

NETGEAR®

User Manual

48-Port Gigabit Ethernet Plus Switch with 2 SFP Ports

Model GS750E

November 2021
202-11784-04

NETGEAR, Inc.

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

Support and Community

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

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

Regulatory and Legal

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

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

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

See the regulatory compliance document before connecting the power supply.

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

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

Do not use this device outdoors.

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
202-11784-04	November 2021	Removed information about the ProSAFE Plus Utility, which has reached end-of-life. Removed information about the NETGEAR Insight app.
202-11784-03	March 2019	Added Change the language of the device UI on page 12. Changed Add devices to the Access Control table on page 39.

48-Port Gigabit Ethernet Plus Switch with 2 SFP Ports Model GS750E

(Continued)

Publication Part Number	Publish Date	Comments
202-11784-02	October 2018	Added <i>with 2 SFP Ports</i> to the switch name. Revised Configure the switch on page 7. Revised Access a switch that is connected to a network on page 8. Added Use the NETGEAR Switch Discovery Tool to access the switch on page 9. Added Access the switch from a Mac using Bonjour on page 11. Removed references to the resource CD. Made multiple minor changes.
202-11784-01	July 2017	First publication.

Contents

Chapter 1 Get Started

Related documentation.....	7
Configure the switch.....	7
Access the switch using a web browser.....	7
Access a switch that is connected to a network.....	8
Access a switch that is off-network.....	9
Use the NETGEAR Switch Discovery Tool to access the switch.....	9
Access the switch from a Mac using Bonjour.....	11
Change the switch password.....	11
Change the language of the device UI.....	12
Register your product.....	13

Chapter 2 Use VLANs for Traffic Segmentation

VLAN overview.....	16
Create basic port-based VLANs.....	16
Assign ports to multiple port-based VLANs.....	18
Create 802.1Q-based VLANs in a basic configuration.....	19
Create 802.1Q-based VLANs in an advanced configuration.....	21
Add tagged or untagged ports to an 802.1Q-based VLAN.....	23
Specify a port PVID for an 802.1Q-based VLAN.....	24
Manage the voice VLAN.....	26
Specify the voice VLAN properties.....	26
Enable the voice VLAN mode for ports.....	27
Manage the OUI table.....	28

Chapter 3 Optimize Performance With Quality of Service

Enable 802.1p/DSCP-based quality of service.....	32
Configure port-based quality of service.....	33
Set up rate limiting.....	34
Set up broadcast filtering.....	35

Chapter 4 Manage Security

Manage access control.....	39
Add devices to the Access Control table.....	39
Remove devices from the Access Control table.....	40
Set the switch management mode.....	41

Disable Bonjour for discovery.....	42
Manage automatic denial of service.....	43

Chapter 5 Manage Network Settings

Specify IP address settings for the switch.....	46
Use browser-based access to specify the switch IP address.....	46
Manage multicast traffic with IGMP snooping.....	47
Customize IGMP snooping.....	48
Specify a VLAN for IGMP snooping.....	49
Enable the Auto-Video configuration.....	50
Set up link aggregation.....	51
Set up a static link aggregation group.....	52
Set up a Link Aggregation Control Protocol group.....	53
Set up the LACP system priority for the switch.....	55
Set Up LACP port priority and time-out values.....	55

Chapter 6 Manage and Monitor the Switch

Manage flow control.....	59
Manage the port speed and the port status.....	60
Enable loop prevention.....	61
Manage power saving options.....	62
Manually download and upgrade the firmware.....	63
Reboot the switch.....	64
Save the switch configuration.....	65
Restore a saved switch configuration.....	66
Restore factory default settings.....	66
Enable port mirroring.....	67
View switch information or change the switch device name.....	69
View or clear the port statistics.....	70

Chapter 7 Diagnostics and Troubleshooting

Test cable connections.....	73
Resolve a subnet conflict to access the switch.....	74

Appendix A Factory Default Settings

1

Get Started

This user manual is for the NETGEAR 48-Port Gigabit Ethernet Plus Switch with 2 SFP Ports, model GS750E.

This chapter covers the following topics:

- [Related documentation](#)
- [Configure the switch](#)
- [Access the switch using a web browser](#)
- [Use the NETGEAR Switch Discovery Tool to access the switch](#)
- [Access the switch from a Mac using Bonjour](#)
- [Change the switch password](#)
- [Change the language of the device UI](#)
- [Register your product](#)

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

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

Related documentation

The following related documentation is available at netgear.com/support/download/:

- Installation guide
- Hardware installation guide
- Data sheet

Configure the switch

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

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

You can configure and manage advanced features of the switch by using your computer's web browser and accessing the switch at its IP address.

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

If your Mac supports Bonjour, you can use Bonjour to discover the switch in your network and access the local browser interface of the switch.

For more information, see the following sections:

- [Access the switch using a web browser](#) on page 7
- [Use the NETGEAR Switch Discovery Tool to access the switch](#) on page 9
- [Access the switch from a Mac using Bonjour](#) on page 11

Access the switch using a web browser

This manual describes how to use the local browser-based management interface, referred to as the device UI.

You can access and configure the switch directly through its device UI by entering the IP address of the switch in the address bar of a browser. When you access the device UI to configure the switch, it's simpler if the switch is not connected to your network

(off-network). You can also configure the switch with it connected to your network, router, or modem, (on-network) but you must be able to determine the IP address of the switch if your network uses DHCP.

Access a switch that is connected to a network

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

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

- If you use a 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 9).
- If you use a Mac that supports Bonjour, use Bonjour to detect the IP address (see [Access the switch from a Mac using Bonjour](#) on page 11).
- Access the DHCP server.
- Use an IP scanner utility.

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

1. Cable the switch to a network with a router or DHCP server that manages IP addresses.
2. Power on the switch.
The DHCP server assigns the switch an IP address.
3. Connect your computer to the same network as the switch.
4. Determine the IP address of the switch.
By default, the DHCP client of the switch is enabled. Use the IP address that the DHCP server assigned to the switch.
5. Open a web browser, and enter the IP address of the switch.
The login page displays.
6. Enter the device admin password.
Use the default password printed on the device label the first time you log in, and then you must set a new device password. The password is case-sensitive.
7. Click the **Login** button.
You can now configure additional options for the switch through the device UI.
For information about setting up a fixed (static) IP address for the switch, see [Specify IP address settings for the switch](#) on page 46.

Access a switch that is off-network

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

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

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

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

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

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

This is the default address of the switch.

The login page displays.

4. Enter the switch password.

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

5. Click the **Login** button.

You can now configure additional options for the switch through the device UI.

For information about setting up a fixed (static) IP address for the switch, see [Specify IP address settings for the switch](#) on page 46.

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.

Use the NETGEAR Switch Discovery Tool to access the switch

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

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

To install the NETGEAR Switch Discovery Tool, discover the switch in your network, and access the device UI of the switch:

1. Download the Switch Discovery Tool by visiting netgear.com/support/product/netgear-switch-discovery-tool.aspx.
Depending on the computer that you are using, download either the Mac version or the version for a 64-bit Windows-based computer.
2. Temporarily disable the firewall, Internet security, antivirus programs, or all of these on the computer that you use to configure the switch.
3. Unzip the Switch Discovery Tool files, double-click the **.exe** or **.dmg** file (for example, `NETGEAR+Switch+Discovery+Tool+Setup+1.2.101.exe` or `NetgearSDT-V1.2.101.dmg`), and install the program on your computer.
The installation process places a **NETGEAR Switch Discovery Tool** icon on your desktop.
4. Reenable the security services on your computer.
5. Power on the switch.
The DHCP server assigns the switch an IP address.
6. Connect your computer to the same network as the switch.
You can use a WiFi or wired connection. The computer and the switch must be on the same Layer 2 network.
7. Open the Switch Discovery Tool.
To open the program, double-click the **NETGEAR Switch Discovery Tool** icon on your desktop.
The initial page displays a menu and a button.
8. From the **Choose a connection** menu, select the network connection that allows the Switch Discovery Tool to access the switch.
9. Click the **Start Searching** button.
The Switch Discovery Tool displays a list of NETGEAR switches that it discovers on the selected network.
For each switch, the tool displays the IP address.
10. To access the device UI of the switch, click the **ADMIN PAGE** button.
The login page of the device UI opens.
11. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.

Access the switch from a Mac using Bonjour

If your Mac supports Bonjour, you can use the following procedure. If your Mac does not support Bonjour, see [Use the NETGEAR Switch Discovery Tool to access the switch](#) on page 9.

To access the switch from a Mac using Bonjour and discover the switch IP address:

1. Open the Safari browser.
2. Select **Safari > Preferences**.
The General page displays.
3. Click the **Advanced** tab.
The Advanced page displays.
4. Select the **Include Bonjour in the Bookmarks Menu** check box.
5. Close the Advanced page.
6. Depending on your Mac OS version, select one of the following, in which xx:xx:xx:xx:xx:xx is the MAC address of the switch:
 - **Bookmarks > Bonjour > GS750E (xx:xx:xx:xx:xx:xx)**
 - **Bookmarks > Bonjour > Webpages GS750E (xx:xx:xx:xx:xx:xx)**

The login page of the local browser interface opens.

7. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays. The page shows the IP address that is assigned to the switch.

Change the switch password

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

To change the password:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **Maintenance > Change Password**.
The Change Password page displays.
6. In the **Old Password** field, type the current password for the switch.
7. Type the new password in the **New Password** field and in the **Re-type New Password** field.
8. Click the **Apply** button.
Your settings are saved. Keep the new password in a secure location so that you can access the switch in the future.

Change the language of the device UI

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

To change the language of the device UI:

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 7.

The login window opens.

4. Enter the switch password.

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

The Switch Information page displays.

5. From the language menu at the top right of the page, select a language.

By default, the selection from the menu is **Auto**.

A pop-up warning window opens.

6. Click the **YES** button.

Your settings are saved and the language changes.

Register your product

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

To register your product through the device UI:

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

You can use a WiFi or wired network connection.

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

2. Launch a web browser.

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

If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.

The login page displays.

4. Enter the switch password.

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

The Switch Information page displays.

5. Select **Help > Registration**.

The Product Registration page displays.

6. Click the **Register** button.

7. Follow the onscreen process to register your product.

2

Use VLANS for Traffic Segmentation

This chapter covers the following topics:

- [VLAN overview](#)
- [Create basic port-based VLANs](#)
- [Assign ports to multiple port-based VLANs](#)
- [Create 802.1Q-based VLANs in a basic configuration](#)
- [Create 802.1Q-based VLANs in an advanced configuration](#)
- [Add tagged or untagged ports to an 802.1Q-based VLAN](#)
- [Specify a port PVID for an 802.1Q-based VLAN](#)
- [Manage the voice VLAN](#)

VLAN overview

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

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

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

Create basic port-based VLANs

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

You can also assign ports to multiple VLANs (see [Assign ports to multiple port-based VLANs](#) on page 18).

By default, all ports are members of VLAN 1.

To create basic port-based VLANs:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.

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

The Switch Information page displays.

5. Select **VLAN**.

The Basic Port-based VLAN Status page displays.

6. If this is the first time that you are accessing this page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with [Step 7](#).

Otherwise, see [Step 9](#).

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

7. Click the **OK** button.

The pop-up window closes.

8. Click the **Apply** button.

Your settings are saved.

The Basic Port-based VLAN Group table displays.

Basic Port-based VLAN Status

Basic Port-based VLAN Status

☐ Disable ☒ Enable

Basic Port-based VLAN Group(1-50 or all)

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

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

You can enter a VLAN ID from 1 to the maximum number of ports that your switch supports. If all the VLANs share an uplink to the Internet or servers, enter **all** in the **VLAN ID** field for the port that you want to use for the uplink.

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

10. Click the **Apply** button.

Your settings are saved.

Assign ports to multiple port-based VLANs

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

By default, all ports are members of VLAN 1.

To assign ports to multiple port-based VLANs:

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

The VLAN Configuration and VLAN Membership sections display.

Advanced Port-based VLAN Status

Advanced Port-based VLAN Status ☐ Disable ☒ Enable

VLAN Configuration

VLAN Identifier Group Operation

Ports	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

VLAN Membership

VLAN ID	Port Members
1	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

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

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

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

Create 802.1Q-based VLANs in a basic configuration

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

In an advanced 802.1Q-based VLAN configuration, you can set up VLANs to which you can add tagged or untagged ports and you can use port VLAN ID (PVID). For more information, [Create 802.1Q-based VLANs in an advanced configuration](#) on page 21.

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

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **VLAN > 802.1Q**.
The Basic 802.1Q VLAN Status page displays.
6. If this is the first time that you are accessing the Basic 802.1Q VLAN Status page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with [Step 7](#).
Otherwise, see [Step 9](#).
A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **OK** button.
The pop-up window closes.
8. Click the **Apply** button.
Your settings are saved.

The Basic 802.1Q VLAN Identifier table displays.

Basic 802.1Q VLAN Status

Basic 802.1Q VLAN Status ☐ Disable ☒ Enable

Basic 802.1Q VLAN Identifier(1-4093 or all)

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

- Under each port to be added to a VLAN, enter the ID of the VLAN.

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

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

- Click the **Apply** button.

Your settings are saved.

Create 802.1Q-based VLANs in an advanced configuration

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

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

- 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.
- 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 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **VLAN > 802.1Q > Advanced > VLAN Configuration**.
The Advanced 802.1Q VLAN Status page displays.
6. If this is the first time that you are accessing the Advanced 802.1Q VLAN Status page or if you are changing the VLAN assignment method, select the **Enable** radio button and continue with [Step 7](#).
Otherwise, see [Step 9](#).
A pop-up window opens, informing you that the current VLAN settings will be lost.
7. Click the **OK** button.
The pop-up window closes.
8. Click the **Apply** button.
Your settings are saved.
The VLAN Identifier Setting table displays.

Advanced 802.1Q VLAN Status

Advanced 802.1Q VLAN Status ☐ Disable ☒ Enable

VLAN Identifier Setting

VLAN ID	Port Members
1	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50
2	
3	

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 23.)

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 21), you must add ports to the VLAN.

While you add ports to a VLAN, you can specify whether the ports must be tagged or untagged. Port tagging allows a port to be associated with a particular VLAN and allows the VLAN ID tag to be added to data packets that are sent through the port. The tag identifies the VLAN that must receive the data.

By default, all ports are untagged.

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

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **VLAN > 802.1Q > Advanced > VLAN Configuration**.
The Advanced 802.1Q VLAN Status page displays. The menu on the left displays more options.
6. Select **VLAN Membership**.

You can select **VLAN Membership** only if you already enabled the advanced 802.1Q VLAN option (see [Create 802.1Q-based VLANs in an advanced configuration](#) on page 21).

VLAN Membership

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

Specify a port PVID for an 802.1Q-based VLAN

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

To assign a PVID to one or more ports:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **VLAN > 802.1Q > Advanced > VLAN Configuration**.
The Advanced 802.1Q VLAN Status page displays. The menu on the left displays more options.
6. Select **Port PVID**.
You can select **Port PVID** only if you already enabled the advanced 802.1Q VLAN option (see [Create 802.1Q-based VLANs in an advanced configuration](#) on page 21).

PVID Configuration

<input type="checkbox"/>	Port	PVID
<input type="checkbox"/>	g1	1
<input type="checkbox"/>	g2	1
<input type="checkbox"/>	g3	1
<input type="checkbox"/>	g4	1
<input type="checkbox"/>	g5	1
<input type="checkbox"/>	g6	1
<input type="checkbox"/>	g7	1
<input type="checkbox"/>	g8	1
<input type="checkbox"/>	g9	1
<input type="checkbox"/>	g10	1
<input type="checkbox"/>	g11	1
<input type="checkbox"/>	g12	1
<input type="checkbox"/>	g13	1
<input type="checkbox"/>	g14	1
<input type="checkbox"/>	g15	1
<input type="checkbox"/>	g16	1

7. Select one or more ports.

8. Enter the PVID.

You can enter a PVID only for a VLAN that already exists.

9. Click the **Apply** button.

Your settings are saved.

Manage the voice VLAN

The switch supports a voice VLAN to facilitate voice over IP (VoIP) traffic.

If you enable the 802.1Q VLAN mode (see [Create 802.1Q-based VLANs in a basic configuration](#) on page 19 or [Create 802.1Q-based VLANs in an advanced configuration](#) on page 21), the voice VLAN is enabled by default. The default ID of the voice VLAN is 2, which you can change.

For more information, see the following sections:

- [Specify the voice VLAN properties](#) on page 26
- [Enable the voice VLAN mode for ports](#) on page 27
- [Manage the OUI table](#) on page 28

Specify the voice VLAN properties

By default, the voice VLAN is enabled. The default ID of the voice VLAN is ID 2. The default Class of Service (CoS) value is 6. You can change the voice VLAN properties only if you enable the 802.1Q VLAN mode (see [Create 802.1Q-based VLANs in a basic configuration](#) on page 19 or [Create 802.1Q-based VLANs in an advanced configuration](#) on page 21).

The voice VLAN can be effective only if you enable the voice VLAN mode for individual interfaces (see [Enable the voice VLAN mode for ports](#) on page 27). The voice VLAN properties apply to all traffic on the voice VLAN.

To specify the voice VLAN properties:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.

The login page displays.

4. Enter the switch password.

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

The Switch Information page displays.

5. Select **VLAN > Voice VLAN > Properties**.

The Voice VLAN Properties page displays.

6. In the **Voice VLAN ID** menu, select the voice VLAN ID.

You can select either one of the default VLAN IDs (1, 2, or 3) or a VLAN ID that you manually added (see [Create 802.1Q-based VLANs in a basic configuration](#) on page 19 or [Create 802.1Q-based VLANs in an advanced configuration](#) on page 21). The default voice VLAN ID is 2.

7. In the **Class of Service** menu, select the class value for the voice VLAN.

You can select a value from 0 (the lowest priority) to 7 (the highest priority). The default CoS value is 6.

8. Click the **Apply** button.

Your settings are saved.

Enable the voice VLAN mode for ports

You can enable the voice VLAN mode for individual ports so that these ports become members of the voice VLAN. By default, the voice VLAN mode is disabled for all ports.

To enable the voice VLAN mode for one or more ports:

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

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

2. Launch a web browser.

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

If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.

The login page displays.

4. Enter the switch password.

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

The Switch Information page displays.

5. Select **VLAN > Voice VLAN > Port Settings**.

OUI Port Settings

<input type="checkbox"/>	Interface	Voice VLAN Mode
		- ▾
<input type="checkbox"/>	g1	Disable
<input type="checkbox"/>	g2	Disable
<input type="checkbox"/>	g3	Disable
<input type="checkbox"/>	g4	Disable
<input type="checkbox"/>	g5	Disable
<input type="checkbox"/>	g6	Disable
<input type="checkbox"/>	g7	Disable
<input type="checkbox"/>	g8	Disable
<input type="checkbox"/>	g9	Disable
<input type="checkbox"/>	g10	Disable
<input type="checkbox"/>	g11	Disable
<input type="checkbox"/>	g12	Disable
<input type="checkbox"/>	g13	Disable
<input type="checkbox"/>	g14	Disable
<input type="checkbox"/>	g15	Disable
<input type="checkbox"/>	g16	Disable

6. Select one or more ports.
7. In the **Voice VLAN Mode** menu, select **Enable**.
By default, the voice VLAN mode is disabled for all ports.
8. Click the **Apply** button.
Your settings are saved.

Manage the OUI table

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

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

To manage the OUI table:

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

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.

The login page displays.

4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **VLAN > Voice VLAN > OUI Table**.

OUI Table

<input type="checkbox"/>	Telephony (OUIs)	Description
	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	00:01:E3	SIEMENS
<input type="checkbox"/>	00:03:6B	CISCO1
<input type="checkbox"/>	00:04:0D	AVAYA1
<input type="checkbox"/>	00:0F:E2	H3C
<input type="checkbox"/>	00:12:43	CISCO2
<input type="checkbox"/>	00:1B:4F	AVAYA2
<input type="checkbox"/>	00:60:B9	NITSUKO
<input type="checkbox"/>	00:D0:1E	PINTEL
<input type="checkbox"/>	00:E0:75	VERILINK
<input type="checkbox"/>	00:E0:BB	3COM

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

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

3

Optimize Performance With Quality of Service

This chapter covers the following topics:

- [Enable 802.1p/DSCP-based quality of service](#)
- [Configure port-based quality of service](#)
- [Set up rate limiting](#)
- [Set up broadcast filtering](#)

Enable 802.1p/DSCP-based quality of service

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

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

To enable 802.1p/DSCP-based QoS:

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

Configure port-based quality of service

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

To configure port-based QoS:

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

Your settings are saved and the Port Priority table displays.

Quality of Service

QoS Mode

☒ Port Based ☐ 802.1p/DSCP Based

Port Priority

<input type="checkbox"/>	Port	Priority
		- <input type="text"/>
<input type="checkbox"/>	g1	Low Priority (P0)
<input type="checkbox"/>	g2	Low Priority (P0)
<input type="checkbox"/>	g3	Low Priority (P0)
<input type="checkbox"/>	g4	Low Priority (P0)
<input type="checkbox"/>	g5	Low Priority (P0)
<input type="checkbox"/>	g6	Low Priority (P0)
<input type="checkbox"/>	g7	Low Priority (P0)
<input type="checkbox"/>	g8	Low Priority (P0)
<input type="checkbox"/>	g9	Low Priority (P0)
<input type="checkbox"/>	g10	Low Priority (P0)
<input type="checkbox"/>	g11	Low Priority (P0)
<input type="checkbox"/>	g12	Low Priority (P0)

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

Set up rate limiting

You can limit the rate at which the switch accepts incoming data and the rate that it retransmits outgoing data.

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

To set up rate limiting:

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

If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.

The login page displays.

4. Enter the switch password.

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

The Switch Information page displays.

5. Select **QoS > Rate Limit**.

Rate Control Setting

<input type="checkbox"/>	Port	Ingress Rate	Egress Rate
		-	-
<input type="checkbox"/>	g1	No Limit	No Limit
<input type="checkbox"/>	g2	No Limit	No Limit
<input type="checkbox"/>	g3	No Limit	No Limit
<input type="checkbox"/>	g4	No Limit	No Limit
<input type="checkbox"/>	g5	No Limit	No Limit
<input type="checkbox"/>	g6	No Limit	No Limit
<input type="checkbox"/>	g7	No Limit	No Limit
<input type="checkbox"/>	g8	No Limit	No Limit
<input type="checkbox"/>	g9	No Limit	No Limit
<input type="checkbox"/>	g10	No Limit	No Limit
<input type="checkbox"/>	g11	No Limit	No Limit
<input type="checkbox"/>	g12	No Limit	No Limit

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

Set up broadcast filtering

You can configure the switch to block broadcast storms (massive transmission of broadcast packets forwarded to every port on the same VLAN). If they are not blocked, broadcast storms 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 packets.

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 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **QoS > Broadcast Filtering**.
The Broadcast Filtering page displays.
6. If this is the first time that you are setting up broadcast filtering, select the **Enable** radio button and continue with the next step.
Otherwise, see [Step 8](#).
7. Click the **Apply** button.

Your settings are saved and the Storm Control Rate table displays.

Broadcast Filtering

Broadcast Filtering

☐ Disable ☒ Enable

Storm Control Rate

<input type="checkbox"/>	Port	Storm Control Rate
		-
<input type="checkbox"/>	g1	No Limit
<input type="checkbox"/>	g2	No Limit
<input type="checkbox"/>	g3	No Limit
<input type="checkbox"/>	g4	No Limit
<input type="checkbox"/>	g5	No Limit
<input type="checkbox"/>	g6	No Limit
<input type="checkbox"/>	g7	No Limit
<input type="checkbox"/>	g8	No Limit
<input type="checkbox"/>	g9	No Limit
<input type="checkbox"/>	g10	No Limit
<input type="checkbox"/>	g11	No Limit
<input type="checkbox"/>	g12	No Limit

8. Set the storm control rate by doing the following:
 - a. Select one or more ports.
 - b. In the **Storm Control Rate** menu, select the maximum rate.
You can set a rate from 512 Kbit/s to 512 Mbit/s. By default, no limit is set.
 - c. Click the **Apply** button.
Your settings are saved.
9. To set a different rate for one or more other ports, repeat [Step 8](#).

4

Manage Security

This chapter covers the following topics:

- Manage access control
- Set the switch management mode
- Disable Bonjour for discovery
- Manage automatic denial of service

Manage access control

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

For more information, see the following sections:

- [Add devices to the Access Control table](#) on page 39
- [Remove devices from the Access Control table](#) on page 40

Add devices to the Access Control table

If you add devices to the Access Control table, use the mask to allow one IP address or a range of IP addresses to access the local browser interface of the switch. Consider the following examples:

- If the mask is 255.255.255.255, only the device for which you specify the host IP address in the Source IP Address field can access the local browser interface.
- If the host IP address in the Source IP Address field is 192.168.100.x (in which x can be any number from 0 to 255) and the mask is 255.255.255.0, any device in the range from 192.168.100.0 to 192.168.100.255 can access the local browser interface.
- If the host IP address in the Source IP Address field is 192.168.100.y (in which y can be any number from 0 to 7) and the mask is 255.255.255.248, any device in the range from 192.168.100.0 to 192.168.100.7 can access the local browser interface.


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

To add devices to the Access Control table:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.

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

Access Control

 Source IP Address	Mask
<input type="text"/>	<input type="text"/>

6. For a device or range of devices that must be able to access the switch, configure the following settings:
 - **Source IP Address.** Enter the IP address of the device or range of devices that must be allowed to access the switch over a web browser.
 - **Mask.** Enter the subnet mask that is associated with the IP address.
7. Click the **Add** button.
The device or range of devices is added to the table and your settings are saved.
Access control is now enabled.
8. Repeat [Step 6](#) and [Step 7](#) for each device or range of devices that you want to add to the Access Control table.

Remove devices from the Access Control table

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

To remove devices from the Access Control table:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.

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

The Switch Information page displays.

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

Access Control

<input type="checkbox"/>	Source IP Address	Mask
	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	192.168.100.0	255.255.255.0
<input type="checkbox"/>	203.0.113.126	255.255.255.255

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

Set the switch management mode

Note: The ProSAFE Plus Utility has reached end-of-life and is no longer supported.

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

To set the switch management mode:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.

4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > Management > Switch Management Mode**.
The Switch Management Mode page displays.
6. Select one of the following radio buttons:
 - **Web browser Only**. You can configure the switch through the local browser interface only.
 - **Web browser GUI and ProSAFE Utility**. You can configure the switch through the local browser interface or through the ProSAFE Plus Utility. This is the default setting. However, the ProSAFE Plus Utility has reached end-of-life and is no longer supported.
7. Click the **Apply** button.
Your settings are saved.

Disable Bonjour for discovery

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

To disable Bonjour on the switch:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.

5. Select **System > Management > Switch Management Mode**.

The Switch Management Mode page displays.

6. Select the **Disable** radio button.

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

7. Click the **Apply** button.

Your settings are saved.

Manage automatic denial of service

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

The TCP and UDP ports are always enabled, but you can shut down individual ports (see [Manage the port speed and the port status](#) on page 60).

To manage the Auto DoS prevention mode:

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

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

2. Launch a web browser.

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

If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.

The login page displays.

4. Enter the switch password.

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

The Switch Information page displays.

5. Select **System > Management > Denial of Service**.

The Auto-DoS Configuration page displays.

6. Select one of the following radio buttons:

- **Enable**. Enables the Auto DoS prevention mode.
- **Disable**. Disables the Auto DoS prevention mode.

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

5

Manage Network Settings

This chapter covers the following topics:

- Specify IP address settings for the switch
- Use browser-based access to specify the switch IP address
- Manage multicast traffic with IGMP snooping
- Set up link aggregation

Specify IP address settings for the switch

By default, the switch IP address works as follows:

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

Use browser-based access to specify the switch IP address

To specify IP address settings for the switch:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.

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

Switch Information

Product Name	GS750E
Switch Name	<input type="text" value="Plus Switch GS750E"/>
Serial Number	526174DPF00B5
MAC Address	40:5D:82:45:C0:74
Firmware Version	1.0.0.19
DHCP Mode	<input type="text" value="Disable"/> <input type="checkbox"/> Refresh
IP Address	<input type="text" value="192.168.100.112"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway Address	<input type="text" value="192.168.100.1"/>

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

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

Manage multicast traffic with IGMP snooping

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

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

Customize IGMP snooping

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

To customize IGMP snooping:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > Multicast**.

IGMP Snooping Configuration

IGMP Snooping Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
VLAN ID Enabled for IGMP Snooping	<input type="text" value="1"/> (1 to 4094)
Validate IGMPv3 IP header	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Block Unknown Multicast Address	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
IGMP Snooping Router Port	<input checked="" type="radio"/> Auto <input type="radio"/> Any <input type="radio"/> Static

6. Select the IGMP Snooping Status **Enable** radio button.
By default, the **Enable** radio button is selected.
7. Make sure that a VLAN ID between 1 and 4094 is stated in the **VLAN ID Enabled for IGMP Snooping** field.
You can specify a VLAN for IGMP snooping only if you enabled port-based or 802.1Q-based VLANs (see [Use VLANs for Traffic Segmentation](#) on page 15).
IGMP snooping functions only on the VLAN that is specified in the **VLAN ID Enabled for IGMP Snooping** field.
8. (Optional) Select the Validate IGMPv3 IP header **Enable** radio button.

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

9. (Optional) Select the Block Unknown MultiCast Address **Enable** radio button.
When this feature is enabled, multicast packets are forwarded only to the ports that are in the multicast group learned from IGMP snooping. All unknown multicast packets are dropped.
10. (Optional) Select a port to be the dedicated IGMP snooping static router port if no IGMP query exists in the network for the switch to discover the router port dynamically.
Select one of the following **IGMP Snooping Static Router Port** radio buttons:
 - **Auto.** If the switch receives a query message, the switch configures the router port or ports dynamically. This is the default setting.
 - **Any.** IGMP Join and Leave packets are sent to every port of the switch.
 - **Static.** Select one port as the dedicated IGMP snooping static router port by selecting the check box that is associated with the port number. All IGMP Join and Leave reports are forwarded to the selected port.
11. Click the **Apply** button.
Your settings are saved.

Specify a VLAN for IGMP snooping

You can specify a VLAN for IGMP snooping only if you enabled port-based or 802.1Q-based VLANs (see [Use VLANs for Traffic Segmentation](#) on page 15).

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 7.
The login page displays.
4. Enter the switch password.

The default password is **password**. The password is case-sensitive.
The Switch Information page displays.

5. Select **System > Multicast**.

IGMP Snooping Configuration

IGMP Snooping Status	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
VLAN ID Enabled for IGMP Snooping	<input type="text" value="1"/> (1 to 4094)
Validate IGMPv3 IP header	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Block Unknown Multicast Address	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
IGMP Snooping Router Port	<input checked="" type="radio"/> Auto <input type="radio"/> Any <input type="radio"/> Static

6. Select the IGMP Snooping Status **Enable** radio button.
By default, the **Enable** radio button is selected.
7. In the **VLAN ID Enabled for IGMP Snooping** field, enter the ID of the VLAN.
By default, if you enable IGMP snooping, snooping occurs on VLAN 1. However, you can enable snooping on any VLAN:
 - For port-based VLANs, you can enter a VLAN ID from 1 to 50.
 - For 802.1Q-based VLANs, you can enter a VLAN ID from 1 to 4094.
8. Click the **Apply** button.
Your settings are saved.

Enable the Auto-Video configuration

You can enable the Auto-Video VLAN for IGMP snooping only if you enabled port-based or 802.1Q-based VLANs (see [Use VLANs for Traffic Segmentation](#) on page 15). By default, the Auto-Video VLAN is disabled. The default ID of the Auto-Video VLAN is ID 3, which you cannot change.

To enable the Auto-Video VLAN:

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

If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.

The login page displays.

4. Enter the switch password.

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

The Switch Information page displays.

5. Select **System > Multicast > Auto-Video**.

The Auto-Video Configuration page displays.

6. Select the Auto-Video Status **Enable** radio button.

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

7. Click the **Apply** button.

Your settings are saved.

Set up link aggregation

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

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

The switch can support eight LAGs.

Set up link aggregation in the following order:

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

For more information, see the following sections:

- [Set up a static link aggregation group](#) on page 52
- [Set up a Link Aggregation Control Protocol group](#) on page 53
- [Set up the LACP system priority for the switch](#) on page 55
- [Set Up LACP port priority and time-out values](#) on page 55

Set up a static link aggregation group

The switch can support eight LAGs, which can be a combination of static link aggregation and LACP groups.

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

To specify LAG membership for a static LAG and enable a static LAG:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > LAG > LAG Membership**.

6. In the **LAG ID** menu, select the LAG ID.
You can select a LAG ID from 1 to 8.
7. Enter a name in the **LAG Name** field.
You can enter a name of up to 15 alphanumeric characters.
8. Select the ports for the LAG by selecting the check boxes that are associated with the port numbers.
A LAG consists of at least two ports.
9. Click the **Apply** button.
Your settings are saved.

10. To enable the LAG for which you just set up the port membership, do the following:
 - a. Select **System > LAG > LAG Configuration**.

LAG Configuration

<input type="checkbox"/>	LAG ID	LAG Name	Admin Mode	LAG Type	Port Member	LAG Status
<input type="checkbox"/>			-	-		
<input type="checkbox"/>	Lag1		Disable	Static		Down
<input type="checkbox"/>	Lag2		Disable	Static		Down
<input type="checkbox"/>	Lag3		Disable	Static		Down
<input type="checkbox"/>	Lag4		Disable	Static		Down
<input type="checkbox"/>	Lag5		Disable	Static		Down
<input type="checkbox"/>	Lag6		Disable	Static		Down
<input type="checkbox"/>	Lag7		Disable	Static		Down
<input type="checkbox"/>	Lag8		Disable	Static		Down

- b. Select the LAG ID of the LAG for which you just set up the port membership.
- c. In the **Admin Mode** menu, select **Enable**.
- d. In the **LAG Type** menu, select **Static**.
 The Port Member field for the selected LAG ID shows the ports that you selected in Step 8.
 The LAG Status field for the selected LAG ID shows whether the LAG is established (Up) or not established (Down).
- e. Click the **Apply** button.
 Your settings are saved.

Set up a Link Aggregation Control Protocol group

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

To specify an LACP group:

1. Connect your computer to the same network as the switch.
 You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
 If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
 The login page displays.
4. Enter the switch password.
 The default password is **password**. The password is case-sensitive.
 The Switch Information page displays.

5. Select **System > LAG > LAG Membership**.

LAG Membership

LAG ID		Lag1		LAG Name	
Ports	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49				
	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50				

6. In the **LAG ID** menu, select the LAG ID.
You can select a LAG ID from 1 to 8.
7. Enter a name in the **LAG Name** field.
You can enter a name of up to 15 alphanumeric characters.
8. Select the ports for the LAG by selecting the check boxes that are associated with the port numbers.
A LAG consists of at least two ports.
9. Click the **Apply** button.
Your settings are saved.
10. To enable the LAG as an LACP LAG, do the following:
 - a. Select **System > LAG > LAG Configuration**.

LAG Configuration

<input type="checkbox"/>	LAG ID	LAG Name	Admin Mode	LAG Type	Port Member	LAG Status
<input type="checkbox"/>			-	-		
<input type="checkbox"/>	Lag1		Disable	Static		Down
<input type="checkbox"/>	Lag2		Disable	Static		Down
<input type="checkbox"/>	Lag3		Disable	Static		Down
<input type="checkbox"/>	Lag4		Disable	Static		Down
<input type="checkbox"/>	Lag5		Disable	Static		Down
<input type="checkbox"/>	Lag6		Disable	Static		Down
<input type="checkbox"/>	Lag7		Disable	Static		Down
<input type="checkbox"/>	Lag8		Disable	Static		Down

- b. Select the LAG ID of the LAG for which you just set up the port membership.
- c. In the **Admin Mode** menu, select **Enable**.
- d. In the **LAG Type** menu, select **LACP**.
The Port Member field for the selected LAG ID shows the ports that you selected in Step 8.
The LAG Status field for the selected LAG ID shows whether the LAG is established (Up) or not established (Down).
- e. Click the **Apply** button.
Your settings are saved.

Set up the LACP system priority for the switch

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

To change the LACP system priority:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > LAG > LACP Configuration**.
The LACP Configuration page displays.
6. In the **LACP System Priority** field, enter a number from 1 to 65535.
The default is 32768.
7. Click the **Apply** button.
Your settings are saved.

Set Up LACP port priority and time-out values

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

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

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > LAG > LACP Port Configuration**.

LACP Port Priority

<input type="checkbox"/>	Port	LACP Priority	Timeout
<input type="checkbox"/>		<input type="text"/>	<input type="text" value="-"/>
<input type="checkbox"/>	g1	128	Long
<input type="checkbox"/>	g2	128	Long
<input type="checkbox"/>	g3	128	Long
<input type="checkbox"/>	g4	128	Long
<input type="checkbox"/>	g5	128	Long
<input type="checkbox"/>	g6	128	Long
<input type="checkbox"/>	g7	128	Long
<input type="checkbox"/>	g8	128	Long
<input type="checkbox"/>	g9	128	Long
<input type="checkbox"/>	g10	128	Long
<input type="checkbox"/>	g11	128	Long
<input type="checkbox"/>	g12	128	Long
<input type="checkbox"/>	g13	128	Long
<input type="checkbox"/>	g14	128	Long
<input type="checkbox"/>	g15	128	Long
<input type="checkbox"/>	g16	128	Long

6. Select one or more ports.
7. In the **LACP Priority** field, enter a new value.
You can enter a value from 1 to 65535. A higher value indicates a lower priority. The default value is 128.
8. In the **Timeout** menu, select the time-out value.
The default value is Long. The other option is Short.
9. Click the **Apply** button.

Your settings are saved.

6

Manage and Monitor the Switch

This chapter covers the following topics:

- [Manage flow control](#)
- [Manage the port speed and the port status](#)
- [Enable loop prevention](#)
- [Manage power saving options](#)
- [Manually download and upgrade the firmware](#)
- [Reboot the switch](#)
- [Save the switch configuration](#)
- [Restore a saved switch configuration](#)
- [Restore factory default settings](#)
- [Enable port mirroring](#)
- [View switch information or change the switch device name](#)
- [View or clear the port statistics](#)

Manage flow control

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

To manage flow control:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > Management > Port Status**.

Port Status

<input type="checkbox"/>	Port	Port Description	Port Status	Speed	Linked Speed	Flow Control
<input type="checkbox"/>				<input type="text" value="Auto"/>		<input type="text" value="Disable"/>
<input type="checkbox"/>	g1		Up	Auto	1000M	Disable
<input type="checkbox"/>	g2		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g3		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g4		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g5		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g6		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g7		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g8		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g9		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g10		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g11		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g12		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g13		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g14		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g15		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g16		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g17		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g18		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.

Manage the port speed and the port status

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

To manage the port speed and the port status:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.

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

Port Status

<input type="checkbox"/>	Port	Port Description	Port Status	Speed	Linked Speed	Flow Control
				<input type="text" value="Auto"/>		<input type="text" value="Disable"/>
<input type="checkbox"/>	g1		Up	Auto	1000M	Disable
<input type="checkbox"/>	g2		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g3		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g4		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g5		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g6		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g7		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g8		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g9		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g10		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g11		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g12		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g13		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g14		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g15		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g16		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g17		Down	Auto	No Speed	Disable
<input type="checkbox"/>	g18		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 autonegotiation with the link partner. This is the default setting.
 - **Disable**. The port is shut down.
 - **10M Half**. The port is forced to function at 10 Mbps with half duplex.
 - **10M Full**. The port is forced to function at 10 Mbps with full duplex.
 - **100M Half**. The port is forced to function at 100 Mbps with half duplex.
 - **100M Full**. The port is forced to function at 100 Mbps with full duplex.
8. To configure more ports, repeat this procedure from [Step 6](#) on.
9. Click the **Apply** button.
Your settings are saved.

Enable loop prevention

If loop prevention is enabled and the switch detects a loop, the switch blocks one of the ports that are part of the loop and both LEDs of that port blink at a constant speed. If two ports are part of a loop, the port with the highest port number is blocked. For example, if port 1 and port 2 are part of a loop, port 2 is blocked while port 1 continues

to process traffic. The loop status (that is, port blocking and LED blinking) is cleared if the switch does not detect the loop for a period of about 16 seconds.

To enable loop prevention:

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

Manage power saving options

You can manage the IEEE 802.3az Energy Efficient Ethernet (EEE) function, cable length power saving, or link-up and link-down power saving, or a combination of these features:

- **Short Cable Power Saving.** Dynamically detects and adjusts power that is required for the detected cable length.
- **Link-Down Power Saving.** Reduces the power consumption considerably when the network cable is disconnected. When the network cable is reconnected, the switch detects an incoming signal and restores normal power.
- **EEE.** Combines the Energy Efficient Ethernet (EEE) 802.3 MAC sublayer with the 100BASE-TX and 1000BASE-T physical layers to support operation in Low Power Idle (LPI) mode. When LPI mode is enabled, systems on both sides of the link can

disable portions of their functionality and save power during periods of low link utilization.

To manage the power saving options:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > Management > Power Saving Mode**.
The Power Saving Mode page displays.
6. Select the one of the following radio buttons:
 - **Enable**. The power saving options are enabled. This is the default setting.
 - **Disable**. The power saving options are disabled.
7. Click the **Apply** button.
Your settings are saved.

Manually download and upgrade the firmware

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

To manually download and upgrade the firmware using the local browser interface:

1. Visit netgear.com/support/download/.
2. Enter your product model number in the **Enter a Product Name/Model Number** field, search by clicking the magnifying glass, and locate the firmware for your switch.

3. Download the firmware to your computer.
4. Read the new firmware release notes to find out if you must reconfigure the switch after upgrading.
5. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
6. Launch a web browser.
7. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
8. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
9. Select **System > Maintenance > Firmware Upgrade**.
The Firmware Upgrade page displays.
10. Click the **Browse** button and locate and select the new firmware image file.
11. Click the **Apply** button.

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

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

Reboot the switch

You can reboot the switch remotely.

To reboot the switch:

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

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > Maintenance > Device Reboot**.
The Device Reboot page displays.
6. Select the check box.
7. Click the **Apply** button.
The switch reboots.

Save the switch configuration

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

To save the switch configuration:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > Maintenance > Save Configuration**.
The Save Configuration page displays.

6. Click the **Save** button.

A pop-up window opens. Depending on the settings of your browser, you can select a location to save the switch configuration file (a `.cfg` file).

7. Follow the directions of your browser to save the switch configuration.

Restore a saved switch configuration

You can restore a switch configuration that you saved.

To restore the switch configuration that you saved:

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

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

2. Launch a web browser.

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

If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.

The login page displays.

4. Enter the switch password.

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

The Switch Information page displays.

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

The Restore Configuration page displays.

6. Click the **Browse** button and locate and select the saved configuration file (a `.cfg` file).

7. Click the **Apply** button.

The saved configuration is restored to the switch.

Restore factory default settings

You can return the switch to its factory settings.

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

To restore factory settings:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > Maintenance > Factory Default**.
The Factory Default page displays.
6. Select the check box.
7. Click the **Apply** button.
The switch returns to its factory settings. The switch reboots to load the restored configuration.

Enable port mirroring

Port mirroring lets you mirror the incoming (ingress) and outgoing (egress) traffic of one or more ports (the source ports) to a single predefined destination port.

To enable port mirroring:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.

4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.

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

Port Mirror Configuration

Mirror Status ☒ Disable ☐ Enable

Source Port

Ports

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50

Destination Port

Ports

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50

6. In the **Destination Port** menu, select the destination port.
You can select a single destination port only. You cannot select a destination port that is a member of a LAG.
7. In the Source Port section, select one or more source ports by selecting the check boxes that are associated with the port numbers.
You can select more than one source port. You cannot select a source port that is a member of a LAG.
8. In the **Mirroring** menu, select **Enable**.
By default, mirroring is disabled.
9. Click the **Apply** button.
Your settings are saved.

View switch information or change the switch device name

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

You can also change the switch device name. This device name shows in, for example, Windows Explorer and Bonjour.

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

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.

Switch Information

Product Name	GS750E
Switch Name	<input type="text" value="Plus Switch GS750E"/>
Serial Number	526174DPF00B5
MAC Address	40:5D:82:45:C0:74
Firmware Version	1.0.0.19
DHCP Mode	<input type="text" value="Disable"/> <input type="checkbox"/> Refresh
IP Address	<input type="text" value="192.168.100.112"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway Address	<input type="text" value="192.168.100.1"/>

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

5. To change the switch device name, do the following:
 - a. In the **Switch Name** field, enter a name of up to 20 characters.
 - b. Click the **Apply** button.
Your settings are saved.

View or clear the port statistics

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

To view or clear the port statistics:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.

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

Port Statistics

Port	Bytes Received	Bytes Sent	CRC Error packets
g1	41096731	879820	0
g2	0	0	0
g3	0	0	0
g4	0	0	0
g5	0	0	0
g6	0	0	0
g7	0	0	0
g8	0	0	0
g9	0	0	0
g10	0	0	0
g11	0	0	0
g12	0	0	0
g13	0	0	0
g14	0	0	0
g15	0	0	0
g16	0	0	0
g17	0	0	0
g18	0	0	0
g19	0	0	0

6. 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

Test cable connections

You can use the cable diagnostic feature to easily find out the health status of network cables. If any problems exist, this feature helps quickly locate the point where the cabling fails, allowing connectivity issues to be fixed much faster, potentially saving technicians hours of troubleshooting.

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

To test cable connections:

1. Connect your computer to the same network as the switch.
You can use a WiFi or wired network connection, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see [Access the switch using a web browser](#) on page 7.
The login page displays.
4. Enter the switch password.
The default password is **password**. The password is case-sensitive.
The Switch Information page displays.
5. Select **System > Monitoring > Cable Tester**.

Cable Tester

<input type="checkbox"/>	Port	Test Results	Cable Fault Distance (meters)
<input type="checkbox"/>	g1		
<input type="checkbox"/>	g2		
<input type="checkbox"/>	g3		
<input type="checkbox"/>	g4		
<input type="checkbox"/>	g5		
<input type="checkbox"/>	g6		
<input type="checkbox"/>	g7		
<input type="checkbox"/>	g8		
<input type="checkbox"/>	g9		
<input type="checkbox"/>	g10		
<input type="checkbox"/>	g11		
<input type="checkbox"/>	g12		
<input type="checkbox"/>	g13		
<input type="checkbox"/>	g14		
<input type="checkbox"/>	g15		
<input type="checkbox"/>	g16		
<input type="checkbox"/>	g17		
<input type="checkbox"/>	g18		
<input type="checkbox"/>	g19		

6. Select one or more check boxes.
7. Click the **Test Selected Port** button.

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

Resolve a subnet conflict to access the switch

If you power on the switch before you connect it to a network that includes a DHCP server, the switch uses its own default IP address of 192.168.0.239. This subnet might be different from the subnet used in your network. You might see the following message if you try to access the switch:

```
The switch and manager IP address are not in the same subnet.
```

To resolve this subnet conflict:

1. Disconnect the Ethernet cable between the switch and your network.
2. Shut down power to the switch.
3. Reconnect the Ethernet cable between the switch and your network.
4. Reapply power to the switch.

The switch powers on. The network DHCP server discovers the switch and assigns it an IP address that is in the correct subnet for the network.

A

Factory Default Settings

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

Table 1. 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. If enabled, the default voice VLAN is VLAN 2. If enabled, the default Auto-Video VLAN is VLAN 3.
802.1p/DSCP-based QoS	Enabled
Port-based QoS	Disabled
Rate limiting	Disabled
Broadcast filtering	Disabled
Loop prevention	Disabled
Port speed	Autonegotiation
Flow control	Disabled
Port mirroring	Disabled
Access control	Disabled

Table 1. Factory default settings (Continued)

Feature	Setting
Power saving mode	Enabled
Bonjour	Enabled
Auto-DoS mode	Enabled