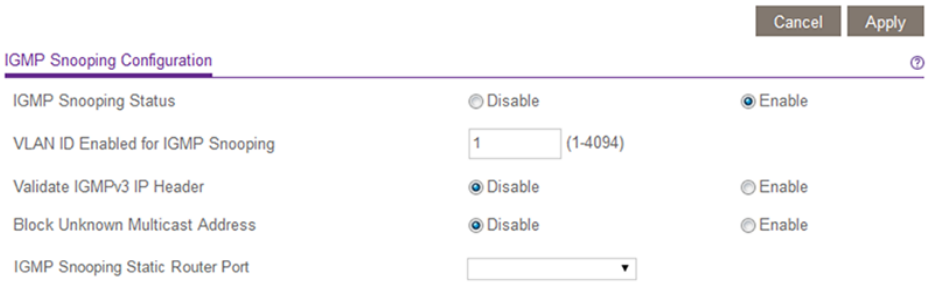
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

   The login window opens.

4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **System > Multicast**.



6. Make sure that the IGMP Snooping Status **Enable** radio button is selected.
   By default, the **Enable** radio button is selected.
7. In the **VLAN ID Enabled for IGMP Snooping** field, enter the ID of the VLAN.
   By default, if you enable IGMP snooping, snooping occurs on VLAN 1. However, you can enable snooping on any VLAN:
   - For port-based VLANs, you can enter a VLAN ID from 1 to the maximum number of ports that the switch supports.
   - For 802.1Q-based VLANs, you can enter a VLAN ID from 1 to 4094.
8. Click the **Apply** button.
   Your settings are saved.

Set Up Link Aggregation Groups

Note: Static link aggregation (port trunking) is supported on models GS116E, JGS516PE, JGS524E, and JGS524PE.

Link aggregation groups (LAGs) allow you to combine multiple Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and load sharing.

The number of LAGs that the switch supports depends on the model.

Configure LAG membership before you enable the LAG.

Note: The switch does not support IEEE 802.3ad Link Aggregation or Link Aggregation Control Protocol (LACP) groups but supports manual static LAGs only.

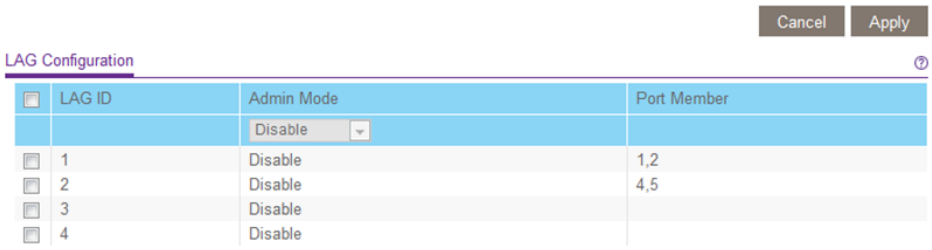
You must set up LAG membership before you can enable LAGs.

To specify LAG membership and enable a LAG:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **System > LAG > LAG Membership**.

   The previous figure is an example. Your switch might provide more or fewer ports.
6. In the **LAG ID** menu, select the LAG ID.
   The number of LAGs that the switch supports depends on the model.
7. Select the ports for the LAG by selecting the check boxes that are associated with the port numbers.
   A LAG consists of at least two ports.
8. Click the **Apply** button.
   Your settings are saved.

9. Select **System > LAG > LAG Configuration**.



10. Select the ID of the LAG for which you just set up the port membership.
11. In the **Admin Mode** menu, select **Enable**.
12. Click the **Apply** button.
    Your settings are saved.

5

Manage and Monitor the Switch

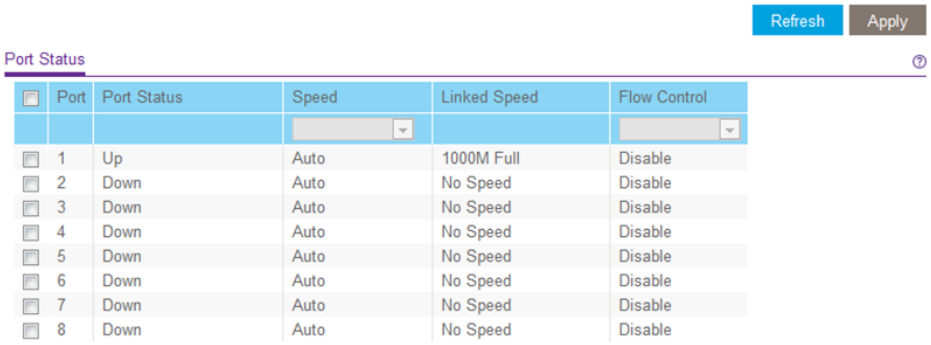
This chapter covers the following topics:

Manage Flow Control

Flow control works by pausing a port if the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. You can enable or disable IEEE 802.3x flow control. By default, flow control is disabled.

To manage flow control:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **System > Management > Port Status**.



   The previous figure is an example. Your switch might provide more or fewer ports.
6. Select one or more ports.
7. In the **Flow Control** menu, select **Enable** or **Disable**.
8. Click the **Apply** button.
   Your settings are saved.

Manage the Port Speed and the Port Status

By default, the port speed on all ports is set automatically after the switch determines the speed using autonegotiation with the link partner. You can select a specific port speed setting for each port, or disable a port by shutting it down manually.

To manage the port speed and the port status:

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

   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

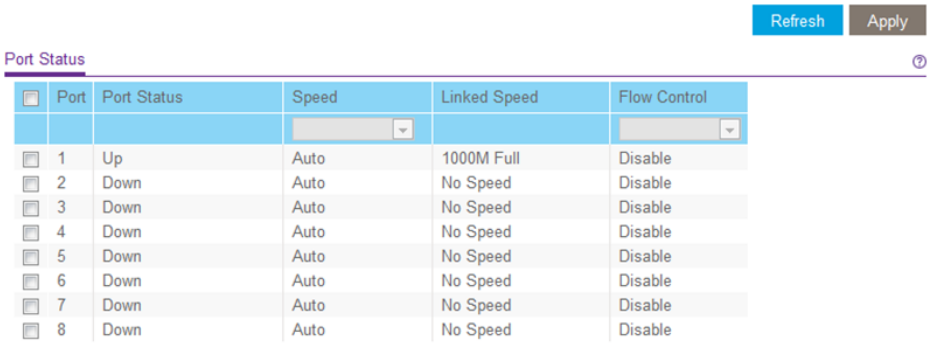
   The login window opens.

4. Enter the switch password.

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

   The Switch Information page displays.

5. Select **System > Management > Port Status**.



   The previous figure is an example. Your switch might provide more or fewer ports.

6. Select one or more ports.
7. In the **Speed** menu, select one of the following options:

   - **Auto**. The port speed is set automatically after the switch determines the speed using autonegotiation with the link partner. This is the default setting.
   - **Disable**. The port is shut down.

- **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.

8. To configure more ports, repeat this procedure from Step 6 on.
9. Click the **Apply** button.
   Your settings are saved.

Enable Loop Detection

If loop detection is enabled and the switch detects a loop, the LED or both LEDs of a port blink at a constant speed.

To enable loop detection:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **System > Management > Loop Detection**.
   The Loop Detection page displays.
6. Select the **Enable** radio button.
7. Click the **Apply** button.
   Your settings are saved.

Manage Power Saving Options

Note: Power saving options are available on models GS105Ev2, GS105PE, GS116Ev2, JGS516PE, JGS524Ev2, and JGS524PE.

Depending on the power saving options that your switch model provides, you can manage the IEEE 802.3az Energy Efficient Ethernet (EEE) function, cable length power saving, or link-down power saving, or a combination of these features:

- **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.
- **EEE**. Combines the Energy Efficient Ethernet (EEE) 802.3 MAC sublayer with the 100BASE-TX and 1000BASE-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.

To manage the power saving options:

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

   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

   The login window opens.

4. Enter the switch password.

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

   The Switch Information page displays.

5. Select **System > Management > Power Saving Mode**.

6. Select the **Enable** button to enable the power saving mode.
   By default, the **Disable** radio button is selected.
7. Click the **Apply** button.
   Your settings are saved.

Download and Update the Firmware

You can manually check for the latest firmware version for your switch by visiting netgear.com/support/download/.

Note: Instead of using the local browser interface, you can use the ProSAFE Plus Utility to update the firmware on the switch. In that situation, do not use a WiFi connection to the switch but use only a direct wired connection over an Ethernet cable. That is, configure a computer with an IP address in the same subnet as the switch and connect directly to the switch using an Ethernet cable before you start the firmware update using the ProSAFE Plus Utility.

To download and update the firmware using the local browser interface:

1. Visit netgear.com/support/download/.
2. In the **Enter a Product Name/Model Number** field, start typing the model number, and select the model from the menu that displays after you start typing.
   The available firmware versions displays.
3. Select and download the firmware version and release notes to your computer.
4. Read the release notes to find out if you must reconfigure the switch after upgrading.
5. Unzip the downloaded file to extract the firmware image.
6. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

7. Launch a web browser.
8. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

   The login window opens.

9. Enter the switch password.

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

   The Switch Information page displays.

10. Select **System > Maintenance > Firmware Update**.

    The Firmware Update page displays.

    The firmware update method depends on the current firmware and boot loader versions on your switch.

11. If the page displays the **Enter Loader Mode** button, click the **Enter Loader Mode** button.

    The switch reboots and enters into the loader mode. The Firmware Upgrade page that displays varies, depending on the firmware boot loader version that is already on your switch.

    Follow either Step 12 or Step 13, depending on which prompts you are presented with.

12. If you are prompted to update the firmware from a file, click the **Browse** button and locate and select the new firmware image file.
13. If you are prompted to provide both the TFTP server IP address and the image file name, do the following:
    a. Complete the **TFTP Server IP** address field.

       Note: This method requires that TFTP server software is installed on your computer to use the assigned TFTP server address from the TFTP server software application. If TFTP server software is not installed on your computer or if you are unsure how to do this, we recommend that you use the ProSAFE Plus Utility to update the firmware. For more information, see the *ProSAFE Plus Utility User Manual*, which you can download by visiting netgear.com/support/download/.

    b. Complete the **Image File Name** field.
    c. Make sure that the TFTP server launches the TFTP server application.

14. Click the **Apply** button.

Warning: To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not turn off the switch or disconnect it.

When the update is complete, your switch restarts. The update process typically takes about three minutes.

Reboot the Switch

You can reboot the switch remotely.

To reboot the switch:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **System > Maintenance > Device Reboot**.
   The Device Reboot page displays.
6. Select the check box.
7. Click the **Apply** button.
   The switch reboots.

Save the Switch Configuration

You can save the switch configuration as a file. We recommend that you save the configuration. Then you can quickly restore the switch configuration if you change the settings and then decide to return the switch to its previous settings.

To save the switch configuration:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **System > Maintenance > Save Configuration**.
   The Save Configuration page displays.
6. Click the **Save** button.
   A pop-up window opens. Depending on the settings of your browser, you can select a location to save the switch configuration file (a `.cfg` file).
7. Follow the directions of your browser to save the switch configuration.

Restore a Saved Switch Configuration

You can restore switch configuration that you saved.

To restore the switch configuration that you saved:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.

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

The Switch Information page displays.

5. Select **System > Maintenance > Restore Configuration**.
   The Restore Configuration page displays.
6. Click the **Browse** button and locate and select the saved configuration file (a `.cfg` file).
7. Click the **Apply** button.
   The saved configuration is restored to the switch.

Restore Factory Default Settings

You can return the switch to its factory settings.

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

To restore factory settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.

   The Switch Information page displays.
5. Select **System > Maintenance > Factory Default**.
   The Factory Default page displays.
6. Select the check box.
7. Click the **Apply** button.

The switch returns to its factory settings. The switch reboots to load the restored configuration.

Manage Access Control

Access control allows you to control which devices can access the switch over a web browser for management purposes. By default, access control is disabled. By adding one or more devices to the Access Control table, access control is enabled and only devices in the table are allowed to access the switch over a web browser.

Note: Models GS108Ev3 and GS108PEv3 do not support access control.

For more information, see the following sections:

- Add Devices to the Access Control Table on page 58
- Remove Devices From the Access Control Table on page 59

Add Devices to the Access Control Table

Be sure that you use a valid subnet mask when you add a device or a range of devices to the Access Control table.

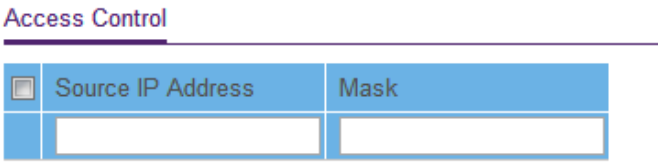
Caution: Add the IP address and subnet mask for the device from which you are accessing the switch to the Access Control table before you add any other devices to the table. Otherwise, you are locked out from the local browser interface of the switch.

To add devices to the Access Control table:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.

The Switch Information page displays.

5. Select **System > Maintenance > Access Control**.



6. For a device or range of devices that must be able to access the switch, configure the following settings:
   - **Source IP Address**. Enter the IP address of the device or range of devices that must be allowed to access the switch over a web browser.
   - **Mask**. Enter the subnet mask that is associated with the IP address.
7. Click the **Add** button.

   The device or range of devices is added to the table and your settings are saved. Access control is now enabled.
8. Repeat Step 6 and Step 7 for each device or range of devices that you want to add to the Access Control table.

Remove Devices From the Access Control Table

You can remove a device from the Access Control table. If you remove all devices from the table, access control is disabled.

To remove devices from the Access Control table:

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

   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

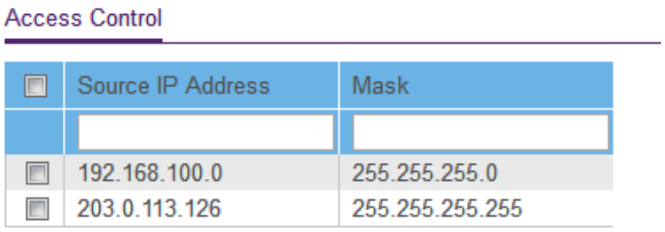
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

   The login window opens.
4. Enter the switch password.

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

   The Switch Information page displays.

5. Select **System > Maintenance > Access Control**.



6. Select one or more devices.
   To select all devices in the table, select the check box in the table heading.
7. Click the **Delete** button.
   The devices are removed from the table and your settings are saved. If you removed all devices from the table, access control is disabled.

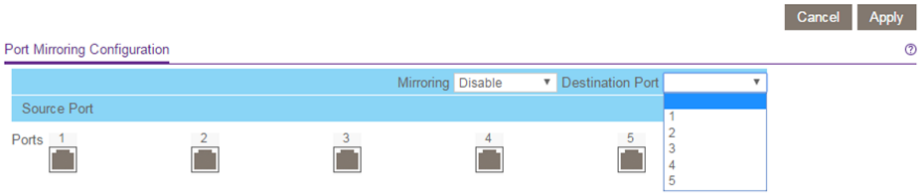
Enable Port Mirroring

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.

To enable port mirroring:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.
   The login window opens.
4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.

5. Select **System > Monitoring > Mirroring**.



   The previous figure is an example. Your switch might provide more or fewer ports.

6. In the **Destination Port** menu, select the destination port.
   You can select a single destination port only. You cannot select a destination port that is a member of a LAG.

7. In the Source Port section, select one or more source ports by selecting the check boxes that are associated with the port numbers.
   You can select more than one source port. You cannot select a source port that is a member of a LAG.

8. In the **Mirroring** menu, select **Enable**.
   By default, mirroring is disabled.

9. Click the **Apply** button.
   Your settings are saved.

View Switch Information or Change the Switch Device Name

You can view the switch product name (model), serial number, MAC address, firmware version, DHCP mode, and other network information.

You can also change the switch device name.

To view information about the switch or change the switch device name:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

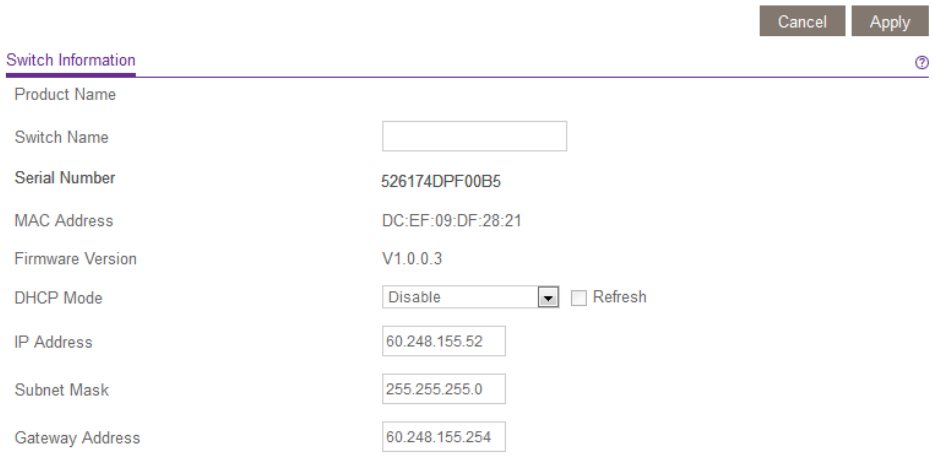
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

The login window opens.

4. Enter the switch password.

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



   To navigate to this page, select **System > Management > Switch Information**.

5. To change the switch device name, do the following:
   a. In the **Switch Name** field, enter a name of up to 20 characters.
   b. 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. Connect your computer to the same network as the switch.

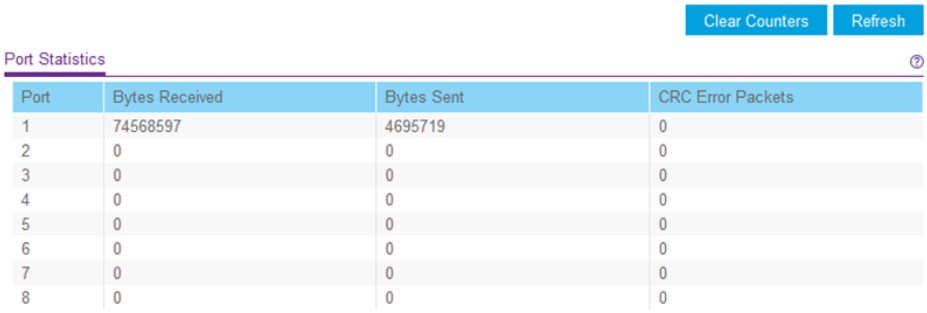
   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

The login window opens.

4. Enter the switch password.
   The default password is **password**. The password is case-sensitive.
   The Switch Information page displays.
5. Select **System > Monitoring > Port Statistics**.



Port	Bytes Received	Bytes Sent	CRC Error Packets
1	74568597	4695719	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0

   The previous figure is an example. Your switch might provide more or fewer ports.
6. To clear the port statistics, click the **Clear Counters** button.
   All statistics counters change to 0.

PoE Considerations for Switches That Support PoE

A switch that supports Power over Ethernet (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 802.3at 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.

The following table describes the PoE classes and switch allocations.

Table 1. Factory default settings

Device Class	Standard	Class Description	Minimum Power Allocated to the Powered Device	Range of Power Delivered to the Powered Device
0	PoE and PoE+	Default power (full)	0.44W	0.44W–12.95W
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–12.95W
4	PoE+ only	High power	30.0W	12.95W–25.5W

6

Diagnostics and Troubleshooting

This chapter covers the following topics:

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

   You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the Switch Using a Web Browser on page 10.

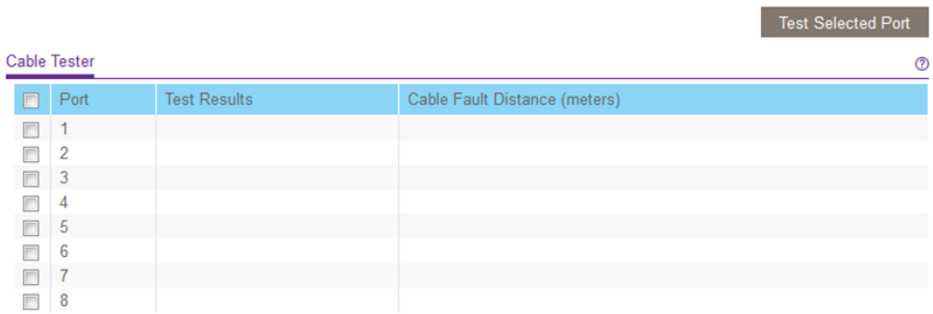
   The login window opens.

4. Enter the switch password.

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

   The Switch Information page displays.

5. Select **System > Monitoring > Cable Tester**.



   The previous figure is an example. Your switch might provide more or fewer ports.

6. Select one or more check boxes.
7. Depending on the model, click the **Test Selected Port** or **TEST** button.

   The switch tests the cable connection for the selected ports and displays the results. This process might take up to a few minutes.

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 use the ProSAFE Plus Utility 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 that are listed in the following table.

Table 2. 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.

A

Factory Default Settings

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

Table 3. Factory default settings

Feature	Setting
Switch 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	Enabled
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 detection	Disabled
Port speed	Autonegotiation
Flow control	Disabled
Port mirroring	Disabled