NETGEAR®

User Manual

8-Port or 16-Port 10-Gigabit/Multi-Gigabit
Smart Managed Plus Switch with
1 Copper/SFP+ Combo Port

Models
XS708Ev2
XS716E

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

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

Revision History

Publication Part Number	Publish Date	Comments
202-11656-04	May 2019	- Added Safety instructions and warnings. - Entirely revised the information in Chapter 2, Getting Started and added the following new sections: - Use the NETGEAR Switch Discovery Tool to access the switch - Use the NETGEAR Insight App to discover and register the switch - Change the language of the local browser interface - Changed the switch product names to the current names. - Changed web-based management interface to local browser interface. - Removed information about the resource CD. - Updated the book to the latest NETGEAR format.
202-11656-03	March 2017	Made corrections to Specify a port PVID for an 802.1Q-based VLAN.
202-11656-02	August 2016	Added switch model XS716E to this manual.
202-11656-01	April 2016	First publication.

User Manual

Contents

Chapter 6   Manage and Monitor the Switch

Chapter 7   Diagnostics and Troubleshooting

Appendix A   Supplemental Information

1

Hardware Setup

The NETGEAR 8-Port or 16-Port 10-Gigabit/Multi-Gigabit Smart Managed Plus Switch provides 10-Gigabit copper ports and one shared (combo) copper/SFP+ fiber port. Switch model XS708Ev2 includes 8 ports. Switch model XS716E includes 16 ports. You can either use the 10G copper port (8T or 16T), or use the 10G fiber SFP+ slot (8F or 16F).

Using the 10G ports, you can create high-speed connections to a server, network-attached storage (NAS) system, or backbone network. For example, you can do the following:

- Connect switches to each other with high-speed links
- Link to high-speed servers
- Provide 100M/1G/10G copper and 1G/10G fiber connectivity

This chapter covers the following topics:

- Package contents
- Switch front panel
- Switch back panel
- Connect equipment to model XS708Ev2
- Connect equipment to model XS716E
- Check the switch status using the LEDs
- Safety instructions and warnings

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/. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

Package contents

The package includes the items shown in the following figures. In addition, the package includes the installation guide.

The power cord is localized to the country of sale. The power cord that is shown in the following figures is for illustration only.

Figure 1. XS708Ev2 switch package contents

Figure 2. XS716E switch package contents

Switch front panel

The switch provides eight 100M/1G/10G copper RJ-45 ports, of which port 8T and slot 8F form a shared (combo) port. The 1G/10G SFP+ slots (8F) accept fiber modules. You use either port 8T or port 8F. Each copper RJ-45 port is capable of sensing the line speed and negotiating the duplex mode with the link partner automatically.

XS708Ev2 front panel

The following figure shows the front panel of the switch.

Figure 3. XS708Ev2 switch front panel

From left to right, the front panel contains the following components:

- Power and Fan LEDs.
- Recessed **Factory Defaults** button to restore the device back to the factory defaults.
- Eight RJ-45 connectors for 100M/1G/10G AutoSensing 10-Gigabit Ethernet switching ports.
- One port (8) is a combo port: You can either use port 8T as Gigabit Ethernet switching port or you can install a fiber module in 1G/10G SFP+ slot 8F.
- Speed and Activity (ACT) LEDs for each port.

XS716E front panel

The following figure shows the front panel of the switch.
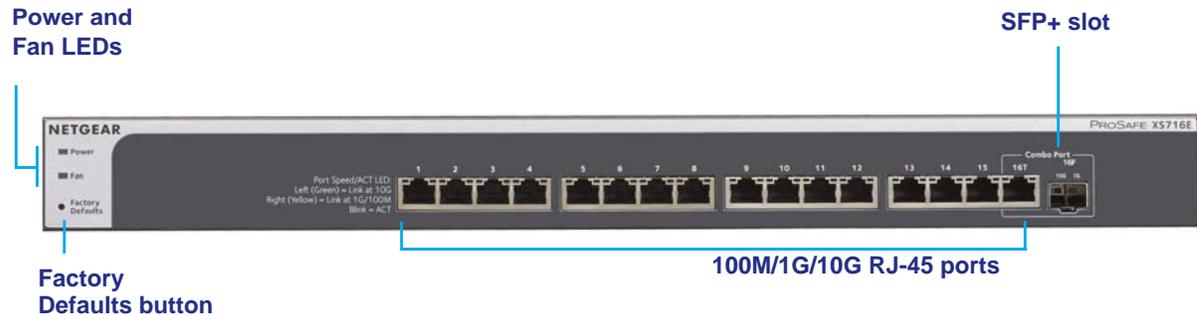
Figure 4. XS716E switch front panel

From left to right, the front panel contains the following components:

- Power and Fan LEDs.
- Recessed **Factory Defaults** button to restore the device back to the factory defaults.
- Sixteen RJ-45 connectors for 100M/1G/10G AutoSensing 10-Gigabit Ethernet switching ports.
- One port (16) is a combo port: You can either use port 16T as Gigabit Ethernet switching port or you can install a fiber module in 1G/10G SFP+ slot 16F.
- Speed and Activity (ACT) LEDs for each port.

Switch back panel

The back panel contains a Kensington™ lock slot and the AC power connector.

The following figure shows the back panel of model XS708Ev2.
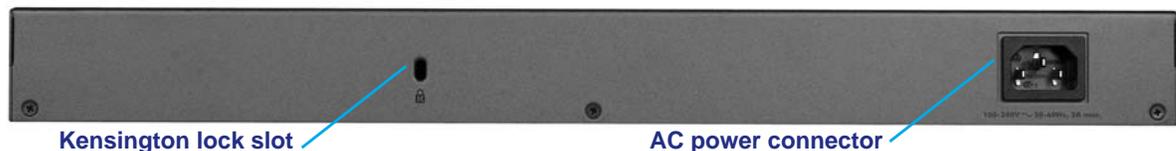
Figure 5. XS708Ev2 switch back panel

The following figure shows the back panel of model XS716E.

Figure 6. XS716E switch back panel

Connect equipment to model XS708Ev2
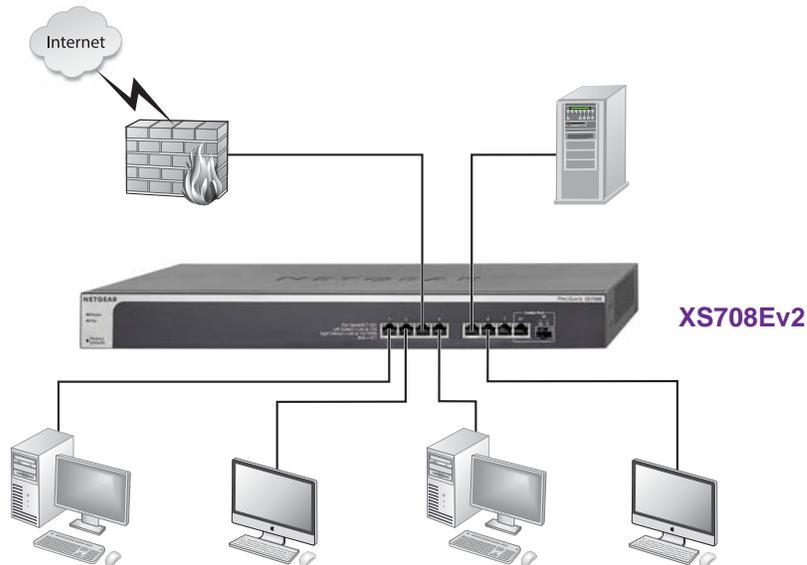
Figure 7. XS708Ev2 desktop switching configuration
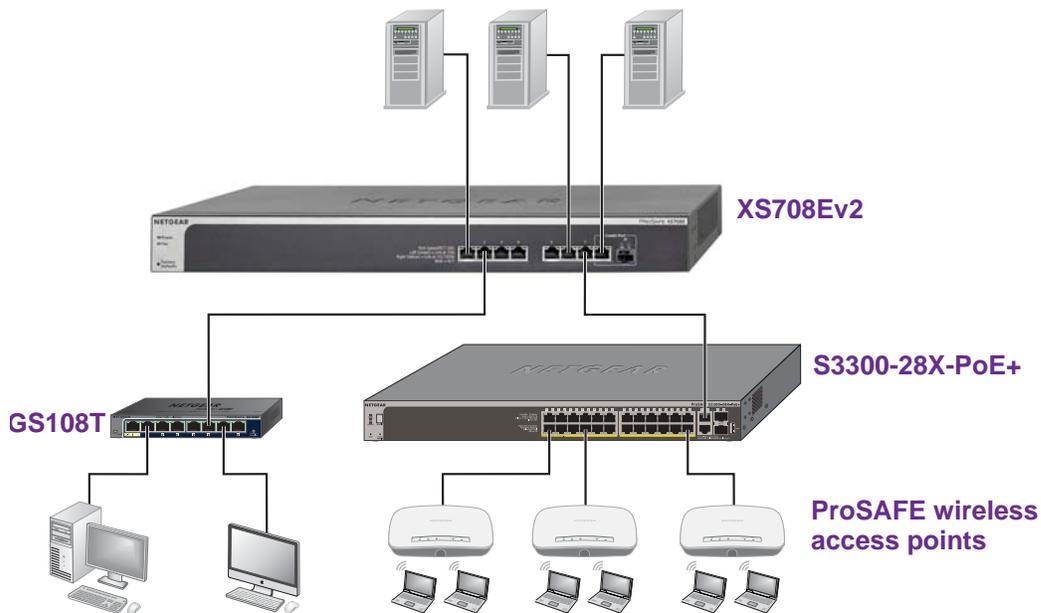
Figure 8. XS708Ev2 backbone switching configuration

Note: Use Category 5e (Cat 5e) or higher rated Ethernet cables (Cat 6, Cat 6a, or Cat 7) to make 10G connections. For 10G speeds, if the cable distance is greater than 148 feet (45 meters), we recommend that you use a Cat 6a cable or higher rated cable.

Connect equipment to model XS716E
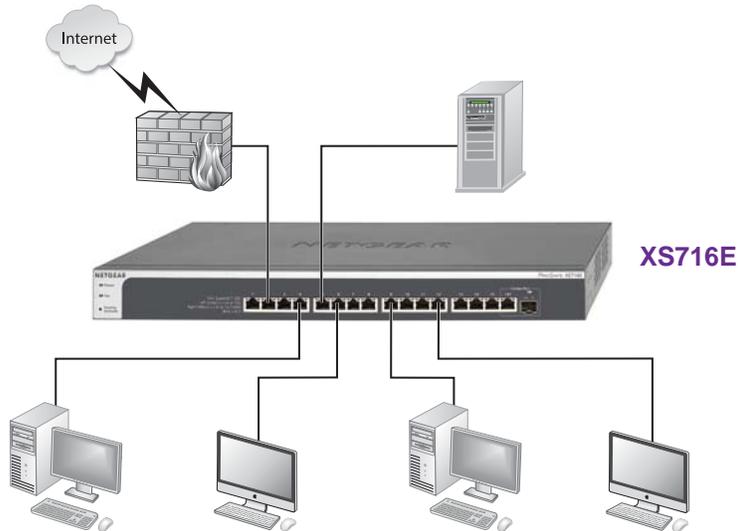
Figure 9. XS716E desktop switching configuration
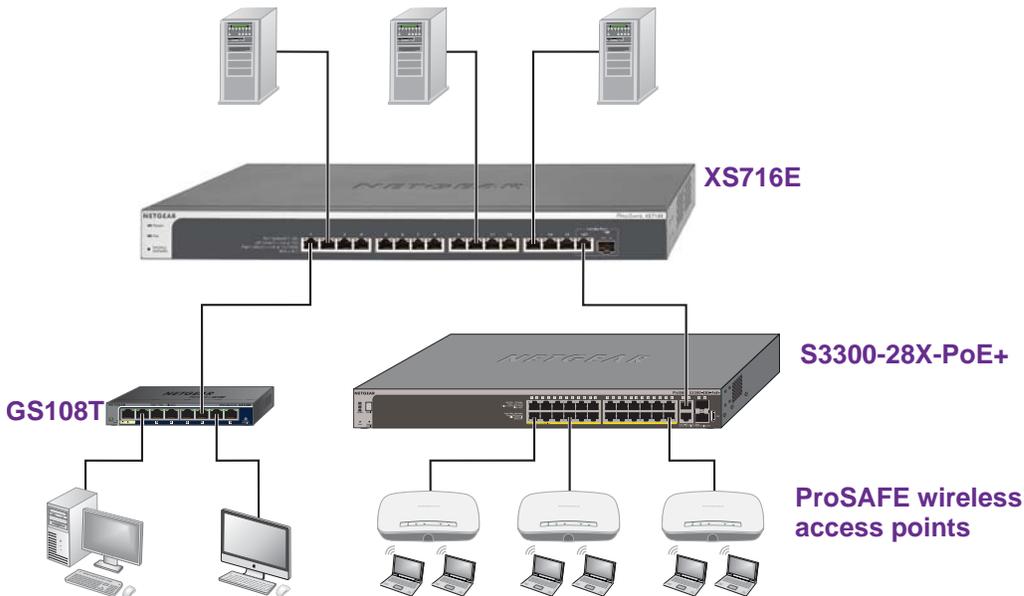
Figure 10. XS716E backbone switching configuration

Note: Use Category 5e (Cat 5e) or higher rated Ethernet cables (Cat 6, Cat 6a, or Cat 7) to make 10G connections. For 10G speeds, if the cable distance is greater than 148 feet (45 meters), we recommend that you use a Cat 6a cable or higher rated cable.

Check the switch status using the LEDs

After you connect power to the switch and the switch starts, LEDs on the front of the switch indicate the status of the switch. When the switch is powered on, the Power LED lights solid green.

The following table describes the RJ-45 and SFP+ slot LED designations. Each RJ-45 port provides a left LED and a right LED. The SFP+ slot provides two LEDs.

Table 1. Port and system LEDs

LED	Designation
Power	• **Solid green**. The device is powered on. • **Off**. Power is not supplied to the device.
Fan	• **Solid yellow**. A fan failure occurred. • **Off**. The fan is operating normally.
Speed and ACT LEDs for copper ports XS708Ev2: ports 1 to 7 and 8T XS716E: ports 1 to 15 and 16T	• **Off**. No link is established. • **Solid green (left LED)**. A valid 10 Gbps link is established. • **Blinking green (left LED)**. The port is transmitting or receiving packets at 10 Gbps. • **Solid yellow (right LED)**. A valid 100/1000 Mbps link is established. • **Blinking yellow (right LED)**. The port is transmitting or receiving traffic at 100/1000 Mbps.
Link and ACT LEDs for SFP+ XS708Ev2: slot 8F XS716E: slot 16F	**10G LED**: • **Off**. No SFP+ module is inserted or no module link is established. • **Solid**. A valid 10 Gbps link is established. • **Blinking**. The module is transmitting or receiving packets at 10 Gbps. **1G LED**: • **Off**. No SFP or SFP+ module is inserted or no module link is established. • **Solid**. A valid 1 Gbps link is established. • **Blinking**. The module is transmitting or receiving packets at 1 Gbps.

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 (0–50°C or 32–122°F) and humidity-controlled (90 percent maximum relative humidity, noncondensing) environment.

  Any device that is located outdoors and connected to this product must be properly grounded and surge protected.

  To the extent permissible by applicable law, failure to follow these guidelines can result in damage to your NETGEAR product, which might not be covered by NETGEAR's warranty.

- Observe and follow service markings:
  - Do not service any product except as explained in your system documentation.
  - 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:
  - The 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.
- 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, be sure that the voltage selection switch (if provided) on the power supply 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.

- Use only approved power cables. 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.

- 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 and 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 cables or plugs. Consult a licensed electrician or your power company for site modifications.

- Always follow your local and national wiring rules.

2
Getting Started

This chapter covers the following topics:

-
-
-
-
-
-
-
-

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).

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 interface of the switch.

You can also use the NETGEAR Insight app on your smartphone to discover the switch in your network and register it with NETGEAR.

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 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 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). 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 21).
- If you use an iOS or Android smartphone, use the NETGEAR Insight mobile app to detect the IP address (see Use the NETGEAR Insight App to discover and register the switch on page 22).
- 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.

   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, use one of the methods that are described in the introduction of this section.

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 through the local browser interface.

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 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 through the local browser 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.

Access the switch with the ProSAFE Plus Utility

The ProSAFE Plus Configuration 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 and its user manual.

Install the ProSAFE Plus Utility

Note: The ProSAFE Plus Utility requires WinPcap and Adobe Air. If WinPcap and Adobe Air are not detected during 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 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 17.

To 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.

   > **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 switches that it 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 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. When prompted, enter the password.

The default password is **password**.

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 the ProSAFE Plus Switch Utility features, see the *ProSAFE Plus Switch Utility User Guide*. You can access the user guide through links 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

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 Too**l 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 App to discover and register the switch

If the switch is connected to a WiFi router or access point, and the switch is connected to the Internet, the NETGEAR Insight app lets you discover the switch in your network, register the switch with NETGEAR, activate your warranty, and access support.

To use the NETGEAR Insight app to discover the switch in your network and register the switch with NETGEAR:

1. On your iOS or Android mobile device, go to the app store, search for NETGEAR Insight, download the latest version of the app, 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 app.

4. If you did not set up a NETGEAR account, tap **Create NETGEAR Account** and follow the onscreen instructions.

5. Enter the email address and password for your account and tap **LOG IN**.

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

6. Write down the IP address for future use.

7. Tap **+** in the upper-right corner.

8. Either use the camera on your phone to scan the serial number bar code located on the bottom of the switch, or enter the serial number.

9. Tap **Go**.

10. Follow the onscreen instructions to add your switch to a network location.

    The switch is registered and added to your account.

Change the language of the local browser interface

By default, the language is set to Auto. 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 <u>Access the switch using a web browser on page 17</u>.

    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. At the top of the page, select a language from the language menu.

    A confirmation pop-up window opens.

6. Click the **OK** button to confirm.

    The switch restarts and you must log in again.

    The language of the local browser interface is now set to the language that you selected.

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.

Use the local browser interface to change the password

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 <u>Access the switch using a web browser on page 17</u>.

    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.

Use the ProSAFE Plus Utility to change the password

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **System > Maintenance > Change Password**.

   The Change Password page displays.

7. In the **Old Password** field, type the current password for the switch.

8. Type the new password in the **New Password** field and in the **Re-type New Password** field.

9. 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

We recommend that you use the NETGEAR Insight app to register your product (see <u>Use the NETGEAR Insight App to discover and register the switch on page 22</u>).

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.

Note: For you to register the switch, the switch must be connected to the Internet.

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 connection.

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 <u>Access the switch using a web browser on page 17</u>.

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.

   Follow the onscreen process to register your product.

3

Network Settings

This chapter covers the following topics:

- Specify the IP address settings for the switch
- Manage multicast traffic with IGMP snooping
- Set up static link aggregation groups

Note: All configuration pages shown are for illustration purposes only and show the XS708Ev2 product. Model XS716E configuration pages look similar but include additional ports to configure.

Specify the 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 the local browser interface 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 <u>Access the switch using a web browser on page 17</u>.

   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 if available, the 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 a 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 Web Managed switches that it discovers on the local network.

3. Select the switch.

    If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

    You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

    The switch's default password is **password**.

    The Switch Status page displays.

6. Click the **IP Setting** button.

Product Name:	XS708Ev2
Switch Name:	
MAC Address:	DC:EF:09:E1:AE:D7
Firmware Version:	V1.0.0.2
DHCP Mode:	Enable ▼ ☐ Refresh
IP Address:	192.168.100.195
Subnet Mask:	255.255.255.0
Gateway Address:	192.168.100.1
∗ Password:	

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

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

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

8. Enter the IP address, subnet mask, and if available, the gateway address.

9. Enter the switch's password in the **Password** field.

   The switch's default password is **password**.

10. 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.

Use the local browser interface to 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 <u>Access the switch using a web browser on page 17</u>.

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

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

7. (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.

8. (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.

9. Click the **Apply** button.

   Your settings are saved.

Use the ProSAFE Plus Utility to 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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **System > Multicast**.

7. Select the IGMP Snooping Status **Enable** radio button.

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. Click the **APPLY** button.

    Your settings are saved.

Use the local browser interface to 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 Chapter 5, Use VLANS for Traffic Segmentation).

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 17.

   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. Make sure that the IGMP Snooping Status **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 8 or 1 to 16, depending on the switch model.

   - For 802.1Q-based VLANs, you can enter a VLAN ID from 1 to 4094.

8. Click the **Apply** button.

   Your settings are saved.

Use the ProSAFE Plus Utility to 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 <u>Chapter 5, Use VLANS for Traffic Segmentation</u>).

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. Double-click the **ProSAFE Plus Utility** icon.

    The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

    If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

    You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

    The switch's default password is **password**.

    The Switch Status page displays.

6. Select **System > Multicast**.

7. Make sure that the IGMP Snooping Status **Enable** radio button is selected.
8. 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 8 or 1 to 16, depending on the switch model.
    *   For 802.1Q-based VLANs, you can enter a VLAN ID from 1 to 4094.

9. Click the **APPLY** button.

    Your settings are saved.

Set up static link aggregation groups

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 switch supports up to four static LAGs. 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. The switch supports manual static LAGs only.

Use the local browser interface to specify LAG membership and enable LAGs

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 <u>Access the switch using a web browser on page 17</u>.

   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.

   The switch supports four static LAGs.

7. Select the ports for the LAG by selecting the associated check boxes under 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.

Use the ProSAFE Plus Utility to specify LAG membership and enable LAGs

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

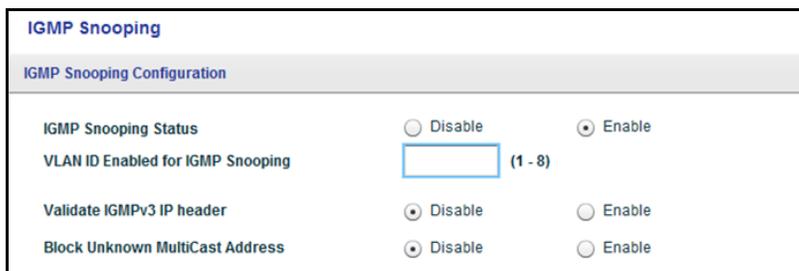4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

The Switch Status page displays.

6. Select **System > LAG > LAG Membership**.

7. In the **LAG ID** menu, select the LAG ID.

The switch supports four static LAGs.

8. Select the ports for the LAG by selecting the associated check boxes under the port numbers.

A LAG consists of at least two ports.

9. Click the **APPLY** button.

Your settings are saved.

10. Select **System > LAG**.

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

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

13. Click the **APPLY** button.

Your settings are saved.

4

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

Note: All configuration pages shown are for illustration purposes only and show the XS708Ev2 product. Model XS716E configuration pages look similar but include additional ports to configure.

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.

Use the local browser interface to enable 802.1p/DSCP-based QoS

This feature is enabled by default.

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 <u>Access the switch using a web browser on page 17</u>.
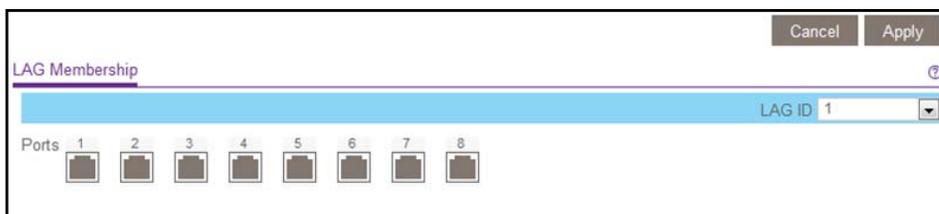
   The login window opens.

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.

Use the ProSAFE Plus Utility to enable 802.1p/DSCP-based QoS

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 connection.

2. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **QoS**.

   The Quality of Service page displays.

7. Select the **802.1p/DSCP Based** radio button.

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

8. Click the **Yes** button.

   The pop-up window closes.

9. Click the **APPLY** button.

   Your settings are saved. Data is now processed based on 802.1p priority tags in the data.

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.

Use the local browser interface to configure port-based QoS

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 17.

   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, go to 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.

      The default setting is **Low Priority(P0)**.

   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 <u>Step 9</u>.

Use the ProSAFE Plus Utility to configure port-based QoS

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

The Switch Status page displays.

6. Select **QoS**.

   The Quality of Service page displays.

7. If this is the first time that you are setting up port-based QoS, select the **Port Based** radio button and continue with Step 8.

   Otherwise, go to Step 9.

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

8. Click the **Yes** button.

   The pop-up window closes and the port priority options display.

9. To set the port priority for one or more ports, do the following:

   a. Select one or more ports.

   b. In the Priority section, select the priority by moving the slider.

      The default setting is **Low Priority(P0)**.

      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.

Use the local browser interface to set up rate limiting

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 <u>Access the switch using a web browser on page 17</u>.

   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 32 to 4096 Mbps. By default, no limit is set.

    c. In the **Egress Rate** menu, select the maximum rate.

    You can set a rate from 32 to 4096 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 <u>Step 6</u>.

Use the ProSAFE Plus Utility to set up rate limiting

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. Double-click the **ProSAFE Plus Utility** icon.

The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

The switch's default password is **password**.

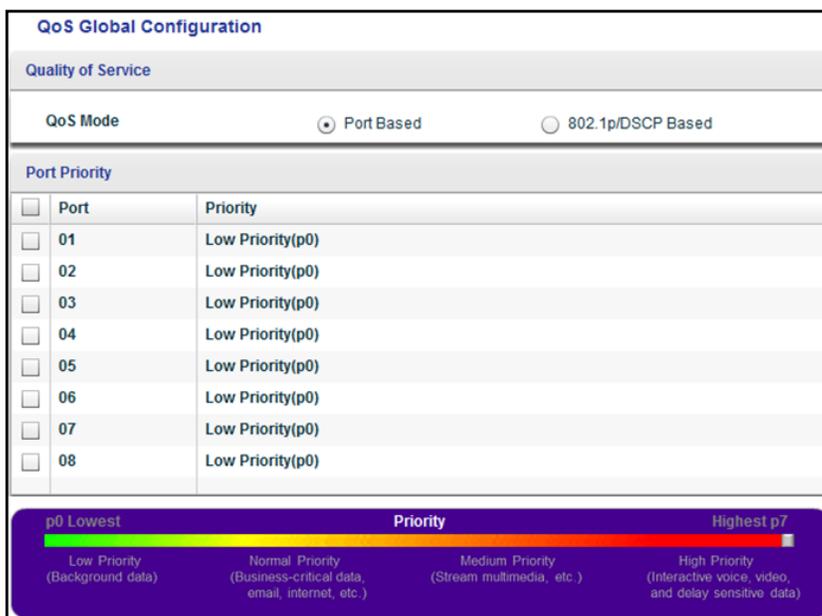The Switch Status page displays.

6. Select **QoS > Rate Limit**.

Port	Ingress Rate	Egress Rate
01	No Limit	No Limit
02	No Limit	No Limit
03	No Limit	No Limit
04	No Limit	No Limit
05	No Limit	No Limit
06	No Limit	No Limit
07	No Limit	No Limit
08	No Limit	No Limit

Rate Limit

Rate Control Setting

Ingress Rate   No Limit

Egress Rate   No Limit

7. Select one or more ports.

8. 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 32 to 4096 Mbit/s. By default, no limit is set.

    c. In the **Egress Rate** menu, select the maximum rate.

       You can set a rate from 32 to 4096 Mbit/s. By default, no limit is set.

    d. Click the **APPLY** button.

       Your settings are saved.

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

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.

Use the local browser interface to set up broadcast filtering

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 17.

   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 <u>Step 7</u>.

   Otherwise, go to <u>Step 8</u>.

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 32 to 4096 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 <u>Step 8</u>.

Use the ProSAFE Plus Utility to set up broadcast filtering

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **QoS > Broadcast Filtering**.

   The Broadcast Filtering page displays.

7. If this is the first time that you are setting up broadcast filtering, select the **Enable** radio button and continue with Step 8.

   Otherwise, go to Step 9.

8. Click the **Apply** button.

   Your settings are saved and the Storm control rate table displays.

9. 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 32 to 4096 Mbps. By default, no limit is set.
   c. Click the **APPLY** button.

      Your settings are saved.

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

5

Use VLANS for Traffic Segmentation

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

Note: All configuration pages shown are for illustration purposes only and show the XS708Ev2 product. Model XS716E configuration pages look similar but include additional ports to configure.

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 of your local network as well as receiving data from other ports that are not in the VLAN. However, 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 53).

By default, all ports are members of VLAN 1.

Use the local browser interface to create basic port-based VLANs

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 17.

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, go to 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.

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 8 or 1 to 16, depending on the switch model. 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.

Use the ProSAFE Plus Utility to create basic port-based VLANs

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **VLAN**.

   The Basic Port-based VLAN page displays.

7. If this is the first time that you are accessing the Basic Port-based VLAN Configuration page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with Step 8.

   Otherwise, go to Step 9.

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

8. Click the **Yes** button.

   The pop-up window closes and the Basic Port-based VLAN Configuration page displays.

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 8 or 1 to 16, depending on the switch model. 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.

Use the local browser interface to assign ports to multiple port-based VLANs

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 <u>Access the switch using a web browser on page 17</u>.

   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 <u>Step 7</u>.

Otherwise, go to 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 check boxes under 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.

Use the ProSAFE Plus Utility to assign ports to multiple port-based VLANs

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **VLAN > Port Based > Advanced**.

   The Advanced Port-based VLAN page displays.

7. If this is the first time that you are accessing the Advanced Port-based VLAN Configuration page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with Step 8.

   Otherwise, go to Step 9.

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

8. Click the **Yes** button.

   The pop-up window closes and 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 check boxes under 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 59.

Use the local browser interface to create 802.1Q-based VLANs in a basic configuration

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 <u>Access the switch using a web browser on page 17</u>.

   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 <u>Step 7</u>.

   Otherwise, go to <u>Step 9</u>.

   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.

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.

Use the ProSAFE Plus Utility to create 802.1Q-based VLANs in a basic configuration

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **VLAN > 802.1Q**.

   The Basic 802.1Q VLAN Configuration page displays.

7. If this is the first time that you are accessing the Basic 802.1Q VLAN Configuration page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with Step 8.

   Otherwise, go to Step 9.

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

8. Click the **Yes** button.

   The pop-up window closes and the Basic 802.1Q VLAN Identifier table displays.

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.

Use the local browser interface to create 802.1Q-based VLANs in an advanced configuration

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 <u>Access the switch using a web browser on page 17</u>.

   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, go to Step 9.

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

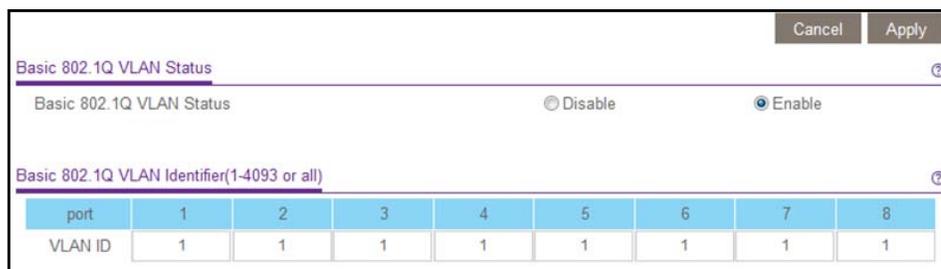**7.** Click the **OK** button.

The pop-up window closes.

8. Click the **Apply** button.

Your settings are saved.

The VLAN Identifier Setting table displays.

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.)

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

Use the ProSAFE Plus Utility to create 802.1Q-based VLANs in an advanced configuration

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. Double-click the **ProSAFE Plus Utility** icon.

    The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

    If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

    You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

    The switch's default password is **password**.

    The Switch Status page displays.

6. Select **VLAN > 802.1Q > Advanced**.

    The Advanced 802.1Q VLAN Configuration page displays.

7. If this is the first time that you are accessing the Advanced 802.1Q VLAN Configuration page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with Step 8.

    Otherwise, go to Step 9.

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

8. Click the **Yes** button.

    The pop-up window closes and the VLAN Identifier Setting table displays.

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 62.)

   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 59), 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.

Use the local browser interface to add tagged or untagged ports to an 802.1Q-based VLAN

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 <u>Access the switch using a web browser on page 17</u>.

   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 <u>Create 802.1Q-based VLANs in an advanced configuration on page 59</u>).
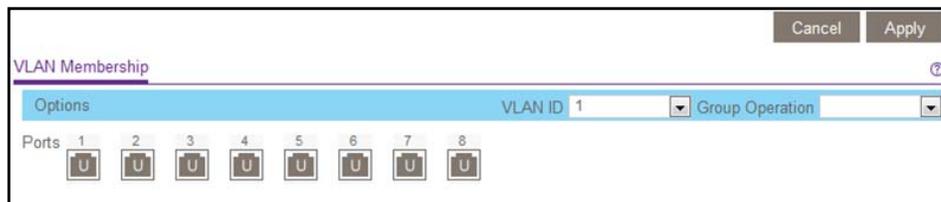
7. In the **VLAN ID** menu, select the VLAN.

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 box under 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 the ProSAFE Plus Utility to add tagged or untagged ports to an 802.1Q-based VLAN

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **VLAN > 802.1Q > Advanced > 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 59).

7. In the **VLAN Identifier** 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 box under 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. 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.

Use the local browser interface to assign a PVID to ports

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 17.

   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 59).

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.

Use the ProSAFE Plus Utility to assign a PVID to ports

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

---

4. Click the **APPLY** button.

    You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

    The switch's default password is **password**.

    The Switch Status page displays.

6. Select **VLAN > 802.1Q > Advanced > 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 59).

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.

6

Manage and Monitor the Switch

This chapter covers the following topics:

- Manage flow control
- Manage the port speed
- Enable loop detection
- Manage Energy Efficient Ethernet and other power saving options
- 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 the port statistics

Note: All configuration pages shown are for illustration purposes only and show the XS708Ev2 product. Model XS716E configuration pages look similar but include additional ports to configure.

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.

Use the local browser interface to manage flow control

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 17.

   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**.

	Port	Port Status	Speed	Linked Speed	Flow Control
	1	Up	Auto	1000M Full	Disable
	2	Down	Auto	No Speed	Disable
	3	Down	Auto	No Speed	Disable
	4	Down	Auto	No Speed	Disable
	5	Down	Auto	No Speed	Disable
	6	Down	Auto	No Speed	Disable
	7	Down	Auto	No Speed	Disable
	8	Down	Auto	No Speed	Disable

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.

Use the ProSAFE Plus Utility to manage flow control

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

Selected Switch

	Product	Switch Name	MAC Address	IP Address	Located on IP Network
⊙	XS708Ev2		dc:ef:09:e1:ae:d7	192.168.100.195	192.168.100.122

Port Status

Port	Port Status	Speed		Linked Speed	Flow Control	
01	Up	Auto	▼	100M	Disable	▼
02	Down	Auto	▼	No Speed	Disable	▼
03	Down	Auto	▼	No Speed	Disable	▼
04	Down	Auto	▼	No Speed	Disable	▼
05	Down	Auto	▼	No Speed	Disable	▼
06	Down	Auto	▼	No Speed	Disable	▼
07	Down	Auto	▼	No Speed	Disable	▼
08	Down	Auto	▼	No Speed	Disable	▼

Note: To navigate to this page, select **Switch > Switch Status**.

6. For each port that you want to configure, in the **Flow Control** menu, select **Enable** or **Disable**.

   By default, flow control is disabled.

7. Click the **APPLY** button.

   Your settings are saved.

Manage the port speed

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.

Use the local browser interface to specify the port speed or shut down a port

To specify the port speed or shut down 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 <u>Access the switch using a web browser on page 17</u>.

   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**.

	Port	Port Status	Speed	Linked Speed	Flow Control
☐					
☐	1	Up	Auto	1000M Full	Disable
☐	2	Down	Auto	No Speed	Disable
☐	3	Down	Auto	No Speed	Disable
☐	4	Down	Auto	No Speed	Disable
☐	5	Down	Auto	No Speed	Disable
☐	6	Down	Auto	No Speed	Disable
☐	7	Down	Auto	No Speed	Disable
☐	8	Down	Auto	No Speed	Disable

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 auto-negotiation with the link partner. This is the default setting.
   - **Disable**. The port is shut down.
   - **100M Full**. The port is forced to function at 100 Mbps with full duplex.

8. To configure more ports, repeat <u>Step 6</u> and <u>Step 7</u>.

9. Click the **Apply** button.

   Your settings are saved.

Use the ProSAFE Plus Utility to specify the port speed or shut down a port

To specify the port speed or shut down 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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

Selected Switch

	Product	Switch Name	MAC Address	IP Address	Located on IP Network
⊙	XS708Ev2		dc:ef:09:e1:ae:d7	192.168.100.195	192.168.100.122

Port Status

Port	Port Status	Speed		Linked Speed	Flow Control	
01	Up	Auto	▼	100M	Disable	▼
02	Down	Auto	▼	No Speed	Disable	▼
03	Down	Auto	▼	No Speed	Disable	▼
04	Down	Auto	▼	No Speed	Disable	▼
05	Down	Auto	▼	No Speed	Disable	▼
06	Down	Auto	▼	No Speed	Disable	▼
07	Down	Auto	▼	No Speed	Disable	▼
08	Down	Auto	▼	No Speed	Disable	▼

Note: To navigate to this page, select **System > Switch Status**.

6. For each port that you want to configure, 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.
   - **100M Full**. The port is forced to function at 100 Mbps with full duplex.
7. Click the **APPLY** button.

   Your settings are saved.

Enable loop detection

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

Use the local browser interface to enable loop detection

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 <u>Access the switch using a web browser on page 17</u>.

   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 Detection**.

   The Loop Detection page displays.
6. Select the **Enable** radio button.
7. Click the **Apply** button.

   Your settings are saved.

Use the ProSAFE Plus Utility to enable loop detection

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **System > Management > Loop Detection**.

   The Loop Detection page displays.

7. Select the **Enable** radio button.

8. Click the **APPLY** button.

   Your settings are saved.

Manage Energy Efficient Ethernet and other power saving options

With the power saving options you can manage the IEEE 802.3az Energy Efficient Ethernet (EEE) function, cable length power saving, and link-up and link-down power saving:

- **EEE**. Combines the Energy Efficient Ethernet (EEE) 802.3 MAC sublayer with the 100BASE-TX, 1000BASE-T, and 10GBASE-T physical layers to support operation in low power idle (LPI) mode. When LPI mode is enabled, systems on both sides of the link can disable portions of their functionality and save power during periods of low link utilization.

  The setting of the administrative mode is either Enable or Disable. The default setting is Disable.

- **Short Cable Power Saving**. Dynamically detects and adjusts power that is required for the detected cable length.

  The setting of the administrative mode is either Enable or Disable. The default setting is Enable.

- **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.

  The setting of the administrative mode is either Enable or Disable. The default setting is Enable.

Note: You can use only the local browser interface to manage the power savings options. You cannot use the ProSAFE Plus Utility to do so.

To use the local browser interface 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 17.

   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**.

6. Enable or disable the power saving options:
   - **EEE**. By default, the **Disable** radio button is selected. To enable EEE, select the **Enable** radio button.
   - **Short Cable Power Saving**. By default, the **Enable** radio button is selected. To disable short power cable saving, select the **Disable** radio button.

- **Link-Down Power Saving**. By default, the **Enable** radio button is selected. To disable link-down power saving, select the **Disable** radio button.

7. Click the **Apply** button.

Your settings are saved.

Upgrade the firmware

You can check for the latest firmware version for your switch. Visit netgear.com/support/download/ and enter in your product model number in the **Enter a Product Name/Model Number** field.

Read the new firmware release notes to find out if you must reconfigure the switch after upgrading. The firmware upgrade method depends on the current firmware and boot loader versions on your switch.

Use the local browser interface to upgrade the firmware

To upgrade the firmware:

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 <u>Access the switch using a web browser on page 17</u>.

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 > Firmware Upgrade**.

The Firmware Upgrade page displays.

6. Click the **Browse** button and locate and select the new firmware image file.

7. 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.

Use the ProSAFE Plus Utility to upgrade the firmware

To upgrade the firmware:

1. Download the new firmware from the NETGEAR support website.

2. 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.

3. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

4. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

5. Click the **APPLY** button.

   You are asked to enter the password for the switch.

6. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

7. If the firmware release notice specifies that you must reconfigure the switch, save the switch configuration settings.

   For more information about how to save the switch configuration, see <u>Save the switch configuration on page 79</u>.

8. Select **System > Maintenance > Firmware Upgrade**.

   The Firmware Upgrade page displays.

9. Click the **BROWSE** button and locate and select the firmware file.

10. 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.

Use the local browser interface to reboot the switch

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 17.

   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.

Use the ProSAFE Plus Utility to reboot the switch

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **System > Maintenance > Device Reboot**.

   The Device Reboot page displays.

7. Select the check box.

8. 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.

Use the local browser interface to save the switch configuration

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 <u>Access the switch using a web browser on page 17</u>.

    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.

Use the ProSAFE Plus Utility to save the switch configuration

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. Double-click the **ProSAFE Plus Utility** icon.

    The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

    If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

    You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

    The switch's default password is **password**.

    The Switch Status page displays.

6. Select **System > Maintenance > Save Configuration**.

    The Save Configuration page displays.

7. Click the **BROWSE** button.

8. Select the location to save the configuration file (a `.cfg` file).

9. Click the **APPLY** button.

   The switch configuration is saved.

Restore a saved switch configuration

You can restore switch configuration that you saved.

Use the local browser interface to restore a saved 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 <u>Access the switch using a web browser on page 17</u>.

   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.

Use the ProSAFE Plus Utility to restore a saved switch configuration

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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **System > Maintenance > Restore Configuration**.

   The Restore Configuration page displays.

7. Click the **BROWSE** button.

8. Find and select the configuration file (a `.cfg` file).

9. Click the **APPLY** button.

   The saved configuration is restored to the switch. The switch reboots to load the restored configuration.

Restore factory default settings

You can return the switch to its factory settings.

Use the local browser interface to restore 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 <u>Access the switch using a web browser on page 17</u>.

    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.

Use the ProSAFE Plus Utility to restore 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. Double-click the **ProSAFE Plus Utility** icon.

    The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

    If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

    You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

    The switch's default password is **password**.

    The Switch Status page displays.

6. Select **System > Maintenance > Factory Default**.

    The Factory Default page displays.

7. Select the check box.

8. 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.

Use the local browser interface to enable port mirroring

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 <u>Access the switch using a web browser on page 17</u>.

   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 > Mirroring**.

6. In the Destination Port section, select the destination port by selecting the check box under the port number.

    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 under 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. Select the Mirror Status **Enable** radio button.

9. Click the **Apply** button.

    Your settings are saved.

Use the ProSAFE Plus Utility to enable port mirroring

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. Double-click the **ProSAFE Plus Utility** icon.

    The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

    If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

    You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

    The switch's default password is **password**.

    The Switch Status page displays.

6. Select **System > Monitoring > Mirroring**.

7. In the Destination Port section, select the destination port by selecting the check box under the port number.

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

8. In the Source Port section, select one or more source ports by selecting the check boxes under the port numbers.

    You can select more than one source port. You cannot select a source port that is a member of a LAG.

9. In the **Mirroring** menu, select **Enable**.

10. 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.

Use the local browser interface to view switch 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 <u>Access the switch using a web browser on page 17</u>.

    The login window opens.

4. Enter the switch's password in the **password** field.

    The switch's default password is **password**.

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

Use the ProSAFE Plus Utility to view switch 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 connection.

2. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **Switch Information**.

Note: To navigate to this page, select **System > Status > Switch Information**.

View the port statistics

For each switch port, you can view the bytes received, bytes sent, and cyclic redundancy check (CRC) error packets.

Use the local browser interface to view and clear the port statistics

To view and 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 <u>Access the switch using a web browser on page 17</u>.

   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.

Use the ProSAFE Plus Utility to view and clear the port statistics

To view and 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. Double-click the **ProSAFE Plus Utility** icon.

   The Switch Selection page displays a list of Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

6. Select **System > Monitoring > Port Statistics**.

Port Statistics			
Port Statistics			
Port	Bytes Received	Bytes Sent	CRC Error Packets
01	24661	5374	0
02	0	0	0
03	0	0	0
04	0	0	0
05	0	0	0
06	0	0	0
07	0	0	0
08	0	0	0

7. To clear the port statistics, click the **CLEAR COUNTERS** button.

   All statistics counters change to 0.

7
Diagnostics and Troubleshooting

This chapter covers the following topics:

- Test cable connections
- Resolve a subnet conflict to access the switch

Note: You can visit the support website at netgear.com/support.

Note: All configuration pages shown are for illustration purposes only and show the XS708Ev2 product. Model XS716E configuration pages look similar but include additional ports to configure.

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 to quickly locate the point where the cabling fails, allowing connectivity issues to be fixed much faster, potentially saving technicians hours of troubleshooting.

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

Use the local browser interface to test a cable connection

To test a cable connection:

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 <u>Access the switch using a web browser on page 17</u>.

    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**.

	Port	Test Results	Cable Fault Distance (meters)
☐	1		
☐	2		
☐	3		
☐	4		
☐	5		
☐	6		
☐	7		
☐	8		
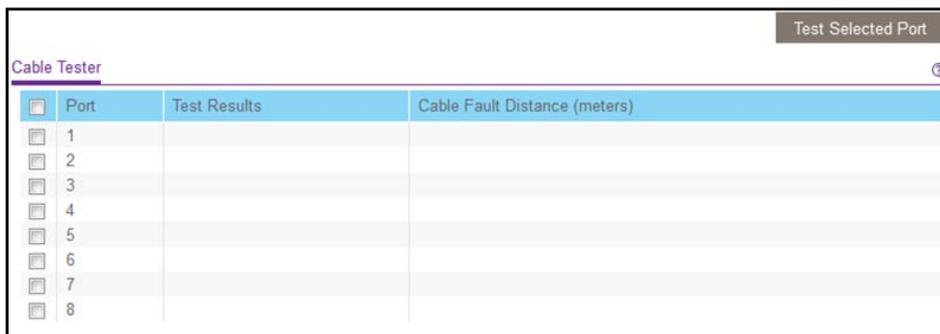
6. Select one or more check boxes.

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.

Use the ProSAFE Plus Utility to test a cable connection

To test a cable connection:

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 Web Managed switches that it discovers on the local network.

3. Select the switch.

   If you do not see the switch, click the **REFRESH** button.

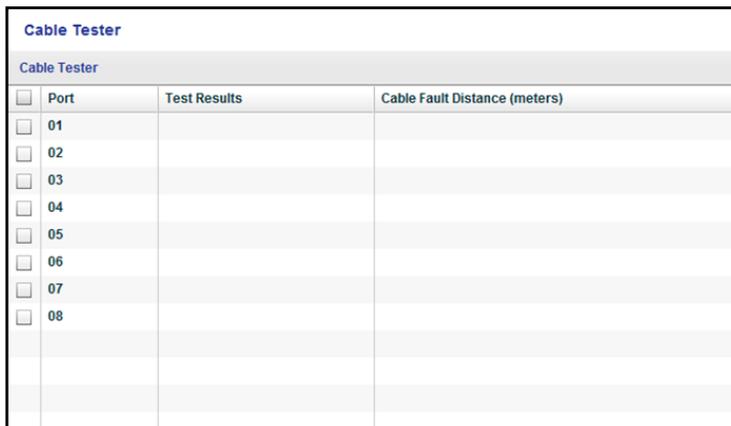4. Click the **APPLY** button.

   You are asked to enter the password for the switch.

5. Enter the switch's password in the **password** field.

   The switch's default password is **password**.

   The Switch Status page displays.

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

Cable Tester		
Cable Tester		
Port	Test Results	Cable Fault Distance (meters)
01		
02		
03		
04		
05		
06		
07		
08		

7. Select one or more check boxes.

8. 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 DCHP server discovers the switch and assigns it an IP address that is in the correct subnet for the network.

A

Supplemental Information

This appendix covers the following topics:

- Factory default settings
- Technical specifications

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 back panel of the switch for at least four seconds. The switch resets and returns to the factory settings that are shown in the following table.

Table 2. 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	Disabled
Port-based QoS	Disabled
Rate limiting	Disabled
Broadcast filtering	Disabled
Loop detection	Disabled
Port speed	Autonegotiation
Flow control	Disabled
Port mirroring	Disabled

Technical specifications

Table 3. Technical specifications

Network Environment	Description	
Network interfaces	RJ-45 connector for 100M/1G/10G copper connections; SFP+ port for 1G/10G fiber connections.	
Network cable	Use Category 5e (Cat 5e) or better terminated with an RJ-45 connector to make 10-Gigabit connections. Cat 6a or Cat 7 cables are recommended for 10-Gigabit cable connections greater than 45 m (148 ft). Use Category 5e (Cat 5e) or higher rated Ethernet cables (Cat 6, Cat 6a, or Cat 7) to make 10G connections. For 10G speeds, if the cable distance is greater than 148 feet (45 meters), we recommend that you use a Cat 6a cable or higher rated cable.	
Operating temperature	0°–50°C (32°–122°F)	
Operating humidity	10%–90% relative humidity, noncondensing	
Electromagnetic approvals	BSMI CE mark (commercial) FCC Part 15 Class A EN 55022 (CISPR 22) Class A VCCI Class A C-Tick KC CCC	
Safety agency approvals	BSMI UL/cUL 60950 CB CCC AS/NZS EN60950 CE LVD	
Model	**XS708Ev2**	**XS716E**
Ports	8	16
Power (maximum)	100–240 VAC, 50–60 Hz, 2A	100–240 VAC 50–60 Hz, 2.5A
Power consumption	43.39W maximum	62.69W maximum
Weight	2.8 kg (6.17 lb)	3.2 kg (7.05 lb)
Dimensions (W X D x H)	440 mm x 204 mm x 43 mm (17.32 in. x 8.03 in. x 1.69 in.)	440 mm x 204 mm x 43 mm (17.32 in. x 8.03 in. x 1.69 in.)