NETGEAR®

Audio Video User Manual

M4500 Intelligent Fully Managed Switches

November 2023
202-12714-01

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

Support and Community

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

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

Regulatory and Legal

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

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

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

See the regulatory compliance document before connecting the power supply.

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

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

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

Applicable to 6 GHz devices only: Only use the device indoors. The operation of 6 GHz devices is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-12714-01	November 2023	First publication.

Contents

Chapter 5 Port Configuration

Chapter 6 Security

Chapter 7 Manage and monitor the switch

Chapter 8 Diagnostics and Troubleshooting

1

Getting Started with the AV UI

This user manual is for the M4500 Intelligent Fully Managed Switches and covers all M4500 switch models.

This chapter provides an overview of how you can use your switch and access the audio-video (AV) local browser user interface (UI), in short AV UI.

The chapter contains the following sections:

Note: For more information about the topics that are 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, you might need to update your firmware.

Supported Switches

This AV user manual is for the NETGEAR M4500 Intelligent Fully Managed Switches, which includes the following models:

- M4500-32C
- M4500-48XF8C

Available publications

You can download the following publications for the M450 Intelligent Fully Managed Switches by visiting netgear.com/support/download.

- Installation guide
- Hardware installation guide
- Audio-video user manual (this manual)
- Software administration manual
- CLI command reference manual

AV local browser UI overview

Your switch contains an embedded web server and management software for managing and monitoring the switch. The switch functions as a simple switch without the management software. However, you can use the management software to configure many advanced features that can improve AV flows, switch efficiency, and overall network performance.

The switch software includes a set of comprehensive management features for configuring and monitoring the switch through one of the following methods:

- Audio-video local browser user interface (AV UI), either over an Ethernet network port or over the out-of-band (OOB) port (also referred to as the service port).
- Simple Network Management Protocol (SNMP)
- Command-line interface (CLI)

Each of the standards-based management methods allows you to configure and monitor the components of the switch. The method you use to manage the system depends on your network size and requirements, and on your preference.

This manual describes how to use the audio-video (AV) local browser user interface (UI) to manage and monitor the switch. We abbreviate the audio-video local browser UI as the AV UI.

The AV UI is a web-based management tool that lets you configure and manage audio-video and other types of network profiles remotely using a standard web browser.

Log in to the AV UI over the OOB port

You can configure network information on the IPv4 service port, also referred to as the out-of-band (OOB) port. The OOB port is a dedicated Ethernet port for out-of-band management of the switch. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.

By default, no IP address is set for the OOB port, but its DHCP client is enabled so that the port can receive an IP address from a DHCP server in your network. If you do not use a DHCP server or prefer to set a fixed IP address for the OOB port, use the CLI to configure an IP address for the OOB port.

For information about setting a fixed IP address for the OOB port, see Set a fixed IP address for the OOB port on page 59.

The local device password that you must use to log in to the AV UI is the password that you set up when you first logged in to the CLI. Using the CLI, you can change the password again.

To use a known IP address that is assigned to the OOB port to access the switch over the AV UI:

1. Connect an Ethernet cable from an Ethernet port on your computer to the OOB port on the switch.
2. If you are using a DHCP server to assign an IP address to the OOB port, reboot the switch so that the OOB port is set to its default IP address.
3. Launch a web browser.
4. In the address field of your web browser, enter the IP address that is assigned to the OOB port.

   The login page displays.
5. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.

Save the running configuration to the startup configuration

After you make changes on a page of the AV UI and click the **Apply** button (or, in some windows, the **Save** button), your changes are saved for the current session but are not retained when you restart the switch. That is, your running configuration is not saved to the startup configuration (the startup-config file), which means that it is not yet permanently saved.

For information about saving your current changes (your running configuration) to the startup configuration, see Save the running configuration on page 55.

Register your switch

To qualify for product updates and product warranty, we encourage you to register your product.

Registration confirms that your email alerts work, lowers technical support resolution time, and ensures your shipping address accuracy. We would also like to incorporate your feedback into future product development. We never sell or rent your email address and you can opt out of communications.

To register your switch with NETGEAR:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. At the top of page, from the **Question/Help** menu, select **Register**.
   The NETGEAR Account Login page displays. If the page does not display, visit the following website:
   my.netgear.com/registration/login.aspx
5. Enter your NETGEAR account email address and password and click the **NETGEAR Sign In** button.

If you did not yet create a NETGEAR account, click the **Create an account** link, follow the directions onscreen to create an account, and then register the switch with your NETGEAR email address and password.

2

Audio-Video Profile Templates and Network Profiles

The switch provides preconfigured audio-video (AV) profile templates that you can configure and assign to switch ports and VLANs, thereby creating network profiles.

You can also set up your own AV profile templates.

These are the essential differences between an AV profile template and a network profile:

- **AV profile template**: A preconfigured or custom template with QoS, multicast, or PTP settings, or a combination of these settings, that you can apply to multiple network profiles.
- **Network profile**: An AV profile template that you configured and assigned to one or more switch ports, to a VLAN, and as an option, to a specific IP address.

The chapter contains the following sections:

Overview of preconfigured AV profile templates

An AV profile template integrates NETGEAR proprietary settings, allowing you to optimize specific audio and video environments. You can use an AV profile template to create one or multiple network profiles. For example, you might use the same AV profile template to set up three network profiles for different areas at the same physical location: one network profile for the lobby, one for the theater, and one for the patio.

The switch provides the following preconfigured AV profile templates:

- **Audio AES67**: Use this template to connect the switch to AES67 audio IP devices and their controller.
- **Audio Dante**: Use this template to connect the switch to Dante audio devices and their controller.
- **Audio Q-SYS**: Use this template to connect the switch to IP audio Q-SYS devices and their controller.
- **Audio Soundgrid**: Use this template to connect the switch to IP Audio SoundGrid devices and their controllers.
- **Crestron DigitalMedia AV Network**: Use this template to connect the switch to Crestron DM NVX (video), Crestron DM NAX (audio), Creston 1 Beyond cameras (NDI), computers, and other Crestron Control network devices.
- **Data**: Use this template to connect the switch to streaming ACN (sACN), Art-Net, mobile ad hoc network (MANET), and other network devices as well as to computers.
- **Lighting**: Use this template to connect the switch to streaming ACN (sACN), Art-Net, and MANET lighting devices.
- **NUCLEUS Converged AV Network**: Use this template to connect the switch to EvertzAV NUCLEUS Session Manager and UXP gateways on a single converged network.
- **Sonos**: Use this template to connect the switch to a Sonos smart home sound system.
- **Video**: Use this template to connect the switch to IP video devices and their controller when audio can be sent and received using another VLAN tag in another profile simultaneously.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.

- **Video NDI4**: Use this template to connect the switch to video devices and cameras that support Network Device Interface (NDI) version 4 with multi-TCP (mTCP) transport.
- **Video NDI5 with Dante, Q-Sys or AES67 audio**: Use this template to connect the switch to video devices and cameras that support NDI version 5 with Reliable User Datagram Protocol (RUDP). Audio Dante, Q-SYS, or AES67 is supported at the same time in the same VLAN.
- **Video with AES67 audio**: Use this template to connect the switch to IP video devices and their controllers when AES67 audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Video with Dante audio**: Use this template to connect the switch to IP video devices and their controllers when Dante audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Video with Q-SYS audio**: Use this template to connect the switch to IP video devices and their controllers when Q-SYS audio is supported in the same VLAN.
  This template can support devices such as Crestron DM NVX systems, AMX SVSI products, ZeeVee products, Aurora Multimedia products, Kramer products, Atlona products, products that support Libav, Visionary Solutions products, Wyrestorm products, Extron NAV products, Dante video products, and products that comply with standardization by the SDVoE Alliance.
- **Visionary AV Network**: Use this template to connect the switch to Visionary AV systems for quick auto-detection and for ease of configuration.

About PTP residency time stamping

Precision Time Protocol (PTP, IEEE 1588) is a protocol that enables precise synchronization of clocks with a sub-microsecond accuracy across a packet-based network. PTP lets network devices of different precision and resolution synchronize to a grandmaster clock through an exchange of packets across the network.

The switch supports a PTP end-to-end transparent clock that is used in the *PTP residency time stamping* feature, which, by default, is enabled globally on the switch. You can

configure PTP residency time stamping globally only (see Configure PTP residency time stamping on page 23).

Network profiles

You can use either a preconfigured AV profile template (for example, Audio Dante) or a custom AV profile template that you created to set up one or multiple network profiles.

Change the Default VLAN profile

The default network profile is the Default VLAN profile, which uses the Data AV profile template and VLAN 1. All ports are untagged members of VLAN 1. You can change the AV profile template and the member ports. For each port, you can either remove the port from VLAN 1 or change the port to a tagged port.

To change the Default VLAN profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Configured Profiles table, to the right of the Default VLAN, click the **3 dots** icon and select **Edit**.
   The Edit Profile Default window displays.
6. Select the ports to which the profile must apply.
   By default, all ports are selected as untagged ports for the profile. That is, each port is marked with a green icon.
   To configure ports, do the following:
   - **Change a port to a tagged port**: Click the port once. The port is marked with a T icon (for tagged).

- **Remove a port from the profile**: Click the port twice to remove it from the profile. The port is not marked with a green icon or T icon.

7. To change the AV profile template, from the **Profile Template** menu, select another template.

   The default AV profile template is the Data template.

8. To change the color for the Default VLAN for visual representation, click the box in the **Color** field, and select a color.
9. Click the **Apply** button.

   Your settings are saved. The window closes. The Network Profiles page displays again.

10. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Use an AV profile template to configure and assign a network profile

When you configure a network profile, you must give the profile a name and assign it to a VLAN. You can also assign a specific IP address to the profile and add a color for visual representation.

To use an AV profile template to configure and assign a network profile:

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

   The login page displays.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.

4. Select **Configure > Network Profiles**.

   The Network Profiles page displays.

5. In the Profile Templates table, to the right of the AV profile template that you want to use, do one of the following:

   - **Preconfigured AV profile template**: Click the **gear** icon.
   - **Custom AV profile template**: Click the **3 dots** icon and select **Configure**.

The Profile Configure window displays.

6. Select the ports to add them to or exclude them from the VLAN to which the network profile must apply:
   - **Untagged port**: Click the port once. The port is added as an untagged port and is marked with a green icon. To untag all ports, click the **Untag all** button.
   - **Tagged port**: Click the port twice. The port is added as a tagged port and is marked with a T icon (for tagged). To tag all ports, click the **Tag all** button.
   - **Excluded port**: Do not click the port. The port is excluded and is not marked with a green icon or T icon. To exclude all ports, click the **Remove all** button.
7. In the **Profile Name** field, enter a name for the profile.

   Note: You cannot change the selection from the **Profile Template** menu.
8. From the **VLAN ID** menu, select the VLAN ID to which the template must apply.
9. To add a color to the network profile for visual representation, click the box in the **Color** field, and select a color.
10. To assign a specific IP address to the network profile, and as an option, use the network profile as a DHCP server, do the following:
    a. Turn on the **Edit VLAN Routing / DHCP Server** toggle so that it displays green and is positioned to the right.
    The IP address menu and fields become available.
    b. From the **VLAN IP Settings** menu, select **Static** or **DHCP client**.
    By default, None is selected. If you select **Static**, you must specify the IP address settings manually and you can also configure the network profile as a DHCP server. (See the following step.)
    If you select **DHCP client**, the network profile functions as a DHCP client and a DHCP server in your network assigns an IP address to the network profile.
    c. If you select **Static** from the **VLAN IP Settings** menu, specify the IP address and subnet mask in the **VLAN IP Address** and **Subnet Mask** fields.
11. Click the **Apply** button.

    Your settings are saved. The window closes. The Network Profiles page displays again.
12. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Change a network profile

You can change an existing network profile.

To change a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Configured Profiles table, to the right of the network profile that you want to change, click the **3 dots** icon and select **Edit**.
   The Edit Profile window displays.
6. Change the settings as needed.
   For more information about the settings, Use an AV profile template to configure and assign a network profile on page 15.
   You cannot change the VLAN ID and AV profile template selection.
7. Click the **Apply** button.
   Your settings are saved. The window closes. The Network Profiles page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove a network profile

You can remove an existing network profile that you no longer need.

To remove a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.

4. Select **Configure > Network Profiles**.

   The Network Profiles page displays.

5. In the Configured Profiles table, to the right of the network profile that you want to remove, click the **3 dots** icon and select **Delete**.

   A confirmation window displays.

6. Click the **Delete** button.

   The network profile is removed. The window closes. The Network Profiles page displays again.

7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Custom AV profile templates

You can create your own AV profile template. After you do so, you can use the custom AV profile template to set up one or multiple network profiles (see Use an AV profile template to configure and assign a network profile on page 15).

The advantage of a custom AV profile template is that you can decide whether to enable multicast, PTP, and QoS. If you enable QoS, you can specify either a DSCP or CoS configuration.

Create a custom AV profile template

Before you create a custom AV profile template, consider the following:

- Does the template require multicast to be enabled?
- Does the template require Precision Time Protocol (PTP) to be enabled?

Note: You can enable PTP and multicast for a custom AV profile template but you cannot configure the PTP and multicast settings in the AV UI. To configure PTP and multicast settings, use the CLI. For more information, see the CLI command reference manual, which you can download by visiting netgear.com/support/download.

To create a custom AV profile template:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. At the top right of the Profile Templates table, click the **Create AV Template** link.
   The Create AV Profiles window displays.
6. In the **Profile Type** field, enter a name for the type of service that the template can provide.
7. In the **Profile Description** field, enter a description for the template.
8. To enable multicast, turn on the **Multicast** toggle so that it displays green and is positioned to the right.
   By default, multicast is disabled and the toggle displays gray and is positioned to the left.
9. To enable PTP, turn the **PTP** toggle so that it displays green and is positioned to the right.
   By default, PTP is disabled and the toggle displays gray and is positioned to the left.
10. Click the **Save** button.
    Your settings are saved. The window closes. The Network Profiles page displays again.
11. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Change a custom AV profile template

You can change an existing custom AV profile template. You cannot change a preconfigured AV profile template.

To change a custom AV profile template:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Profile Templates table, to the right of the custom AV profile template that you want to change, click the **3 dots** icon and select **Edit**.
   The Edit AV Profiles window displays.
6. Change the settings as needed.
   For more information about the settings, Create a custom AV profile template on page 18.
   You cannot change the name of the AV profile template.
7. Click the **Save** button.
   Your settings are saved. The window closes. The Network Profiles page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove a custom AV profile template

You can remove an existing custom AV profile template that you no longer need. You cannot remove a preconfigured AV profile template.

To remove a custom AV profile template:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

The local device password is the password that you set up when you first logged in to the CLI.

The Overview page displays.

4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Profile Templates table, to the right of the custom AV profile template that you want to remove, click the **3 dots** icon and select **Delete**.
   A confirmation window displays.
6. Click the **Delete** button.
   The AV profile template is removed. The window closes. The Network Profiles page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Auto-Trunk overview

Auto-trunk is a feature that lets the switch automatically enable Trunk mode on capable physical links and LAG interfaces between partner devices. A trunk can carry all active VLANs. By default, the Auto-Trunk feature is enabled on the switch.

If the switch automatically configures a port as a trunk (that is, an Auto-Trunk), all VLANs on the switch become part of the trunk, allowing automatic configuration of all VLANs on the switch and on the partner device with which the trunk is established.

Before the switch configures an Auto-Trunk, the switch first detects the physical links with the partner device that also supports the Auto-Trunk feature, and then automatically configures the ports that are connected and capable of forming a trunk at both ends.

A trunk carries multiple VLANs and accepts both tagged and untagged packets. Typically, a connection between the switch and a partner device such as a router, access point, or another switch functions as a trunk.

For the switch to form an Auto-Trunk with a partner device, the following are required:

- The Auto-Trunk feature must be supported and globally enabled on the switch and the partner device.
- The interconnected ports on both the switch and the partner device must be enabled.

- LLDP must be enabled on the interconnected ports on both the switch and the partner device.
- The interconnected ports on the switch and the partner device must be in the default switch port mode, which is the General mode. If the ports are in the Access mode or already in the Trunk mode, an Auto-Trunk cannot be formed on an Auto-LAG.

For an Auto-Trunk, the PVID is automatically set to the default VLAN. If you want to change the PVID for an Auto-Trunk, change the default VLAN.

The Auto-Trunk feature functions together with the Auto-LAG feature (see Auto-LAG overview on page 27). After an Auto-LAG is formed, the switch automatically applies trunk mode (that is, an Auto-Trunk) to the LAG at both ends. In other words, after an Auto-LAG is formed, the mode for the ports that participate in an Auto-LAG is automatically changed from the default switch port mode to the trunk port mode, and the Auto-LAG then becomes an Auto-Trunk.

After a port or an Auto-LAG becomes an Auto-Trunk, all VLANs on the switch become part of the trunk, and all VLANs on the switch and the partner device can be configured automatically.

Enable or disable Auto-Trunks

By default, the Auto-Trunk feature is globally disabled but you can globally enable it.

To enable or disable Auto-Trunks:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.

5. Below the graphical display of the switch, do one of the following:

   - **Disable Auto-Trunks**: Do the following:
     a. Turn off the toggle so that it displays gray and is positioned to the left.
        A pop-up window displays a warning.
     b. Click the **Yes** button.
        Your settings are saved.

   - **Enable Auto-Trunks**: Turn on the toggle so that it displays green and is positioned to the right.
     Your settings are saved automatically.

6. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure PTP residency time stamping

Depending on the network profile that is enabled, you can disable or enable the PTP residency time stamping manually, which then applies globally.

To globally enable or disable PTP residency time stamping:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. Below the graphical display of the switch, do one of the following:

   - **Disable PTP residency time stamping**: Turn off the toggle so that it displays gray and is positioned to the left.

   - **Enable PTP residency time stamping**: Turn on the toggle so that it displays green and is positioned to the right.
     By default, PTP residency time stamping is enabled.

Your settings are saved automatically.

6. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure the IGMP querier for a network profile

IGMP snooping requires that one central switch or router in a VLAN periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP querier. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port and network profile basis. If the switch does not receive updated membership information in a timely fashion, it stops forwarding multicasts to the port where the end device is located.

Each network profile can function as a querier in the VLAN in which it operates. The IGMP querier for the Default network profile with VLAN 1 is enabled by default. You can configure an IGMP querier for use with a network profile in another VLAN than VLAN 1.

To configure the IGMP querier for a network profile:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Network Profiles**.
   The Network Profiles page displays.
5. In the Configured Profiles table, to the right of the network profile that you want to change, click the **3 dots** icon and select **Querier**.
   The Edit default querier profile window displays.

6. Configure the settings for the querier:

   - **Election Participate**: Select to enable or disable the querier election participate mode for the network profile":

     - **Enabled**: Turn on the toggle so that it displays green and is positioned to the right. This setting indicates that the querier for the network profile participates in querier election, in which the lowest numbered IP address operates as the querier in the VLAN. Any other querier moves to the non-querier state.
     - **Disabled**: Turn off the toggle so that it displays gray and is positioned to the left. This setting indicates that if the querier for the network profile detects another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.

     Except for the Default network profile, the election participation is disabled by default, and the toggle displays gray and is positioned to the left

   - **Querier VLAN address**: Specify the IP address to be used as the source IP address in periodic IGMP queries that are sent on the VLAN.

   The Operational State field displays DISABLED or QUERIER, indicating if the network profile is functioning as a querier.

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

8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

3

Link Aggregation

Link aggregation groups (LAGs), which are also known as port-channels, allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing.

You can create a LAG that includes two or more ports as members and apply the LAG to a network profile. A LAG can be static or dynamic, and you can configure the LAG as a trunk. The switch can support multiple LAGs.

The chapter contains the following sections:

For more information about the LAG options of the switch, see the CLI reference manual, which you can download by visiting netgear.com/support/download.

Auto-LAG overview

An Auto-LAG is a LAG that forms automatically between two devices that support the Auto-LAG feature. An Auto-LAG is a dynamic Layer 2 LAG that is based on the Link Aggregation Control Protocol (LACP).

Note: A LAG is also referred to as a port channel or an EtherChannel.

The switch can detect the physical links with a partner device and automatically configure a LAG (that is, an Auto-LAG) on interconnected and capable ports at both ends. The switch can form one Auto-LAG only with each partner device.

The Auto-LAG feature functions together with the Auto-Trunk feature, which must also be supported and enabled on the partner device with which the LAG is formed. After an Auto-LAG is formed, the switch automatically applies trunk mode (that is, an Auto-Trunk) to the LAG at both ends. In other words, after an Auto-LAG is formed, the mode for the ports that participate in an Auto-LAG changes from the default switch port mode to the trunk port mode. For more information about the Auto-Trunk feature, see Auto-Trunk overview on page 21.

For the switch to form an Auto-LAG with a partner switch, the following are required:

- Both the Auto-LAG and Auto-Trunk features must be supported and globally enabled on the switch and the partner device.
- At least two links must be established between the switch and the partner device, and these links must support the same speed and duplex mode.
- The links cannot be members of a manually configured static or dynamic LAG.
- LLDP must be enabled on the interconnected ports on the switch and the partner device.
- The interconnected ports on the switch and the partner device must be in the default switch port mode, which is the General mode. If the ports are in the Access mode or already in the Trunk mode, an Auto-Trunk cannot be formed on the Auto-LAG.

An Auto-LAG can form with up to eight interfaces as members. Interfaces are automatically selected for the Auto-LAG based on whether they are up and available and on the following conditions:

- The interface is not already manually configured as a member of a LAG.
- The interface is not manually configured as a trunk port or an access port. That is, the interface must be a general interface.

Note: The switch can support multiple static and dynamic LAGs, but with each partner device, the switch can support a single Auto-LAG only.

Enable or disable Auto-LAGs

By default, the Auto-LAG feature is globally disabled but you can globally enable it.

To enable or disable Auto-LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. Below the graphical display of the switch, do one of the following:
   - **Disable Auto-LAGs**: Do the following:
     a. Turn off the toggle so that it displays gray and is positioned to the left
        A pop-up window displays a warning.
     b. Click the **Yes** button.
        Your settings are saved.
   - **Enable Auto-LAGs**: Turn on the toggle so that it displays green and is positioned to the right.
     Your settings are saved automatically. By default, the Auto-LAG feature is enabled.
6. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure the hash mode for Auto-LAGs

By default, the Auto-LAG feature is enabled and uses the *Layer 2; Destination* mode, which auto-configures a LAG based on the destination MAC address, VLAN, EtherType, and incoming port in the packet. You can change the hash mode (that is, the load balancing mode) for the Auto-LAG feature.

The switch balances traffic on a LAG by selecting one of the links in the channel over which packets must be transmitted. The switch selects the link by creating a binary pattern from selected fields in a packet and associating that pattern with a particular link. The hash mode determines which fields in a packet the switch selects.

To change the hash mode for the Auto-LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. Below the graphical display of the switch, from the **Auto-LAG Hash** menu, select the hash mode for the Auto-LAGs:
   - **Layer 2; Source**: Based on the source MAC address, VLAN, EtherType, and incoming port associated with the packet.
   - **Layer 2; Destination**: Based on the destination MAC address, VLAN, EtherType, and incoming port in the packet. This is the default mode.
   - **Layer 2; Source + Destination**: Based on the source and destination MAC addresses, VLAN, EtherType, and incoming port in the packet.
   - **Layer 3+4; Source**: Based on the source IP address and source TCP or UDP port field in the packet.
   - **Layer 3+4; Destination**: Based on the destination IP address and destination TCP or UDP port field in the packet.
   - **Layer 3+4; Source + Destination**: Based on the source and destination IP addresses and source and destination TCP or UDP port field in the packet.
   - **Enhanced Hashing Mode**: Based on dynamic selections of fields that are based on packet flow. For layer 2 packets, the source and destination MAC addresses are used. For IP packets, the source IP and destination IP addresses and TCP or UDP ports are used.

   Your settings are saved automatically.

6. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Create a LAG

Although the maximum number of LAGs that you can create and add is eight, the actual number of LAGs is limited by the number of ports that are available.

When you create a LAG, we recommend that you configure a network profile on the LAG rather than on a physical interface. By default, the network profile for a LAG is the default profile with VLAN 1.

To create a LAG:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. Below the graphical display of the switch, click the **Create LAG** link.
   The Create Link Aggregation Group window displays.
6. Select two or more ports that must become members of the LAG by clicking the individual ports.
7. In the **LAG Name** field, specify a name for the LAG.
8. From the **Hash** menu, select the hash mode for the LAG:
   - **Layer 2; Source**: Based on the source MAC address, VLAN, EtherType, and incoming port associated with the packet.
   - **Layer 2; Destination**: Based on the destination MAC address, VLAN, EtherType, and incoming port in the packet. This is the default mode.
   - **Layer 2; Source + Destination**: Based on the source and destination MAC addresses, VLAN, EtherType, and incoming port in the packet.

- **Layer 3+4; Source**: Based on the source IP address and source TCP or UDP port field in the packet.
- **Layer 3+4; Destination**: Based on the destination IP address and destination TCP or UDP port field in the packet.
- **Layer 3+4; Source + Destination**: Based on the source and destination IP addresses and source and destination TCP or UDP port field in the packet.
- **Enhanced Hashing Mode**: Based on dynamic selections of fields that are based on packet flow. For layer 2 packets, the source and destination MAC addresses are used. For IP packets, the source IP and destination IP addresses and TCP or UDP ports are used.

The switch balances traffic on a LAG by selecting one of the links in the channel over which packets must be transmitted. The switch selects the link by creating a binary pattern from selected fields in a packet and associating that pattern with a particular link. The hash mode determines which fields in a packet the switch selects.

9. From the **LAG ID** menu, select an ID from 1 to 8.
10. To create a static LAG instead of a dynamic LAG, turn on the **Static** toggle so that it displays green and is positioned to the right.

    When you create a static LAG, the member ports do not transmit LACPDUs, and the LACPDUs that the member ports receive are dropped.

11. Click the **Apply** button.

    Your settings are saved. The window closes. The Link Aggregation Group page displays again.

12. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Change a LAG

You can change an existing LAG.

To change a LAG:

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

   The login page displays.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

The local device password is the password that you set up when you first logged in to the CLI.

The Overview page displays.

4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. In the Link Aggregation Group table, to the right of the LAG that you want to change, click the **3 dots** icon and select **Edit**.
   The Edit Link Aggregation Group window displays.
6. Change the settings as needed.
   For more information about the settings, Create a LAG on page 30.
   You cannot change the LAG ID.
7. Click the **Apply** button.
   Your settings are saved. The window closes. The Link Aggregation Group page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove a LAG

You can remove an existing LAG that you no longer need.

To remove a LAG:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.
4. Select **Configure > Link Aggregation**.
   The Link Aggregation Group page displays.
5. In the Link Aggregation Group table, to the right of the LAG that you want to remove, click the **3 dots** icon and select **Delete**.

A confirmation window displays.

6. Click the **Delete** button.
   The LAG is removed. The window closes. The Link Aggregation Group page displays again.

7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

4

Multicast

Communication from point to multipoint is called multicasting. The source host (point) transmits a message to a group of zero or more hosts (multipoint) that are identified by a single IPv4 destination address. Although the task can be accomplished by sending unicast (point-to-point) messages to each of the destination hosts, multicasting is the preferred method for this type of transmission.

A multicast message is delivered to all members of its destination host group with the same best-efforts reliability as regular unicast IPv4 messages. The message is not guaranteed to arrive intact at all members of the destination group or in the same order relative to other messages.

Multicast is best suited for video and audio traffic requiring multicast packet control for optimal operation. Multicast for IPv4 includes support for IGMPv1, IGMPv2, and IGMPv3. For information about NETGEAR IGMP Plus™ and an example of a multicast spine and leaf topology, visit netgear.com/business/solutions/video-over-ip/.

The chapter contains the following sections:

- Configure the multicast mode for one or more ports
- Add or remove blocked multicast address ranges
- Display the multicast groups in your network

Configure the multicast mode for one or more ports

By default, if the switch detects multicast traffic on a port, it allows the traffic on the port. You can also force the switch to use one or more specific ports to process multicast traffic. As another option, you can block multicast traffic from selected networks on one or more ports.

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. If you choose to block multicast traffic on one or more ports, you can select one, several, or all of these multicast address ranges.

To configure the multicast mode for one or more ports:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.
4. Select **Configure > Multicast**.
   The Multicast page displays.
5. Select the port or ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
6. From the **Multicast Mode** menu, select the multicast mode:
   - **Default**: Multicast traffic is allowed on the selected port or ports based on the protocols that the switch detects.
     This is the default mode.
   - **Force Multicast**: Multicast traffic is forced through the selected port or ports.
   - **Block Multicast**: Multicast traffic from the networks that you select (see the next step) is blocked on the selected port or ports.

7. If you select **Block Multicast** from the **Multicast Mode** menu in the previous step, in this step select one or more multicast address ranges to be blocked from the **Multicast Block Addresses** menu:
   - **Individual multicast address ranges**: Click the **Network Ranges** text (*not* the check box) and select one or more check boxes for individual network ranges.
   - **All multicast network ranges**: Select the **Network Ranges** check box.

   The switch does not let traffic from a blocked address pass through.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Add or remove blocked multicast address ranges

Multicast host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. You can block one, several, or all of these multicast address ranges, which you then can apply to one or more ports. The switch does not let traffic from a blocked address pass through.

Note: If you want remove a blocked multicast range from a port, we recommend that you set the multicast mode for the port to default mode rather than remove the blockage for the multicast range. For more information, see Configure the multicast mode for one or more ports on page 35.

To add or remove blocked multicast address ranges:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.
4. Select **Configure > Multicast**.

The Multicast page displays.

5. From the **Multicast Block Addresses** menu, select one or more ranges to block or unblock:
   - **Individual multicast address ranges**: Click the **Network Ranges** text (*not* the check box) and select or clear one or more check boxes for individual network ranges.
   - **All multicast network ranges**: Select or clear the **Network Ranges** check box.
6. Click the **Apply** button.
   Your settings are saved.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Display the multicast groups in your network

The switch automatically detects the multicast groups in your network.

To display the multicast groups in your network:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Multicast**.
   The Multicast page displays.
   The Multicast Groups table displays detailed information about each multicast group in your network.

Legend	Description
Forwarding Port	The port on which multicast is enabled and on which multicast traffic is forwarded in the network.
Network Profile (VLAN)	The network profile to which the port is assigned (see Change the Default VLAN profile on page 14 or Use an AV profile template to configure and assign a network profile on page 15). By default, the port is assigned to the Data network profile with VLAN 1.
Subscriber Address	The IP address of the network device that is subscribed to receive multicast traffic.
Subscriber MAC Address	The MAC address of the network device that is subscribed to receive multicast traffic.
Multicast Address	The IP address of the device from which the multicast traffic originates.
Multicast MAC Address	The MAC address of the device from which the multicast traffic originates.
Type	The IGMP version that is being used (IGMPv1, IGMPv2, or IGMPv3).

5

Port Configuration

For the physical ports and LAGs on the switch, you can display the settings and configure the administrative mode of a port or LAG (both of which are enabled by default), the frame size for a port, and the flow control for a port. You can also add port descriptions.

Note: In this chapter, we use the term *interface* to indicate both physical ports and link aggregation interfaces.

The chapter contains the following sections:

- Administratively enable or disable one or more interfaces
- Add a description to one or more interfaces
- Set the frame size for one or more interfaces
- Configure flow control for one or more interfaces
- Display detailed information about the physical ports and LAGs

Administratively enable or disable one or more interfaces

By default, all ports and LAGs are administratively enabled. You can manually disable a port or LAG, but this can also occur automatically if a fault or other condition occurs. After a port or LAG is manually or automatically disabled, you can reenable the port or LAG.

To administratively enable or disable one or more ports or LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Port configuration**.
   The Port Configuration page displays.
5. Click the **Port Interface Settings** link:
   The Interface Settings page displays.
6. Select the one or more ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
   If you configured LAGs (see Link Aggregation on page 26), you can also select one or more LAGs.
7. Do one of the following:
   - **Disable the selected interfaces**: Turn off the **Enable Port** toggle so that it displays gray and is positioned to the left.
   - **Enable the selected interfaces**: Turn on the **Enable Port** toggle so that it displays green and is positioned to the right.
8. Click the **Apply** button.
   Your settings are saved.

9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Add a description to one or more interfaces

You can add a description for a port or LAG. This description is for informational purposes only.

To add a description for one or more ports or LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Port configuration**.
   The Port Configuration page displays.
5. Click the **Port Interface Settings** link:
   The Interface Settings page displays.
6. Select the one or more ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
   If you configured LAGs (see Link Aggregation on page 26), you can also select one or more LAGs.
7. In the **Port Description** field, type a text.
8. Click the **Apply** button.
   Your settings are saved. The description displays in the Port Interface Details table.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Set the frame size for one or more interfaces

The frame size is the maximum Ethernet frame size that the interface supports or is configured to use, including the Ethernet header, CRC, and payload. The default size is 1518.

To set the frame size for one or more ports or LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Port configuration**.
   The Port Configuration page displays.
5. Click the **Port Interface Settings** link:
   The Interface Settings page displays.
6. Select the one or more ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
   If you configured LAGs (see Link Aggregation on page 26), you can also select one or more LAGs.
7. In the **Frame Size** field, enter a value from **1518** (the minimum) to **9216** (the maximum).
   The default value is 1518.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Configure flow control for one or more interfaces

You can configure IEEE 802.3x flow control, which can help to prevent data loss when the port cannot keep up with the number of frames being switched:

- **Symmetric flow control**: With symmetric flow control, the switch can send a pause frame to stop traffic on the port if the amount of memory used by the packets on the port exceeds a preconfigured threshold and responds to pause requests from partner devices. The paused port does not forward packets for the time that is specified in the pause frame. When the pause frame time elapses, or the utilization returns to a specified low threshold, the switch enables the port to again transmit frames.
- **Asymmetric flow control**: With asymmetric flow control, the switch does not send pause frames, but does honor incoming pause frames by temporarily halting transmission.

To configure flow control for one or more ports or LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Port configuration**.
   The Port Configuration page displays.
5. Click the **Port Interface Settings** link:
   The Interface Settings page displays.
6. Select the one or more ports to which the settings must apply by clicking individual ports or, to select all ports, select the **Select All Ports** check box.
   If you configured LAGs (see Link Aggregation on page 26), you can also select one or more LAGs.

7. From the **Flow Control** menu, select a setting to configure what happens if the port buffers become full:
   - **Disable**: The switch does not send pause frames, and data loss could occur. This is the default setting.
   - **Symmetric**: The switch sends pause frames to stop traffic. The switch also honors incoming pause frames by temporarily halting transmission.
   - **Asymmetric**: The switch does not send pause frames, and data loss could occur. However, the switch does honor incoming pause frames by temporarily halting transmission.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Display detailed information about the physical ports and LAGs

To display detailed information about the physical ports and LAGs:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Port configuration**.
   The Port Configuration page displays.
   The Port Interface Details table displays detailed information about each port and LAG.

Legend	Description
Port Description	The description that you added (see Add a description to one or more interfaces on page 41). If you did not add a description, this field is blank.
Media Type	The media type that the port supports. The media type can be copper for an Ethernet port or fiber for a port that supports an SFP or SFP+ transceiver for a fiber connection.
Physical Status	The detected port speed and duplex mode.
Speed & Duplex Mode	The configured port speed and duplex mode.
Frame Size	The frame size (see Set the frame size for one or more interfaces on page 42). If you did not change the frame size, the default frame size is 9198.
Flow Control	The mode of flow control (see Configure flow control for one or more interfaces on page 43) . If you did not configure flow control, it is disabled.
Network Profile	The network profile to which the port is assigned (see Change the Default VLAN profile on page 14 or Use an AV profile template to configure and assign a network profile on page 15). By default, the port is assigned to the Data network profile.

6

Security

You can configure 802.1X port authentication and the associated RADIUS server settings.

The chapter contains the following sections:

For information about all security options of the switch, see the CLI reference manual, which you can download by visiting netgear.com/support/download.

Port authentication

With port-based authentication, if 802.1X is enabled both globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. 802.1X is the default authentication mode. 802.1X is also referred to as dot1x.

An 802.1X network includes three components:

- **Authenticator**: The port that is authenticated before access to system services is permitted.
- **Supplicant**: The host that is connected to the authenticated port requesting access to the system services.
- **Authentication server**: The external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

For port authentication to function, you must configure at least one RADIUS server (see RADIUS servers on page 50).

Manage port authentication for individual ports

After you enable 802.1X port authentication globally, the default port authentication mode on the ports is Auto.

However, before you enable 802.1X access authentication globally (see Manage 802.1X authentication on page 48), manually set the port authentication mode of the uplink port or ports to Authorized to enable the switch to keep its network connection and, if applicable, Internet connection.

To assign a port authentication mode to individual ports:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

The local device password is the password that you set up when you first logged in to the CLI.

The Overview page displays.

4. Select **Configure > Security**.
   The Security page displays.
5. Select the ports to which you want to assign a port authentication mode.
   To select all ports, select the **Select All Ports** check box.
6. From the menu below the graphical display, select the authentication mode for the selected ports:
   - **Auto**: The authenticator port access entity (PAE) sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. This is the default setting.
   - **Force-Authorized**: The authenticator PAE unconditionally sets the controlled port to authorized.
   - **Force-Unauthorized**: The authenticator PAE unconditionally sets the controlled port to unauthorized.
7. Click the **Apply** button.
   Your settings are saved.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Manage 802.1X authentication

If you enable 802.1X access authentication, port authentication is performed by a RADIUS server. If you disable 802.1X access authentication, port authentication is globally disabled and the switch allows traffic on any ports without authentication.

Note: Before you enable 802.1X access authentication globally, manually set the port authentication mode of the uplink port or ports to Authorized (see Manage port authentication for individual ports on page 47) to enable the switch to keep its network connection and, if applicable, Internet connection.

To manage 802.1X access authentication:

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

The login page displays.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Security**.
   The Security page displays.
5. In the RADIUS Server Settings section, do one of the following:
   - **Enable 802.1X access authentication**: Turn on the **802.1x Access Authentication** button so that it displays green and is positioned to the right.

     CAUTION: Before you enable 802.1X access authentication, manually set the port authentication mode of the uplink port or ports to Authorized (see Manage port authentication for individual ports on page 47).

   - **Disable 802.1X access authentication**: Turn off the **802.1x Access Authentication** button so that it displays gray and is positioned to the left. This is the default setting.
6. Click the **Apply** button.
   Your settings are saved.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove port authentication from individual ports

After you remove port authentication form a port, the switch allows traffic on the port without authentication.

To remove port authentication mode from individual ports:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.

4. Select **Configure > Security**.

   The Security page displays.

5. Select the ports from which you want to remove port authentication.

   To select all ports, select the **Select All Ports** check box.

6. Click the **Remove Port Authentication** button.
7. Click the **Apply** button.

   Your settings are saved.

8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

RADIUS servers

RADIUS servers provide additional security for networks. A RADIUS server maintains a user database, which can contain per-user or per-port authentication information. The switch passes information to the configured RADIUS server, which can authenticate a user name and password or port and password before authorizing use of the network.

Configure the basic settings for a RADIUS server

After you enable 802.1X access authentication globally (see Manage 802.1X authentication on page 48), you can configure one or more RADIUS servers.

The CLI lets you manage extensive RADIUS settings. For more information, see the CLI reference manual, which you can download by visiting netgear.com/support/download.

To configure the basic settings for a RADIUS server:

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

   The login page displays.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.

4. Select **Configure > Security**.

   The Security page displays.

5. In the RADIUS Server Settings section, do one of the following:

   - **Add a new RADIUS server**: To add the settings for a new RADIUS server, click the **+ Add Server** link.
   - **Change a RADIUS server**: To change the settings for a RADIUS server that you previously added, click the server link, for example, **Server1** or **Server2**.

6. Configure the settings for the RADIUS server in the following fields:

   - **RADIUS Address**: The IP address of the RADIUS server. The switch must be able to reach this IP address.
     You cannot change the IP address for a RADIUS server that you previously added.
   - **Port Number**: The UDP port number used to reach the RADIUS server. The default is port 1812. You can specify a custom port in the range from 1 to 65535.
   - **Secret Key**: The secret key is the password for authentication and encryption of all RADIUS communications between the switch and the RADIUS server. This password must match the one that is configured on the RADIUS server.
     You cannot change the secret key for a RADIUS server that you previously added.

7. Click the **Apply** button.

   Your settings are saved.

8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Remove a RADIUS server

You can remove a RADIUS server that you no longer need.

To remove the settings for a RADIUS server:

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

The login page displays.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.

4. Select **Configure > Security**.
   The Security page displays.

5. In the RADIUS Server Settings section, next to the server, click the **x**.
   For example, to remove the second RADIUS server that you added, click the **x** next to Server2 .

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

7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

7

Manage and monitor the switch

The chapter contains the following sections:

For information about all management and monitoring options of the switch, see the CLI reference manual, which you can download by visiting netgear.com/support/download.

Update the firmware

You can update the firmware through the AV UI.

You can update the firmware for the switch image only, for example, QNOS-m4500-48xf8c-7.0.2.5.deb. That is, you cannot update the firmware that combines the switch image and Linux OS.

To update the firmware:

1. Download the firmware file to the computer that you use to access the AV UI.
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. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
5. Select **Configure > Maintenance**.
   The Maintenance page displays.

   Note: The switch can hold two firmware versions. If it does, the page displays the active firmware version. The CLI lets you manage firmware files, and change from one version to another. The AV UI lets you update the firmware but does not let you manage firmware versions. If you update firmware using the AV UI, the new firmware becomes the active firmware.

6. Click in the **Browse Field** field, navigate to the firmware file, and select it.
7. Click the **Upload** button.
   A pop-up window displays the progress of the firmware file upload.
8. After the upload completes, in the pop-up window, click the **Reboot Now** button.
   The firmware upgrade process starts. During the firmware upgrade, do not power down the switch. The switch reboots and restart with the new firmware version. When the process is complete, you can log in again to the AV UI.

Startup configuration

You can manage the startup configuration, that is, the startup-config file. You can do the following:

- Save the running configuration to the startup configuration.
- Download the running configuration file.
- Restore the running and startup configurations from a previously downloaded configuration file.

Save the running configuration

After you make changes on a page of the AV UI and click the **Apply** button (or, in some windows, the **Save** button), your changes are saved for the current session, but are not retained when you restart the switch. That is, your running configuration is not saved to the startup configuration (the startup-config file).

Note: The idle time-out period for an AV UI session is five minutes. However, if you are automatically logged out of the AV UI and then log in again, the running configuration is not lost and you can save it to the startup configuration.

To save the running configuration to the startup configuration:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. At the top of the page, click the **Save** icon or text.
   The running configuration is saved to the startup configuration.

Download the running configuration

You can download the running configuration (that is, the current configuration) to a computer. If you do so, you can restore both the running configuration and startup configuration from your saved configuration file.

To download the running configuration:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.
4. Select **Configure > Maintenance**.
   The Maintenance page displays.
5. In the Configuration Management section, click the **Download Configuration** button.
   A pop-up window displays.
6. Navigate to a location on your computer and save the text file.
   The file is saved with a `.cfg` extension.

Restore the configuration

If you downloaded the configuration to a computer (see Download the running configuration on page 55), you can restore both the running configuration and startup configuration from your saved configuration file.

To restore the configuration:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.
4. Select **Configure > Maintenance**.
   The Maintenance page displays.
5. In the Configuration Management section, click in the **Browse File** field.

A pop-up window displays.

6. Navigate to and select the saved configuration file.
   The file has a `.cfg` extension.
7. Click the **Upload** button.
   A pop-up window displays.
8. Click the **Restore Now** button.
   The running configuration and startup configuration are restored.

Manually set the date and time

You can manually set the date and time for the switch.

To manually set the date and time:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.
4. In the Device Details section, below the Date & Time field, click the **pencil** icon.
   The Time Configuration window displays.
5. Click in the **Date** field, and from the pop-up calendar, select a date.
6. Click in the **Time** field, use the menus to select the hour, minutes, seconds, and meridian setting, and click the **OK** button.
7. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Add a system name

You can add a system name, which allows you and others to identify the switch in the network. By default, no system name is configured.

To add a system name:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. In the Device Details section, below the System Name field, click the **pencil** icon.
   The Edit System Name window displays.
5. In the **New System Name** field, specify a system name.
6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

OOB port IP address

The OOB port, also referred to as the IPv4 service port, is a dedicated Ethernet port for out-of-band (OOB) management of the switch. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.

By default, no IP address is set for the OOB port, but its DHCP client is enabled so that the port can receive an IP address from a DHCP server in your network.

You can also set a fixed IP address for the OOB port.

Set a fixed IP address for the OOB port

By default, no IP address is set for the OOB port and the DHCP client is enabled. You can disable the DHCP client for the OOB port and set a fixed (static) IP address.

To set a fixed IP address for the OOB port:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. In the Device Details section, below the OOB IP Address field, click the **pencil** icon.
   The Edit OOB IP Address window displays.
5. From the **OOB IP Settings** menu, select **Static** and specify the following settings:
   - **OOB IP Address**: The static IP address for the OOB port. By default, no IP address is set for the OOB port.
   - **Subnet Mask**: The IP subnet mask for the OOB port. By default, no subnet mask is set for the OOB port.
   - **Default Gateway**: The gateway through which the OOB port can be reached. By default, no IP address is set for the default gateway.

   WARNING: If you are logged in to switch over the OOB port, when you click the **Apply** button, you are disconnected and need to log in to the switch at the new IP address.
6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Enable the DHCP client for the OOB port

By default, the DHCP client for the OOB port is enabled.

If you set a fixed IP address for the OOB port, the DHCP client is disabled. You can enable the DHCP client again.

To enable the DHCP client for the OOB port:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. In the Device Details section, below the OOB IP Address field, click the **pencil** icon.
   The Edit OOB IP Address window displays.
5. From the **OOB IP Settings** menu, select **DHCP Client**.

   WARNING: If you are logged in to switch over the OOB port, when you click the **Apply** button, you are disconnected and need to log in to the switch at the new IP address that is assigned by the DHCP server. If you do not know the new IP address, determine it by accessing the DHCP server or by using an IP scanner utility.

6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Set the STP network redundancy for the switch

You can set the Spanning Tree Protocol (STP) network redundancy for the switch. This is also referred to as the bridge priority, which is the priority for a multiple spanning tree (MST) instance on the switch.

When switches or bridges are running STP, each is assigned a priority. After exchanging bridge protocol data units (BPDUs), the switch with the lowest priority value becomes the root bridge and the other devices become backup or redundant bridges. The bridge priority is a multiple of 4096. The range is from 0 to 61440. The default is 32768.

Table 1. STP network redundancy in the AV UI

Configurable Setting in the AV UI	Associated Bridge Priority Value in the AV UI
Primary mode	0
Neutral mode	32768
Backup mode	61440

You can set the STP network redundancy to Primary mode, Neutral mode, or Backup mode.

To set the STP network redundancy for the switch:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. In the Device Details section, below to the STP Network Redundancy field, click the **pencil** icon.
   The Edit STP Network Redundancy window displays.
5. Select the **Primary mode**, **Neutral mode**, or **Backup** radio button.
   By default, the Neutral mode radio button is selected.
6. Click the **Apply** button.
   Your settings are saved. The window closes. The Overview page displays again.
7. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Restart the switch from the AV UI

You can restart the switch from the AV UI.

To restart the switch:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. At the top of the page, click the **Reboot** icon or text.
   A pop-up window displays a warning.
5. Click the **Yes** button.
   The switch restarts. During the restart process, do not power down the switch.

Reset the switch to factory default settings

You can reset the switch to factory default settings. This process erases all your custom settings, including your network profile assignments and any custom profile templates.

To reset the switch to factory default settings:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Configure > Maintenance**.
   The Maintenance page displays.

5. Click the **Factory Default** button.
   A pop-up window displays a warning.

   CAUTION: This process erases all your custom settings, including your network profile assignments and any custom profile templates.

6. In the pop-up window, click the **Confirm** button.
   The factory default reset process starts. During the reset process, do not power down the switch. The switch reboots and restarts with factory default settings. When the process is complete, you can log in again to the AV UI, but you first might need to determine the IP address of the switch.

Display the status of the ports and switch

To display the status of the ports and switch:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.
4. To display detailed information about a port that is connected to a device, point to the port in the graphical display of the switch.
   A pop-up window displays information about multiple properties of the port.
5. If the port legends do not display below the graphical display of the switch, select the **Show Legends** check box.
   The following table describes the ports legend.

Legend	Description
Connected	The port is connected to a device that is powered up.
Error	An error occurred on the port.
Disabled	The port is disabled.

(Continued)

Legend	Description
Available	The port is not connected to a device but is available.
Blocked	The port is blocked. That is, STP blocked the port to prevent a loop.
Admin Down	The port is administratively down.
Warning	The port reached 98 percent of its ingress or egress transmit rate.
Force-Authorized	802.1X access authentication is enabled and the port authentication mode is Force-Authorized (see Port authentication on page 47).
Force-Unauthorized	802.1X access authentication is enabled and the port authentication mode is Force-Unauthorized (see Port authentication on page 47).
Authorized	802.1X access authentication is enabled and the port authentication status is Authorized.
Unauthorized	802.1X access authentication is enabled and the port authentication status is Unauthorized.
LAG	The port is member of a LAG (see Link Aggregation on page 26).
VLAN Trunk	The port functions as a VLAN trunk. That is, the port is a tagged port that processes tagged VLAN traffic.
Auto Trunk	The port functions as an Auto-Trunk (see Auto-Trunk overview on page 21).
Force Multicast	This port is configured for forced multicast (see Configure the multicast mode for one or more ports on page 35).
1G SFP Fiber Port	Depending on the switch model, the port is a 1G SFP fiber port that can accept an SFP transceiver module.
10G SFP+ Fiber Port	Depending on the switch model, the port is a 10G SFP+ fiber port that can accept an SFP or SFP+ transceiver module.
25G SFP28 Fiber Port	Depending on the switch model, the port is a 25G SFP28 fiber port that can accept an SFP28 transceiver module.
100G QSFP28 Fiber Port	Depending on the switch model, the port is a 100G QSFP28 fiber port that can accept an QSFP28 transceiver module.
Creston Device Connected	Depending on the switch model, a Creston device is connected to the port.

(Continued)

Legend	Description
Visionary Device Connected	Depending on the switch model, a Visionary device is connected to the port.
NUCLEUS Device Connected	Depending on the switch model, a NUCLEUS device is connected to the port.

For more information about the ports, see Display detailed information about the physical ports and LAGs on page 44.

The following table describes the information that displays in the Device Details section, Configured Profiles section, CPU Utilization graph, Memory Utilization graph, and Fans & Temperature section.

Field or Graph	Description
Device Details	
Product Name	M4500 by default. This field is fixed.
Serial Number	The serial number of the switch. This field is fixed.
Model	The model number of the switch. This field is fixed.
Date & Time	The configured date and time (see Manually set the date and time on page 57).
Country/Region	This field does not apply to the switch (N/A).
Base MAC Address	The MAC address of the switch. This field is fixed.
System Name	The configured system name, if any (see Add a system name on page 58).
Firmware Version	The active main firmware version of the switch (see Update the firmware on page 54).
AV UI Version	The active firmware version for the AV UI. This firmware is included in the main firmware.
Boot Version	The active boot version of the switch. This firmware is included in the main firmware.
System Uptime	The period in days, hours, minutes, and seconds since the switch was last started.
OOB IP Address	The IP address for access to the AV UI over the out-of-band (OOB) port of the switch (see OOB port IP address on page 58). (This port is also referred to as the service port.)

(Continued)

Field or Graph	Description
STP Network Redundancy	The configured STP network redundancy mode of the switch (see Set the STP network redundancy for the switch on page 60).
Configured Profiles For more information about network profiles, see Network profiles on page 14.	
Profile Name	The name of the network profile.
Profile Type	The profile template on which the network profile is based. The profile template can be any of the preconfigured profile template (for example, Data or Video, see Overview of preconfigured AV profile templates on page 12) or a custom profile template (see Custom AV profile templates on page 18).
VLAN ID	The VLAN ID that is assigned to the network profile.
IP Address	The IP address that is assigned to the network profile.
# of Assigned Ports	The number of ports that are assigned to the network profile.
CPU Utilization	The CPU utilization as a percentage of the CPU capacity.
Memory Utilization	The memory utilization as a percentage of the total memory.
Fans & Temperature	The number of internal fans depends on the switch model. The state of the fan must be Active. If the state is not Active, there might be a problem with the fan and the cooling.

Display the neighboring devices

You can display the devices that are connected to the switch.

To display the neighboring devices:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.

The local device password is the password that you set up when you first logged in to the CLI.

The Overview page displays.

4. Select **Configure > Neighbor**.

   The Neighbor page displays.

   For each detected device, the page displays the following:

   - **Port**: The port to which the device is attached.
   - **Host**: The system name of the device, if any.
   - **MAC Address**: The MAC address of the device.
   - **VLAN ID**: The VLAN ID of the port to which the device is attached.
   - **IP Address**: The IP address of the device.
   - **Remote Port ID**: The port number of the device.

8

Diagnostics and Troubleshooting

You can diagnose and troubleshoot the switch and its network.

The chapter contains the following sections:

Manage the switch log, console log, and command log

The switch generates messages in response to events, faults, and errors as well as changes in the configuration or other occurrences. These messages are stored locally and can be forwarded to one or more centralized points of collection for monitoring purposes or long-term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

To configure a syslog server and set up remote logging, use the CLI. For more information, see the CLI command reference manual, which you can download by visiting netgear.com/support/download.

By default, the switch log is enabled at the Notice logging level but the console log and command log are disabled.

To manage the switch log, console log, and command log that are stored locally:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Diagnostics > Logs**.
   The Logs page displays.
5. In the Log Settings section enable or disable logs by doing the following for each individual log:
   - **Enable one or more logs**: Click the **Switch Logging** button, **Console Logging** button, **Command Logging** button, or a combination of these buttons so that they turn green.
   - **Disable one or more logs**: Click the **Switch Logging** button, **Console Logging** button, **Command Logging** button, or a combination of these buttons so that they turn gray.

   By default, the switch log, console log, and command log are enabled.

6. For the switch log and the console log individually, in the Log Settings section, select the logging level from the **Switch Logging Level** menu or the **Console Logging Level** menu:
   - **Emergency**: Level 0, the system is unusable.
   - **Alert**: Level 1, action must be taken immediately.
   - **Critical**: Level 2, critical conditions.
   - **Error**: Level 3, error conditions. If you enable console logging, this is the default level.
   - **Warning**: Level 4, warning conditions.
   - **Notice**: Level 5, normal but significant conditions.
   - **Informational**: Level 6, informational messages. This is the default level for switch logging.
   - **Debug**: Level 7, debug-level messages.

   Note: A log records messages equal to or above the selected severity level. For example, if you select the **Warning** level from the menu, the switch records messages at the Warning, Error, Critical, Alert, and Emergency levels.

7. Click the **Apply** button.
   Your settings are saved.
8. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Display or download the message log

You can display or download the message log.

To display or download the message log:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.

4. Select **Diagnostics > Logs**.
   The Logs page displays. The Logs section shows the recorded log entries.
5. To download the logs, do the following:
   a. Click the **Download Logs** link.
      A pop-up window displays.
   b. Navigate to a location on your computer and save the file.

Display or clear the port statistics

You can display or clear the port statistics.

To display or clear the port statistics:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.
4. Select **Diagnostics > Port Statistics**.
   The Port Statistics page displays.
   The Inbound Traffic table displays detailed information about the inbound traffic on each port and LAG. The separate Outbound Traffic table displays detailed information about the outbound traffic on each port and LAG.

Table 2. Inbound traffic

Legend	Description
Port	The port or LAG to which the statistics apply.
InOctets	The number of inbound octets (bytes).
InUcastPkts	The number of inbound unicast packets.
InMcastPkts	The number of inbound multicast packets.

Table 2. Inbound traffic (Continued)

Legend	Description
InBcastPkts	The number of inbound broadcast packets.
InDropPkts	The number of inbound packets that were dropped.
InBitRate	The bit rate for inbound traffic.
rxError	The number of received packets with errors.

Table 3. Outbound traffic

Legend	Description
Port	The port or LAG to which the statistics apply.
OutOctets	The number of outbound octets (bytes).
OutUcastPkts	The number of outbound unicast packets.
OutMcastPkts	The number of outbound multicast packets.
OutBcastPkts	The number of outbound broadcast packets.
OutDropPkts	The number of outbound packets that were dropped.
OutBitRate	The bit rate for outbound traffic.
txError	The number of transmitted packets with errors.

5. To clear all statistics, click the **Clear all statistics** link above the table.
   A pop-up window displays a warning.
6. Click the **Delete** button.
   The port statistics counters are reset to zero.

Send a ping, traceroute, or DNS lookup request to an IP address or host name

You can you take the following actions independently of each other or simultaneously (or rather, one after the other):

- **Send a ping**: The switch sends a fixed number of ping requests to a particular IP device to determine if it can communicate with the device.
- **Send a traceroute**: The switch attempts to trace the route to a particular IP device to determine the precise path to the device.
- **Send a DNS lookup request**: The switch contacts DNS servers to determine the IP address that is associated with a host name.

When you run one or more tests, the test results are displayed in the panes onscreen.

To send a ping, traceroute, or DNS lookup request to an IP address or host name:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Diagnostics > Troubleshoot**.
   The Troubleshoot page displays.
5. In the **IP Address/Host Name** field, specify the IP address or host name.
6. Do one or more of the following:
   - **Ping**: To ping the IP address or host name, turn on the **Ping** toggle so that it displays green and is positioned to the right.
   - **Traceroute**: To send a traceroute to the IP address or host name, turn on the **Traceroute** toggle so that it displays green and is positioned to the right.
   - **DNS Lookup**: To send a DNS lookup to a host name, turn on the **DNS Lookup** toggle so that it displays green and is positioned to the right.
7. Click the **Run Tests** button.

The selected tests run one after the other. The results display in the result panes.

Configure port mirroring

Port mirroring lets you select the network traffic of specific switch ports for analysis by a network analyzer. You can select many switch ports as source ports but only a single switch port as the destination port.

A packet that is copied to the destination port is in the same format as the original packet. That means that if the mirror is copying an incoming packet, the copied packet is VLAN-tagged or untagged as it was received on the source port. If the mirror is copying an outgoing packet, the copied packet is VLAN-tagged or untagged as it is being transmitted on the source port.

To configure port mirroring:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Diagnostics > Port Mirroring**.
   The Port Mirroring page displays.
5. Click the **Port Mirroring** toggle so that it displays green and is positioned to the right.
   The page shows two graphical displays of the switch.
6. In the upper graphical display, select one or more source ports.
7. In the lower graphical display, select a single destination port.
8. Click the **Apply** button.
   Your settings are saved.
9. To save the settings to the running configuration, at the top of the page, click the **Save** icon or text.

Access the CLI through the terminal in the AV UI

You can access the command-line interface (CLI) from the AV UI. While you work in the CLI, the AV UI can remain open.

To access the CLI from the AV UI:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.
   The Overview page displays.
4. Select **Diagnostics > Terminal**.
   Depending on how you configured your browser, the CLI opens in a new browser tab or browser window.

Download diagnostics files for technical support

NETGEAR technical support might request diagnostic files from your switch. Such files might help troubleshooting a problem. The combined diagnostic files might include the following information:

- Configuration file
- Buffered log
- Tech support file
- Crash logs
- Full memory dump
- Supported MIBs

Please do not send files unless instructed to do so by NETGEAR technical support.

To download the combined diagnostics files in a text file:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.
   The login page displays.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter your local device password, and click the **AV UI Login** button.
   The local device password is the password that you set up when you first logged in to the CLI.

   The Overview page displays.
4. Select **Diagnostics > Support Diagnostics**.
   The Support Diagnostics page displays.
5. Click the **Download Files** link.
   A pop-up window displays.
6. Navigate to a location on your computer and save the text file.