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

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

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

See the regulatory compliance document before connecting the power supply.

Trademarks
© NETGEAR, Inc., NETGEAR, and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.
This chapter covers the following topics:

- Configure the Switch
- Access the Switch Using a Web Browser
- Access the Switch Using the NETGEAR Insight App
- Access the Switch With the ProSAFE Plus Utility
- Change the Password
- Register Your Product

Note For hardware information, see the hardware installation guide (HIG) for your switch model. You can download the HIG by visiting downloadcenter.netgear.com.

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 downloadcenter.netgear.com. You can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, see the latest firmware release notes for your switch model.
Configure the Switch

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. You can also configure and manage additional advanced features of the switch either by using your computer’s web browser or by installing the ProSAFE® Plus Utility on your Windows-based computer.

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 (on-network). 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).

Access the Switch Using a Web Browser

This manual describes the web browser–based management interface.

You can access and configure the switch directly through its web browser–based management interface by entering the switch’s IP address in the address bar of a browser. When using web-browser setup, 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 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.

4. When prompted, enter the password.
   The default password is password.

5. Click the Login button.
   You can now configure additional options for the switch in the web management interface.

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.

Get Started

6
Access a Switch That Is Connected to a Network

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.
   DHCP is enabled on the switch by default. Use the IP address that the DHCP server assigned to the switch. If you are unsure how to determine the IP address of the switch, you can use the ProSAFE® Plus Utility or an IP scanner utility.
5. Open a web browser, and enter the IP address of the switch.
6. When prompted, enter the password.
   The default password is password.
7. Click the Login button.
   You can now configure additional options for the switch in the web management interface.

Access the Switch Using the NETGEAR Insight App

The switch supports the NETGEAR Insight app, which you can install on a mobile device.
Using the NETGEAR Insight app, you can discover the switch on the network, register it, and add the switch to the NETGEAR Insight app. Once the switch is added to the NETGEAR Insight app, you can configure basic management settings, locally monitor the switch status, and launch the web management interface.
You can choose from three methods to add the switch to the NETGEAR Insight app. All three methods require that the smartphone on which the NETGEAR Insight app is installed is connected to the same network as the switch. Use one of the following methods:

- Add the switch from the Day Zero discovery page.
- Add the switch from the Network page.
- Add the switch from the Device List page.

For more information, see the NETGEAR knowledge base articles at netgear.com/support.

Access the Switch With the ProSAFE Plus Utility

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. The utility is located on the resource CD that came with the switch. You can also visit netgear.com/support/product/PCU to download the 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 from the resource CD:

1. Insert the resource CD into a computer that is connected to the switch. The Resource CD page displays.

2. Click the **Install ProSAFE Plus Utility** link and follow the prompts to install the program. The utility is installed in the program directory of your computer and a **ProSAFE Plus Utility** icon is placed on your desktop.

3. 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 6.

▶ 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 address.

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.

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.
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.

Note

5. Select the Smart Managed Plus Switch that you want to configure.
   If you do not see the switch, click the REFRESH button.

6. When prompted, enter the password.
   The default password is password.
   The Switch Information page displays.

7. Use the utility to configure the switch settings.

8. 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 links on the Help tab of the utility or from the resource CD, or you can download it by visiting downloadcenter.netgear.com.

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 6.
   The login window opens.

4. Enter the switch's password in the password field.
   The switch's default password is password.
   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.

## Register Your Product

Registering your product allows you to receive email alerts and streamlines the technical support process.

*To register your product:*

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 6.
   The login window opens.
4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
   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.
This chapter covers the following topics:

- Specify IP Address Settings for the Switch
- Manage Multicast Traffic With IGMP Snooping
- Set Up Link Aggregation
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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   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

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.

   ![IP Setting](image)

   **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’s password in the **Password** field.
   The switch’s default password is **password**.

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 6.
   The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
   The Switch Information page displays.
5. Select **System > Multicast**.

6. Select the IGMP Snooping Status **Enable** radio button. By default, the **Enable** radio button is selected.

7. Make sure that a VLAN ID between 1 and 4094 is stated in the **VLAN ID Enabled for IGMP Snooping** field. 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 23).

   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) 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. Select one of the following **IGMP Snooping Static Router Port** radio buttons:

   - **Auto**. If the switch receives a query message, the switch configures the router port or ports dynamically. This is the default setting.
   - **Any**. IGMP Join and Leave packets are sent to every port of the switch.
   - **Static**. Select one port as the dedicated IGMP snooping static router port by selecting the check box that is associated with the port number. All IGMP Join and Leave reports are forwarded to the selected 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 23).

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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

5. Select System > Multicast.

6. Select the IGMP Snooping Status Enable radio button.
   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 50.
   - For 802.1Q-based VLANs, you can enter a VLAN ID from 1 to 4094.

8. Click the Apply button.
   Your settings are saved.
Enable the Auto-Video Configuration

You can enable the Auto-Video VLAN for IGMP snooping only if you enabled port-based or 802.1Q-based VLANs (see Use VLANS for Traffic Segmentation on page 23). By default, the Auto-Video VLAN is disabled. The default ID of the Auto-Video VLAN is ID 3, which you cannot change.

To enable the Auto-Video 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 6.
   The login window opens.
4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.
5. Select System > Multicast > Auto-Video.
   The Auto-Video Configuration page displays.
6. Select the Auto-Video Status Enable radio button.
   By default, the Disable radio button is selected.
7. Click the Apply button.
   Your settings are saved.

Set Up Link Aggregation

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. Configure LAG membership before you enable the LAG. The switch supports eight LAGs.

The switch supports both static link aggregation (port trunking) and Link Aggregation Control Protocol (LACP) groups through IEEE 802.3ad Link Aggregation.

Set up link aggregation in the following order:

1. Set up the LAG on the switch.
2. Connect the ports that you made members of the LAG on the switch to the ports that are members of a LAG on another device in your network.

For more information, see the following sections:
Set Up a Static Link Aggregation Group

The switch supports eight LAGs, which can be a combination of static link aggregation and LACP groups. You must set up LAG membership before you can enable LAGs.

To specify LAG membership for a static LAG and enable a static 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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

5. Select System > LAG > LAG Membership.

6. In the LAG ID menu, select the LAG ID.

7. Enter a name in the LAG Name field.
   You can enter a name of up to 15 alphanumeric characters.

8. 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.

9. Click the Apply button.
   Your settings are saved.
10. Select **System > LAG > LAG Configuration**.

11. Select the LAG ID of the LAG for which you just set up the port membership.

12. In the **Admin Mode** menu, select **Enable**.

13. In the **LAG Type** menu, select **Static**.
   - The Port Member field for the selected LAG ID shows the ports that you selected in **Step 8**.
   - The LAG Status field for the selected LAG ID shows whether the LAG is established (Up) or not established (Down).

14. Click the **Apply** button.
   - Your settings are saved.

---

**Set Up a Link Aggregation Control Protocol Group**

The switch supports eight LAGs, which can be a combination of Link Aggregation Control Protocol (LACP) groups and static link aggregation groups.

**To specify an LACP group:**

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 6.
   - The login window opens.

4. Enter the switch’s password in the **password** field.
   - The switch’s default password is **password**.
   - The Switch Information page displays.
5. Select System > LAG > LAG Membership.

![LAG Membership](image)

6. In the LAG ID menu, select the LAG ID.

7. Enter a name in the LAG Name field.
   You can enter a name of up to 15 alphanumeric characters.

8. 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.

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

10. Select System > LAG > LAG Configuration.

![LAG Configuration](image)

11. Select the LAG ID of the LAG for which you just set up the port membership.

12. In the Admin Mode menu, select Enable.

13. In the LAG Type menu, select LACP.
   The Port Member field for the selected LAG ID shows the ports that you selected in Step 8.
   The LAG Status field for the selected LAG ID shows whether the LAG is established (Up) or not established (Down).

14. Click the Apply button.
   Your settings are saved.

**Set Up the LACP System Priority for the Switch**

The LACP system priority specifies the link aggregation priority of the switch relative to the devices at the other ends of the links on which link aggregation is enabled. The default is 32768. A higher value indicates a lower priority. The value of the priority applies to all LACP LAGs that you set up on the switch.

---

**Manage Network Settings**

20
To change the LACP system priority:

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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

5. Select System > LAG > LACP Configuration.
   The LACP Configuration page displays.

6. In the LACP System Priority field, enter a number from 1 to 65535.
   The default is 32768.

7. Click the Apply button.
   Your settings are saved.

Set Up LACP Port Priority and Time-Out Values

You can set the LACP port priority value and LACP time-out value for a port. By default, the LACP port priority value for a port is 128 and the time-out value is Long.

To specify LACP port priority value and LACP time-out value for a port:

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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

---

Manage Network Settings

21
5. Select **System > LAG > LACP Port Configuration**.

6. Select one or more ports.

7. In the **LACP Priority** field, enter a new value.
   You can enter a value from 1 to 65535. A higher value indicates a lower priority. The default value is 128.

8. In the **Timeout** menu, select the time-out value.
   The default value is Long. The other option is Short.

9. Click the **Apply** button.
   Your settings are saved.
This chapter covers the following topics:

- VLAN Overview
- Create Basic Port-Based VLANs
- Assign Ports to Multiple Port-Based VLANs
- Create 802.1Q-Based VLANs in a Basic Configuration
- Create 802.1Q-Based VLANs in an Advanced Configuration
- Add Tagged or Untagged Ports to an 802.1Q-Based VLAN
- Specify a Port PVID for an 802.1Q-Based VLAN
- Manage the Voice VLAN
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 25). 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 6.
   The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
   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 the Basic Port-based 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.

Use VLANS for Traffic Segmentation
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.

<table>
<thead>
<tr>
<th>Port</th>
<th>g1</th>
<th>g2</th>
<th>g3</th>
<th>g4</th>
<th>g5</th>
<th>g6</th>
<th>g7</th>
<th>g8</th>
<th>g9</th>
<th>g10</th>
<th>g11</th>
<th>g12</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>g13</th>
<th>g14</th>
<th>g15</th>
<th>g16</th>
<th>g17</th>
<th>g18</th>
<th>g19</th>
<th>g20</th>
<th>g21</th>
<th>g22</th>
<th>g23</th>
<th>g24</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Group</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>g25</th>
<th>g26</th>
<th>g27</th>
<th>g28</th>
<th>g29</th>
<th>g30</th>
<th>g31</th>
<th>g32</th>
<th>g33</th>
<th>g34</th>
<th>g35</th>
<th>g36</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Group</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>g37</th>
<th>g38</th>
<th>g39</th>
<th>g40</th>
<th>g41</th>
<th>g42</th>
<th>g43</th>
<th>g44</th>
<th>g45</th>
<th>g46</th>
<th>g47</th>
<th>g48</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Group</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>g49</th>
<th>g50</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Group</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

9. Under each port to be added to a VLAN, enter the VLAN 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.

**Use VLANS for Traffic Segmentation**
If you do not know the IP address of the switch, see *Access the Switch Using a Web Browser* on page 6.

The login window opens.

4. Enter the switch’s password in the **password** field.
The switch’s default password is **password**.
The Switch Information page displays.

5. Select **VLAN > Port Based > Advanced**.
The Advanced Port-based VLAN Status page displays.

6. If this is the first time that you are accessing the Advanced Port-based 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 Configuration and VLAN Membership sections display.

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 checkes box that are associated with the port numbers.

---

**Use VLANS for Traffic Segmentation**

26
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 28.

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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   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.

Use VLANS for Traffic Segmentation
The Basic 802.1Q VLAN Identifier table displays.

<table>
<thead>
<tr>
<th>Port</th>
<th>g1</th>
<th>g2</th>
<th>g3</th>
<th>g4</th>
<th>g5</th>
<th>g6</th>
<th>g7</th>
<th>g8</th>
<th>g9</th>
<th>g10</th>
<th>g11</th>
<th>g12</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Port</td>
<td>g13</td>
<td>g14</td>
<td>g15</td>
<td>g16</td>
<td>g17</td>
<td>g18</td>
<td>g19</td>
<td>g20</td>
<td>g21</td>
<td>g22</td>
<td>g23</td>
<td>g24</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Port</td>
<td>g25</td>
<td>g26</td>
<td>g27</td>
<td>g28</td>
<td>g29</td>
<td>g30</td>
<td>g31</td>
<td>g32</td>
<td>g33</td>
<td>g34</td>
<td>g35</td>
<td>g36</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Port</td>
<td>g37</td>
<td>g38</td>
<td>g39</td>
<td>g40</td>
<td>g41</td>
<td>g42</td>
<td>g43</td>
<td>g44</td>
<td>g45</td>
<td>g46</td>
<td>g47</td>
<td>g48</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Port</td>
<td>g49</td>
<td>g50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN ID</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

9. Under each port to be added to a VLAN, enter the VLAN 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 6.
   The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
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.

By default, all ports are members of VLAN 1.

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 28), 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.

**Use VLANS for Traffic Segmentation**
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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   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 28).

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.

Use VLANS for Traffic Segmentation
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. 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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   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 28).

### PVID Configuration

<table>
<thead>
<tr>
<th>Port</th>
<th>PVID</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>1</td>
</tr>
<tr>
<td>g2</td>
<td>1</td>
</tr>
<tr>
<td>g3</td>
<td>1</td>
</tr>
<tr>
<td>g4</td>
<td>1</td>
</tr>
<tr>
<td>g5</td>
<td>1</td>
</tr>
<tr>
<td>g6</td>
<td>1</td>
</tr>
<tr>
<td>g7</td>
<td>1</td>
</tr>
<tr>
<td>g8</td>
<td>1</td>
</tr>
<tr>
<td>g9</td>
<td>1</td>
</tr>
<tr>
<td>g10</td>
<td>1</td>
</tr>
<tr>
<td>g11</td>
<td>1</td>
</tr>
<tr>
<td>g12</td>
<td>1</td>
</tr>
<tr>
<td>g13</td>
<td>1</td>
</tr>
<tr>
<td>g14</td>
<td>1</td>
</tr>
<tr>
<td>g15</td>
<td>1</td>
</tr>
<tr>
<td>g16</td>
<td>1</td>
</tr>
</tbody>
</table>

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.

### Manage the Voice VLAN

The switch supports a voice VLAN to facilitate voice over IP (VoIP) traffic. If you enable the 802.1Q VLAN mode (see *Create 802.1Q-Based VLANs in a Basic Configuration* on page 27 or *Create 802.1Q-Based VLANs in an Advanced Configuration* on page 28), the voice VLAN is enabled by default. The default ID of the voice VLAN is ID 2, which you can change.

For more information, see the following sections:

- *Specify the Voice VLAN Properties* on page 33
- *Enable the Voice VLAN Mode for Ports* on page 33
- *Manage the OUI Table* on page 35
Specify the Voice VLAN Properties

By default, the voice VLAN is enabled. The default ID of the voice VLAN is ID 2. The default Class of Service (CoS) value is 6. The voice VLAN properties apply to all traffic on the voice VLAN.

You can change the voice VLAN properties only if you enable the 802.1Q VLAN mode (see Create 802.1Q-Based VLANs in a Basic Configuration on page 27 or Create 802.1Q-Based VLANs in an Advanced Configuration on page 28).

The voice VLAN can be effective only if you enable the voice VLAN mode for individual interfaces (see Enable the Voice VLAN Mode for Ports on page 33).

To specify the voice VLAN properties:

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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

5. Select VLAN > Voice VLAN > Properties.
   The Voice VLAN Properties page displays.

6. In the Voice VLAN ID menu, select the voice VLAN.
   You can select either one of the default VLAN IDs (1, 2, or 3) or a VLAN that you manually added (see Create 802.1Q-Based VLANs in a Basic Configuration on page 27 or Create 802.1Q-Based VLANs in an Advanced Configuration on page 28). The default voice VLAN ID is 2.

7. In the Class of Service menu, select the class value for the voice VLAN.
   You can select a value from 0 (the lowest priority) to 7 (the highest priority). The default CoS value is 6.

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

Enable the Voice VLAN Mode for Ports

You can enable the voice VLAN mode for individual ports so that these ports become members of the voice VLAN. By default, the voice VLAN mode is disabled for all ports.
To enable the voice VLAN mode for 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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

5. Select VLAN > Voice VLAN > Port Settings.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Voice VLAN Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>Disable</td>
</tr>
<tr>
<td>g2</td>
<td>Disable</td>
</tr>
<tr>
<td>g3</td>
<td>Disable</td>
</tr>
<tr>
<td>g4</td>
<td>Disable</td>
</tr>
<tr>
<td>g5</td>
<td>Disable</td>
</tr>
<tr>
<td>g6</td>
<td>Disable</td>
</tr>
<tr>
<td>g7</td>
<td>Disable</td>
</tr>
<tr>
<td>g8</td>
<td>Disable</td>
</tr>
<tr>
<td>g9</td>
<td>Disable</td>
</tr>
<tr>
<td>g10</td>
<td>Disable</td>
</tr>
<tr>
<td>g11</td>
<td>Disable</td>
</tr>
<tr>
<td>g12</td>
<td>Disable</td>
</tr>
<tr>
<td>g13</td>
<td>Disable</td>
</tr>
<tr>
<td>g14</td>
<td>Disable</td>
</tr>
<tr>
<td>g15</td>
<td>Disable</td>
</tr>
<tr>
<td>g16</td>
<td>Disable</td>
</tr>
</tbody>
</table>

6. Select one or more ports.

7. In the Voice VLAN Mode menu, select Enable.
   By default, the voice VLAN mode is disabled for all ports.

8. Click the Apply button.
   Your settings are saved.
Manage the OUI Table

The switch supports 10 default Organizationally Unique Identifiers (OUIs), which are associated with VoIP phones of specific manufacturers. All traffic received on voice VLAN ports from VoIP phones with a listed OUI is forwarded on the voice VLAN.

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

To manage the OUI 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 6.
   The login window opens.
4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.
5. Select VLAN > Voice VLAN > OUI Table.

<table>
<thead>
<tr>
<th>Telephony (OUIs)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:01:E3</td>
<td>SIEMENS</td>
</tr>
<tr>
<td>00:03:6B</td>
<td>CISCO1</td>
</tr>
<tr>
<td>00:04:0D</td>
<td>AVAYA1</td>
</tr>
<tr>
<td>00:0F:E2</td>
<td>H3C</td>
</tr>
<tr>
<td>00:12:43</td>
<td>CISCO2</td>
</tr>
<tr>
<td>00:1B:4F</td>
<td>AVAYA2</td>
</tr>
<tr>
<td>00:50:B9</td>
<td>NITSUKO</td>
</tr>
<tr>
<td>00:D0:1E</td>
<td>PINETEL</td>
</tr>
<tr>
<td>00:E0:75</td>
<td>VERILINK</td>
</tr>
<tr>
<td>00:E0:BB</td>
<td>3COM</td>
</tr>
</tbody>
</table>

6. Take one of the following actions:
• To add an OUI prefix to the table, do the following:
  
a. In the **Telephony (OUIs)** field, enter an OUI in the format AA:BB:CC.
  
b. In the **Description** field, enter a description with a maximum of 32 characters.
  
c. Click the **Add** button.
      The OUI is added to the table.

• To delete one or more OUI prefixes from the table, do the following:
  
a. Select one or more OUIs.
  
b. Click the **Delete** button.
      The OUIs are removed from the table.

• To change an existing OUI prefix in the table, do the following:
  
a. Select the OUI.
  
b. Change the OUI in the **Telephony (OUIs)** field, change the description in the **Description** field,
      or change both.
  
c. Click the **Apply** button.
      Your settings are saved.
Manage Security

This chapter covers the following topics:

- Manage Access Control
- Set the Switch Management Mode
- Disable Bonjour for Discovery
- Manage the Auto Denial of Service Mode
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.

For more information, see the following sections:

- Add Devices to the Access Control Table on page 38
- Remove Devices From the Access Control Table on page 39

Add Devices to the Access Control Table

Use the following guidelines for adding devices to the Access Control table:

- The IP address must be a unicast address.
- The subnet mask must be valid.
- To allow all devices under a subnet, enter 0 for the host address, that is, the host ID portion of the IP address. For example, if you enter 192.168.100.0, all devices in the 192.168.100.1–192.168.100.254 range are allowed to access the switch over a web browser.

CAUTION:
Add the MAC 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 web management 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 6.
   The login window opens.

4. Enter the switch's password in the password field.
   The switch’s default password is password.
   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 6.
   The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
   The Switch Information page displays.
5. Select **System > Maintenance > Access Control**.

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>203.0.113.126</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

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.

**Set the Switch Management Mode**

By default, you can manage the switch through a web browser and through the ProSAFE Plus Utility. You can change the switch management mode so that only management through a web browser is enabled and access through the ProSAFE Plus Utility is disabled. Even if you disable management through the ProSAFE Plus Utility, the switch and its IP address on the network are still discoverable through the ProSAFE Plus Utility.

To set the switch management mode:

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 6.
   The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
   The Switch Information page displays.

5. Select **System > Management > Switch Management Mode**.
   The Switch Management Mode page displays.

6. Select one of the following radio buttons:
Web browser Only. You can configure the switch through a web browser only.

Web browser GUI and ProSAFE Utility. You can configure the switch through a web browser or through the ProSAFE Plus Utility. This is the default setting.

7. Click the Apply button.
   Your settings are saved.

Disable Bonjour for Discovery

By default, the Bonjour protocol is enabled on the switch to allow for native discovery on macOS devices. For additional security, you can disable Bonjour on the switch, preventing macOS devices from discovering the switch.

To disable Bonjour on 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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

5. Select System > Management > Switch Management Mode.
   The Switch Management Mode page displays.

6. Select the Disable radio button.
   By default, the Enable radio button is selected.

7. Click the Apply button.
   Your settings are saved.

Manage the Auto Denial of Service Mode

Automatic denial of service mode (Auto DoS mode) enables all the DoS features. By default, Auto DoS mode is enabled but you can disable it. We recommend that you keep the Auto DoS mode enabled.

The TCP and UDP ports are always enabled, but you can shut down individual ports (see Manage the Port Speed and the Port Status on page 51).
To manage the Auto DoS mode:

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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

5. Select System > Management > Denial of Service.
   The Auto-DoS Configuration page displays.

6. Select one of the following radio buttons:
   - Enable. Enables the Auto DoS mode.
   - Disable. Disables the Auto DoS mode.

7. Click the Apply button.
   Your settings are saved.
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

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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   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 6. The login window opens.

4. Enter the switch’s password in the password field. The switch’s default password is password. 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 Step 7. 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.
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 6.
   The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
   The Switch Information page displays.
5. Select **QoS > Rate Limit**.

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 6.

The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   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 Step 7.
   Otherwise, see Step 8.

7. Click the Apply button.
   Your settings are saved and the Storm Control Rate table displays.

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 Kbps to 512 Mbps. 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.
Manage and Monitor the Switch

This chapter covers the following topics:

- Manage Flow Control
- Manage the Port Speed and the Port Status
- Enable Loop Prevention
- Manage Power Saving Options
- Download and Upgrade the Firmware
- Reboot the Switch
- Save the Switch Configuration
- Restore a Saved Switch Configuration
- Restore Factory Default Settings
- Enable Port Mirroring
- View Switch Information
- View or Clear the Port Statistics
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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

5. Select System > Management > Port Status.

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 and Monitor the Switch
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 6.
   The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
   The Switch Information page displays.

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

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 Step 6 and Step 7.

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

---

**Enable Loop Prevention**

If loop prevention is enabled and the switch detects a loop, the switch blocks one of the ports that are part of the loop and both LEDs of that port blink at a constant speed. If two ports are part of a loop, the port with the highest port number is blocked. For example, if port 1 and port 2 are part of a loop, port 2 is blocked while port 1 continues to process traffic. The loop status (that is, port blocking and LED blinking) is cleared if the switch does not detect the loop for a period of about 16 seconds.

To enable loop prevention:

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 6.
   The login window opens.

4. Enter the switch's password in the **password** field.
   The switch's default password is **password**.
   The Switch Information page displays.

5. Select **System > Management > Loop Prevention**.
   The Loop Prevention page displays.

6. Select the **Enable** radio button.
   By default, the **Disable** radio button is selected.

7. Click the **Apply** button.
   Your settings are saved.
Manage Power Saving Options

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-up and 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 6.
   The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
   The Switch Information page displays.

5. Select **System > Management > Power Saving Mode**.
   The Power Saving Mode page displays.

6. Select the one of the following radio buttons:
   - **Enable.** The power saving options are enabled. This is the default setting.
   - **Disable.** The power saving options are disabled.

7. Click the **Apply** button.
   Your settings are saved.
Download and Upgrade the Firmware

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

To download and upgrade the firmware:

2. Enter your product model number in the Enter a Product Name/Model Number field, search by clicking the magnifying glass, and locate the firmware for your switch.
3. Download the firmware to your computer.
4. Read the new firmware release notes to find out if you must reconfigure the switch after upgrading.
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.
7. 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 6.
   The login window opens.
8. Enter the switch’s password in the password field. The switch’s default password is password.
   The Switch Information page displays.
10. Click the Browse button and locate and select the new firmware image file.
11. 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. The upgrade 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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
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 6.
   The login window opens.

4. Enter the switch's password in the password field.
   The switch's default password is password.
   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.

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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.

   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.

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 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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
5. Select **System > Monitoring > Mirroring**.

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**

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

▶ To view information about 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 6.

The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.

---

### 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 6.
   The login window opens.

4. Enter the switch’s password in the **password** field.
   The switch’s default password is **password**.
   The Switch Information page displays.
5. Select **System > Monitoring > Port Statistics**.

6. To clear the port statistics, click the **Clear Counters** button.
   
   All statistics counters change to 0.
This chapter covers the following topics:

- Test Cable Connections
- Resolve a Subnet Conflict to Access the Switch
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 6.
   The login window opens.

4. Enter the switch’s password in the password field.
   The switch’s default password is password.
   The Switch Information page displays.

5. Select System > Monitoring > Cable Tester.

<table>
<thead>
<tr>
<th>Port</th>
<th>Test Results</th>
<th>Cable Fault Distance (meters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g18</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. Select one or more check boxes.

7. Click the Test Selected Port 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. Unplug the switch's power cord.
3. Reconnect the Ethernet cable between the switch and your network.
4. Plug the switch's power cord into an electrical outlet.

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.
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 1. Factory default settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch password</td>
<td>password</td>
</tr>
<tr>
<td>IP address</td>
<td>192.168.0.239 (if the switch is not connected to a network with a DHCP server)</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DHCP mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>IGMP snooping</td>
<td>Enabled</td>
</tr>
<tr>
<td>LAGs</td>
<td>None configured</td>
</tr>
<tr>
<td>VLANs</td>
<td>Disabled. If enabled, by default, all ports are members of VLAN 1.</td>
</tr>
<tr>
<td></td>
<td>If enabled, the default voice VLAN is VLAN 2.</td>
</tr>
<tr>
<td></td>
<td>If enabled, the default Auto-Video VLAN is VLAN 3.</td>
</tr>
<tr>
<td>802.1p/DSCP-based QoS</td>
<td>Enabled</td>
</tr>
<tr>
<td>Port-based QoS</td>
<td>Disabled</td>
</tr>
<tr>
<td>Rate limiting</td>
<td>Disabled</td>
</tr>
<tr>
<td>Broadcast filtering</td>
<td>Disabled</td>
</tr>
<tr>
<td>Loop prevention</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port speed</td>
<td>Autonegotiation</td>
</tr>
<tr>
<td>Flow control</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port mirroring</td>
<td>Disabled</td>
</tr>
<tr>
<td>Access control</td>
<td>Disabled</td>
</tr>
<tr>
<td>Power saving mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>Switch Management mode</td>
<td>Web browser and ProSAFE Plus Utility</td>
</tr>
</tbody>
</table>
Table 1. Factory default settings (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bonjour</td>
<td>Enabled</td>
</tr>
<tr>
<td>Auto-DoS mode</td>
<td>Enabled</td>
</tr>
</tbody>
</table>