NETGEAR®

Config Example Guide

Configuration Example Guide for ProAV Installations

March 2026
202-12836-03

NETGEAR, Inc.
3553 N. First Street
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/.

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

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

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-12836-03	March 2026	We made revisions to the following section: • Optional step: Contact the NETGEAR Pro AV Design support team on page 111
202-12836-02	January 2026	Added new network profile limitations. • Network profile limitations on page 14
202-12836-01	July 2025	First publication.

Contents

1

Introduction

This Configuration Example Guide for ProAV is for the Fully Managed Switches M4250, M4300, M4350, and M4500 Series and covers all M4250, M4300, M4350, and M4500 switch models. The guide also describes select configuration examples for the Pro Router model PR460X and the WBE718 and WBE758 access points.

This guide is specifically for ProAV installations (as opposed to IT installations). The guide provides selected configuration examples for the NETGEAR Engage Controller UI and the Audio-Video (AV) UI that is accessible from the Engage Controller UI. In addition, the guide provides some background information about ProAV configuration options.

In this guide, we refer to the NETGEAR Engage Controller as the *controller*.

In this guide and in the Engage Controller user interface (UI), we often refer to topologies with *core* and *edge* switches, but you could also call switches with such as function *spine* and *leaf* switches. The terms *core* and *spine* are interchangeable and the terms *edge* and *leaf* are interchangeable.

The chapter includes the following sections:

Note: For more information about the topics that are covered in this manual, visit the support website at netgear.com/support, enter your model number in the search box, and then select your product.

Documentation and training modules

NETGEAR ProAV documentation and training modules are available:

- Engage controller: netgear.com/support/product/engage-controller/#docs
- M4250 series switches: netgear.com/support/product/m4250/#docs
- M4300 series switches: netgear.com/support/product/m4300/#docs
- M4350 series switches: netgear.com/support/product/m4350/#docs
- M4500 series switches: netgear.com/support/product/m4500/#docs
- PR460X Pro Router: netgear.com/support/product/pr460x/#docs
- WBE718 access point: netgear.com/support/product/wbe718/#docs
- WBE758 access point: netgear.com/support/product/wbe758/#docs
- Tech Guides: netgear.com/hub/business/av/av-tech-guides
- ProAV training modules: academy.netgear.com
- Webinars, including ProAV webinars: netgear.com/about/webinars
- ProAV catalog: downloads.netgear.com/files/netgear/pdfs/NETGEAR_ProAV_Catalog.pdf
- AV Resources Center: netgear.com/business/solutions/proav-resources

Network considerations

When you plan a network, you need to find out the requirements: How essential is quality, or is some latency tolerated? How much bandwidth is required to support the traffic at the quality that you need?

The following sections discuss these topics.

Consider video compression, latency, quality, and bandwidth

When you plan a network, consider the relationship between video compression, latency, quality, and bandwidth.

For example, the highest quality and lowest latency is required for a live broadcast to larger TVs or a video wall where video magnification (zoom in) is required; lower quality and more latency might be acceptable for video streaming to mobile phones, tablets, and laptops, where the screens are smaller.

Ideally, your equipment and connection speed support a lot of bandwidth for high quality, no latency, and no compression. However, often you must find an acceptable compromise between the various components, for example, if your equipment or connection speed support only a limited amount of bandwidth.

The following figure shows the relation between video compression, latency, video quality, and bandwidth.

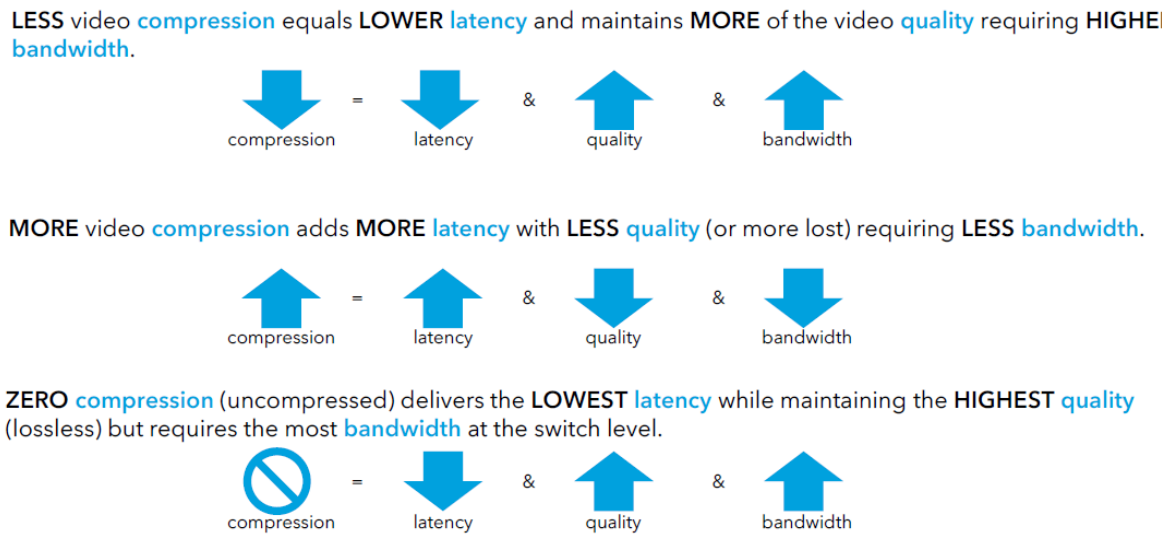


Figure 1. Video compression, latency, quality, and bandwidth

For the individual components, the relationship means the following:

- **Video compression**:
  - **Less compression**: Lower latency, better quality, more bandwidth
  - **More compression**: Higher latency, lower quality, less bandwidth
  - **No compression**: *Lowest latency, highest quality, most bandwidth*
- **Acceptable latency**:
  - **Lower latency**: Less compression, better quality, more bandwidth
  - **Higher latency**: More compression, lower quality, less bandwidth
  - **Lowest latency**: *No compression, highest quality, most bandwidth*
- **Required or acceptable quality**:

  - **Lower quality**: More compression, higher latency, less bandwidth
  - **Higher quality**: Less compression, lower latency, more bandwidth
  - **Highest quality**: *No compression, lowest latency, most bandwidth*
- **Available bandwidth**:
  - **Less bandwidth**: More compression, higher latency, lower quality
  - **More bandwidth**: Less compression, lower latency, better quality
  - **Most bandwidth**: *No compression, lowest latency, highest quality*

Consider the required bandwidth

When you plan a network, consider the required bandwidth per switch and switch uplink.

For example, model M4250-26G4XF-PoE+ is a switch with twenty-six 1GBASE-T ports and four 10G SFP+ fiber uplink ports. This switch can use 26 Gbps (26 x 1 Gbps), so you need sufficient bandwidth for non-blocking traffic transfer. In this situation, you would use the four 10G SFP+ fiber uplink ports as a LAG, which gives you 40 Gbps non-blocking traffic transfer.

Take into consideration that all transmitters and receivers can be active simultaneously. For example, in the following figures:

- Switch 1 has three 1G transmitters and four 1G receivers: a throughput of at least 7G is required.
- Switch 2 has no transmitters but six 1G receivers: a throughput of at least 6G is required.

If you connect Switch 1 to Switch 2 over a 1G connection, you end up with insufficient bandwidth to cover the traffic between the switches.

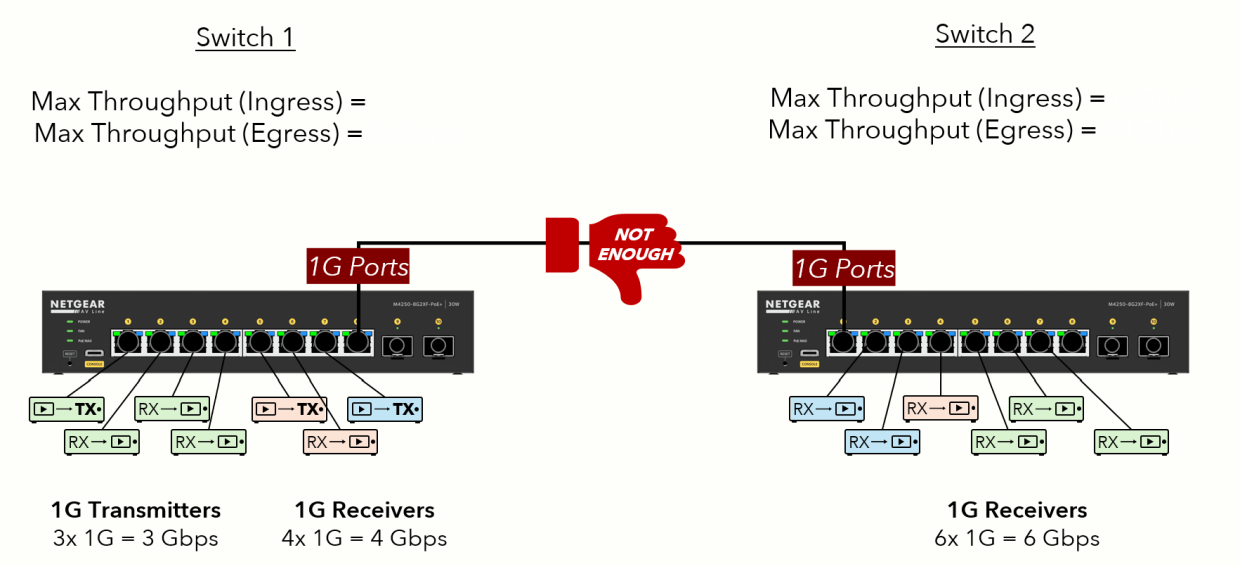


Figure 2. Insufficient bandwidth

However, if you connect the switches over a 10G connection using a SFP port on each switch, there is sufficient bandwidth to cover the traffic.

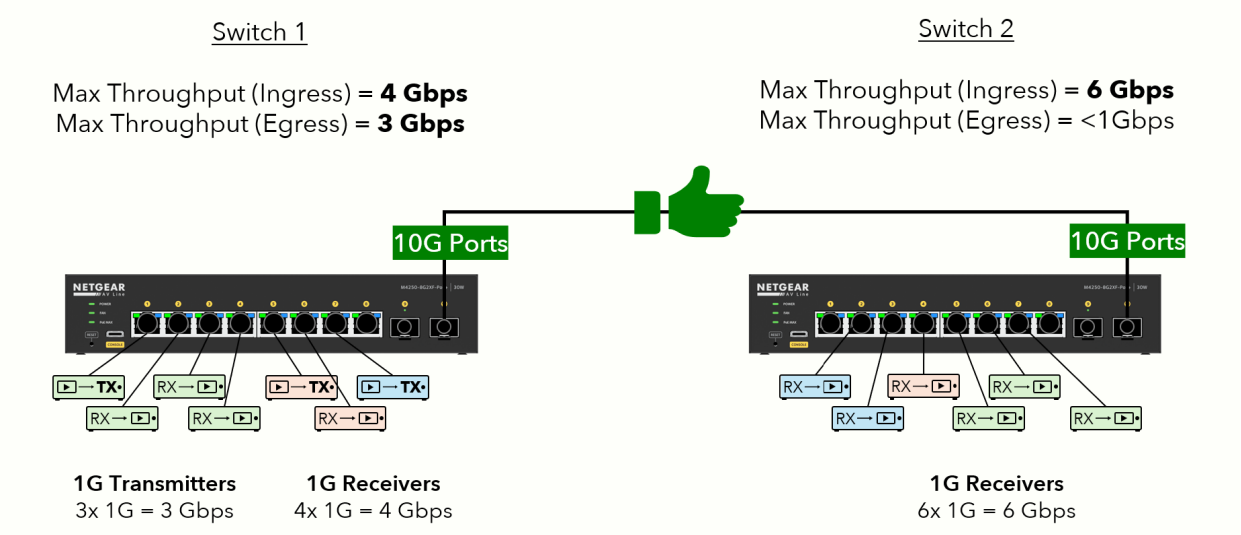


Figure 3. Sufficient bandwidth

Use the same type of calculations for your uplink traffic to a core switch.

2

AV profile templates, network profiles, and VLANs

Examples of provisioning network profiles are provided in the NETGEAR Tech Guides that are listed below. This chapter provides concept and example task sections that are related to network profiles.

The chapter includes the following sections:

- About AV profile templates, network profiles, and VLANs
- How you can display the default settings of a network profile
- Quality of Service
- Which major profiles can co-exist in a mix-and-match environment
- Network profile limitations
- Configure an SMPTE broadcast network with a core switch and three edge switches
- Change the priority for a clock

The following profile template related Tech Guides are available at the NETGEAR ProAV site at Provisioning AV profiles in Engage
Dante
AES67
Audio and Video Over IP
Audio Over IP and Lighting
Audio Video AVB
VLANs For Different Types of AV Over IP

About AV profile templates, network profiles, and VLANs

The controller and onboarded fully managed switches provide preconfigured audio-video (AV) profile templates that you can configure and assign to switch ports and VLANs at a site, thereby creating network profiles.

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

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

  By default, VLAN routing (layer 3 IP routing) is disabled for a network profile (VLAN) at a site. The exception is the management VLAN for the site, which is the VLAN for the default network profile. For more information about VLAN routing, see VLAN routing on page 24.

For information about the supported AV profile templates, see the "Overview of preconfigured AV profile templates " section in the NETGEAR Engage Controller User Manual.

How you can display the default settings of a network profile

The default settings of a profile template include the setting for multiple features, including the following:

- Fast leave
- IGMP or MLD Querier
- QoS
- Multicast
- Auto-Trunk
- Auto-LAG
- L2 CoS or L3 DSCP and queue assignments

- PTP
- Clock settings
- Discovery protocols

We do not publish the default settings for each profile template because it would be highly complex and time-consuming to configure the settings in the main UI and even more so in the CLI. The AV UI and Engage UI are the preferred methods to enable and configure a network profile for a specific environment.

However, you can access the CLI and display the settings for a network profile:

1. In the controller, go to the Managed Devices page
2. For the switch for which you want to display information, click the **3 dots** icon, and select **Launch Terminal**.
3. Log in to the CLI, go to Privileged EXEC mode, and enter the **show run** command to display all settings of a configured network profile.

Quality of Service

Our Quality of Service (QoS) strategy is designed to combine different protocols, where timing, reliability, and stability are critical. Rather than relying solely on standard traffic markings, we use a combination of traffic classification methods to ensure optimal performance across different AV protocols.

- **Time-sensitive traffic**: Prioritized using unique identifiers such as destination addresses, which ensures precise clock synchronization even in diverse environments.
- **Audio and video streams**: Classified by traffic type to guarantee low latency and high reliability during transmission.
- **Control and management traffic**: Handled separately to maintain responsiveness and operational efficiency.
- **AVB traffic**: Prioritized using standards-based Layer 2 mechanisms for full protocol compatibility.

This approach allows us to maintain consistent and predictable performance across all AV protocols and systems, regardless of the underlying transport or manufacturer-specific implementations.

We do not publish the QoS default settings for a profile template because it would be highly complex and time-consuming to configure the settings in the main UI and even more so in the CLI. The AV UI and Engage UI are the preferred methods to enable and configure a network profile for a specific environment, which automatically results in specific QoS settings.

However, you can access the CLI and display the QoS settings for a profile template:

1. In the controller, go to the Managed Devices page
2. For the switch for which you want to display information, click the **3 dots** icon, and select **Launch Terminal**.
3. Log in to the CLI, go to Privileged EXEC mode, and enter the **show run** command to display all settings of a configured network profile.

You cannot adjust the QoS settings in the AV UI and Engage UI. You can do so in the main UI and CLI, but we recommend that you do so only if you understand the consequences of the changes that you intend to make. For more information, see the (main) user manual and the CLI command reference manual for your switch model.

Note: If you make too many QoS or other changes to a profile and contact us for assistance, we might not be able to provide assistance. We might ask you to remove your custom changes and revert to the profile template. After all, each profile template is *certified by the manufacturer*.

Which major profiles can co-exist in a mix-and-match environment

In an environment with audio and video devices from a variety of vendors, you can select different profiles on the same switch or even on the same VLAN that is supported on multiple switches. The following table shows how the major network profiles can function together.

As a general guideline, if your network consists of up to 200 devices, you can use the same VLAN for multiple devices. For a network with more than 200 devices, we recommend that you set up different VLANs.

Coexisting Profiles	Audio Video AVB	AES67	Dante	Video with jumbo frames	Q-SYS
Audio Video AVB	Yes	**No**	Yes	**No**	**No**
AES67[1]	**No**	Yes	Yes	Yes	Yes
Dante[2]	Yes	Yes	Yes	Yes	Yes
Video with jumbo frames[3]	**No**	Yes	Yes	Yes	Yes
Q-SYS[4]	**No**	Yes	Yes	Yes	Yes

Table notes:

[1] **AES67**: Refers to three network profiles: *Audio AES67*, *Video NDI5 / NDI6 with Dante, Q-Sys and AES67 audio* and *Video with AES67 audio*.

[2] **Dante**: Refers to three network profiles: *Audio Dante*, *Video NDI5 / NDI6 with Dante, Q-Sys or AES67 audio*, and *Video with Dante audio*. Dante generally works well with Audio Video AVB, but we do recommended that you use 10G uplinks in a configuration with multiple switches.

[3] **Video with jumbo frames**: Refers to any type of video network profile that uses jumbo frames. AVB and video that uses jumbo frames does not work in a configuration with multiple switches. However, it might work on a single switch.

[4] **Q-SYS**: Refers to three network profiles: *Audio Q-SYS*, *Video NDI5 / NDI6 with Dante, Q-SYS or AES67 audio*, and *Video with Q-SYS audio*.

Network profile limitations

The following table lists network profile limitations, problems and solutions, and requirements.

Network profile	Hardware or software (if applicable)	Limitation, problem, or requirement	Solution (if applicable) or notes
Allen & Heath gigaACE/TGX	--	Packets are dropped	In a configuration with multiple switches, use the AV UI to disable broadcast storm control on the uplink port.
Audio AES67	Dante device	PTP-TC and PTPv2 must be enabled	--
Audio Q-SYS	--	The MTU must be 1500	--
	--	PTP-TC must be enabled	--
Audio Video AVB	--	No AES67	The reason why Audio Video AVB and AES67 cannot function together is that gPTP conflicts do occur with PTPv2. (AVB is incompatible with PTP-TC.)
	--	Jumbo frames are not supported	--
	M4300 and M4500 series switches	Not supported	Use M4250 and M4350 series switches
Blustream Multicast	ACM210	Video port cannot be routed across VLANs.	Only the control port can be routed

(Continued)

Network profile	Hardware or software (if applicable)	Limitation, problem, or requirement	Solution (if applicable) or notes
Crestron DigitalMedia AV Network	CP4N 4-Series Control System	The CP4N does not support multicast.	On the NETGEAR switch, use the AV UI to block multicast traffic from going to the CP4N.
	CP4N 4-Series Control System	You can use the default gateway only for the control port.	Add a second USB Ethernet port that you can configure with the non-default gateway IP address settings.
	PRO4 4-Series Control System	The PRO4 sends IGMP queries, causing the connected switch port to be flooded with multicast traffic.	Blocking the multicast traffic does not resolve the situation. Instead, isolate the PRO4 in a separate VLAN.
Data	--	PTP-TC is not supported	--
	CobraNet	IGMP join and leave messages do not work	CobraNet can be supported on the Data VLAN and on one other VLAN that is not VLAN 1. Disable broadcast storm control.
G&D KVM-over-IP	G&D Control Center	Control Center does not provide a link-up if the port is not manually set to 1G	On the NETGEAR switch, use the AV UI to set the port to 1Gbps manually. Select Port Configuration. On the Port Configuration page, select the port. Disable Autonegotiation on the port and set the speed to 1000 / 1Gbps.
Lighting	--	PTP-TC is not supported	--
NUCLEUS Converged AV Network	--	PTP-TC is not supported	--
Poly StudioNet Modular Room	Applicable only to Poly G62 LLN	This profile is intended to extend the number of LLN ports, as there are limited number of ports available on the hardware. LLN utilizes a proprietary Poly CODEC, so this profile is only compatible with the G62 LLN.	If the Poly hardware is not a G62 LLN, use the Dante profile instead.

(Continued)

Network profile	Hardware or software (if applicable)	Limitation, problem, or requirement	Solution (if applicable) or notes
Shure Converged Audio and Control Network and Shure Split Audio and Control Network	--	You can configure only one network profile, not multiple	--
	--	Address problems occur on an Apple Mac that uses a link-local IP address	Broadcast the discovery packets by adding a MAC filter for the address 239.255.254.253 / 01:00:5e:7f:fe:fd You can use the switch main UI to add a MAC filter (in the main UI, select Security > Traffic Control > MAC filter).
Sonos	--	PTP-TC is not supported	--
Video	--	PTP-TC is not supported	--
Video NDI4	--	Requires flow control	--
	--	PTP-TC is not supported	--
Visionary AV Network	Multiple devices	Visionary AV Network devices have a LAN 2 port that supports low PoE passthrough, as well as networking for control or other devices	If required in other VLANs than VLAN 1, tag the VLANs on the LAN 2 port to differentiate between low PoE passthrough traffic and networking and control traffic.
	--	PTP-TC is not supported	--

Configure an SMPTE broadcast network with a core switch and three edge switches

For you to be able to configure an SMPTE broadcast network using the controller, your network must include one or more of the following M4350 series SMPTE-capable switches:

- M4350-8M2V (SKU MSM4310)
- M4350-16V4C (SKU VSM4320C)
- M4350-24F4X (SKU MSM4328F)
- M4350-24M4X4V (SKU MSM4332)
- M4350-40F4C (SKU XSM4344FC)
- M4350-40X4C (SKU XSM4344C)

The controller lets you configure the following SMPTE network profiles:

- **Audio Video SMPTE network profile**: If your network includes one or more M4350 series SMPTE-capable switches, you can use the Audio Video SMPTE network profile to connect AES67 Audio and ST 2110 Video devices and their controller. With this network profile, the PTPv2 boundary clock/grandmaster clock (BC/GM) settings are automatically enabled for all M4350 series SMPTE-capable switches that you use.
- **Hybrid SMPTE AES67 Core and Audio AES67 Edge network profile**: If your network includes one or more M4350 series SMPTE-capable switches *and other fully managed switch models*, you can use the Hybrid SMPTE AES67 Core and Audio AES67 Edge network profile, which does the following:
  - **Audio Video SMPTE**: Sets the Audio Video SMPTE network profile on the core switch (which must be a M4350 series SMPTE-capable switch) with PTPv2 BC/GM enabled.
  - **AES67 Audio**: Sets the AES67 Audio edge profile with PTP residency time stamping (also referred to as TC, for transparent clock) enabled on all other fully managed switches in the same VLAN.

  In the current firmware release of the controller, you can use the *Hybrid SMPTE AES67 Core and Audio AES67 Edge* profile template on the management VLAN only. That is, you change the profile on the management VLAN (by default, VLAN 1

with the name *default*) to the *Hybrid SMPTE AES67 Core and Audio AES67 Edge* profile template.

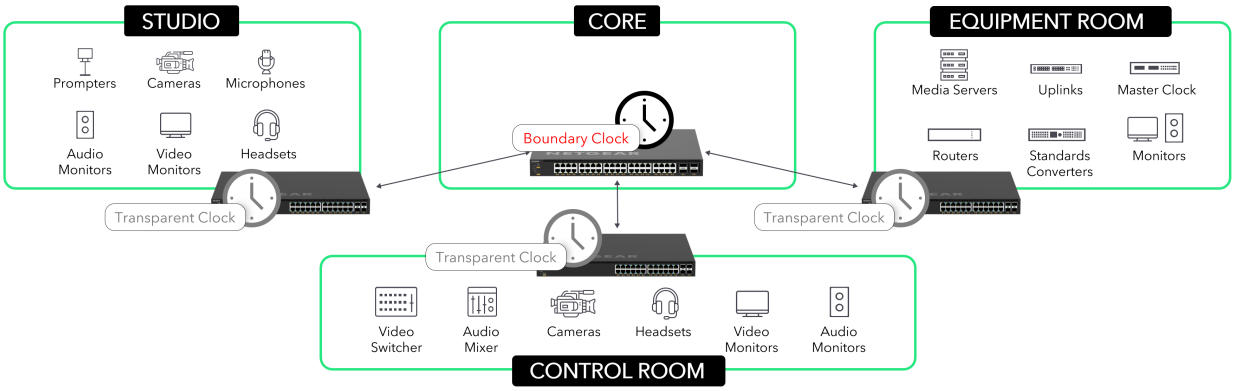


Figure 4. Broadcast network with a Hybrid SMPTE AES67 Core and Audio AES67 Edge network profile

In this example configuration, the network consist of the switches and port connections that are listed in the following table, and that are also used in the example configuration procedure.

Table 1. Switches and ports used in the example

Device	Model	Description
Router	PR460X	The router (which is not shown in the previous figure) has the following port connections: • **Port LAN5 WAN2**: 10G connection to the Internet. • **Port LAN4**: 10G connection to the Core switch.
Core switch	M4350-40X4C	This switch functions as the core switch and supports PTPv2 BC/GM with the Audio Video SMPTE network profile. The switch has the following port connections: • **Port 1**: 10G downlink to Edge 1 switch. • **Port 2**: 10G downlink to Edge 2 switch. • **Port 3**: 10G downlink to Edge 3 switch. • **Port 4**: 10G uplink to the router.
Edge switch 1	M4350-24X4V	This switch supports PTP-TC with the Audio AES67 network profile. The switch has the following port connections: • **Ports 1, 2, 3, 4, 5, and 6**: Access ports, each connected over 1G to an audio or video device in the studio. • **Port 25**: 10G uplink to the Core switch.

Table 1. Switches and ports used in the example (Continued)

Device	Model	Description
Edge switch 2	M4350-24X4V	This switch supports PTP-TC with the Audio AES67 network profile. The switch has the following port connections: • **Ports 1, 2, 3, 4, 5, and 6**: Access ports, each connected over 1G to an audio or video device in the studio. • **Port 25**: 10G uplink to the Core switch.
Edge switch 3	M4350-24X4V	This switch supports PTP-TC with the Audio AES67 network profile. The switch has the following port connections: • **Ports 1, 2, 3, 4, 5, and 6**: Access ports, each connected over 1G to an audio or video device in the studio. • **Port 25**: 10G uplink to the Core switch.

On the model M4350-40X4C switch and the three model M4350-24X4V+ switches, to change the management VLAN to a network profile based on the Hybrid SMPTE AES67 Core and Audio AES67 Edge profile template:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
4. Select **Site Settings**.

   The Network Profiles page displays.
5. In the table, for the management VLAN, click the **3 dots** icon and select **Edit**.

   The Edit Profile page displays the Profile Template section.
6. From the **Profile Templates** menu, select **Hybrid SMPTE AES67 Core and Audio AES67 Edge**.
7. Click the **Next** button.

The Edit Profile page displays the Profile Settings section.

The **PTP-TC** and **PTPv2 BC/GM** toggle displays blue or green and is positioned to the right. With this profile selection, you cannot disable this toggle.

PTPv2 BC/GM is automatically configured on the Core switch; PTP-TC is automatically configured on the three edge switches.

8. In the **Profile Name** field, enter a name for identification purposes.

   Note: You cannot change the selection from the **Profile Template** menu.

9. To add a color to the network profile for visual representation, click the box in the **Color** field, and select a color.
10. Click the **Next** button.

    The Edit Profile page displays the Port Assignment section.

    Note: In this example, we did not add access points (APs) to the site. Therefore, the WiFi options are not displayed. If you did add APs, you can click the **Next** button to skip the WiFi configuration. If needed, you can always add a WiFi configuration later. For more information, see the "Add the global site SSID to a network profile" section or "Add a new dedicated WiFi network to a network profile" section in the NETGEAR Engage Controller User Manual.

11. Add the ports on the Core switch to the network profile:
    a. Click the graphical display of the Core switch.

       The page adjusts to display the switch ports of the Core switch.

    b. Select ports **1**, **2**, **3**, and **4** as tagged ports by clicking the ports until a T displays.

       Ports 1, 2, and 3 are downlinks to the edge switches. Port 4 is an uplink to the router.

       Note: By default, the Auto-Trunk feature is enabled. If you keep this feature enabled, ports 1, 2, 3, and 4 are automatically set as tagged (T) trunk ports, but you still must select them.

12. Add the ports on the Edge switch 1 to the network profile:
    a. Click the graphical display of the Edge switch 1.

       The page adjusts to display the switch ports of the Core switch.

    b. Select ports **1** through **6** as untagged ports by clicking the ports until a flag displays.

       Ports 1 through 6 are access ports that are connected to the end devices.

    c. Select port **25** as a tagged port by clicking the port until a T displays.

       Port 25 is an uplink port to the Core switch.

Note: By default, the Auto-Trunk feature is enabled. If you keep this feature enabled, port 25 is automatically set as a tagged (T) trunk port, but you still must select it.

13. Repeat Step 12 for the Edge switch 2, which has the same port configuration as the Edge switch 1.

    Uplink ports must be tagged. Access ports to end devices must be untagged.

14. Repeat Step 12 for the Edge switch 3, which has the same port configuration as the Edge switch 1.

    Uplink ports must be tagged. Access ports to end devices must be untagged.

15. Click the **Apply** button.

    The Edit Profile pop-up window displays.

16. Click the **Yes** button.

    The Network Profiles page displays.

    The Audio Video SMPTE profile with PTPv2 BC/GM is set on the Core switch and the Audio AES67 profile with PTP TC is automatically set on the edge switches.

17. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Change the priority for a clock

The PTPv2 boundary clock/grandmaster clock feature is supported on the M4350 series SMPTE-capable switches:

- M4350-8M2V (SKU MSM4310)
- M4350-16V4C (SKU VSM4320C)
- M4350-24F4X (SKU MSM4328F)
- M4350-24M4X4V (SKU MSM4332)
- M4350-40F4C (SKU XSM4344FC)
- M4350-40X4C (SKU XSM4344C)

By default, the priority of a clock is set to 128. If another clock in your network has a lower priority, that clock functions as the master clock, and the clock on the M4350 series SMPTE-capable switch functions as the boundary clock. However, you can change the clock priority so that a switch functioning as a boundary clock becomes the master clock.

Note the following about the PTPv2 boundary clock (BC)/grandmaster (GM) clock feature:

- If a network profile that uses AVB is enabled (for example, a network profile that is based on Audio AVB), the PTPv2 BC clock (or transparent clock) is automatically disabled and you cannot manually enable the feature. AVB and a PTPv2 BC/GM cannot coexist.
- A PTPv2 BC/GM is not supported on a stack.

To change the priority for a clock:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. In the Managed Devices table, for the switch that functions as the core switch, click the **Configure** button.

   The Overview page displays.

5. Select **Configure > Network Profiles** .

   The Network Profiles page displays.

6. Below the graphical display of the switch, to the right of PTPv2 BC/GM, click the **3 dots** icon.

   The PTPv2 BC/GM Setting pop-up window displays.

7. From the **Local Clock Prority1** menu, select **0**, which is the lowest value and the highest priority.

   The priority 1 determines which switch that is capable of functioning as a grandmaster clock is elected to be the active grandmaster clock in the network.

8. From the **Local Clock Prority2** menu, select **0**.

   If two switches in your network have the same priority 1 value, the priority 2 value determines which switch becomes the active grandmaster clock in the network.

9. Click the **Apply** button.

Your setting are saved.

10. To save the settings to the running configuration, at the top right of the page, click the **Save** button.
11. To return to the Devices page of the controller, select **Devices Management**.

3

VLAN routing

The chapter includes the following sections:

The following VLAN-routing related Tech Guide is available at the NETGEAR ProAV site:

Configuring VLAN Routing Using Engage

Set up three routing VLANs and allow inter-VLAN routing

The fully managed switches that the controller supports are capable of Layer 3 routing. This capability allows network traffic to be routed between different VLANs that might represent different subnets. We call this inter-VLAN routing.

By default, inter-VLAN routing is enabled between all VLANs. (Also see Block routing between two or more VLANs on page 70.)

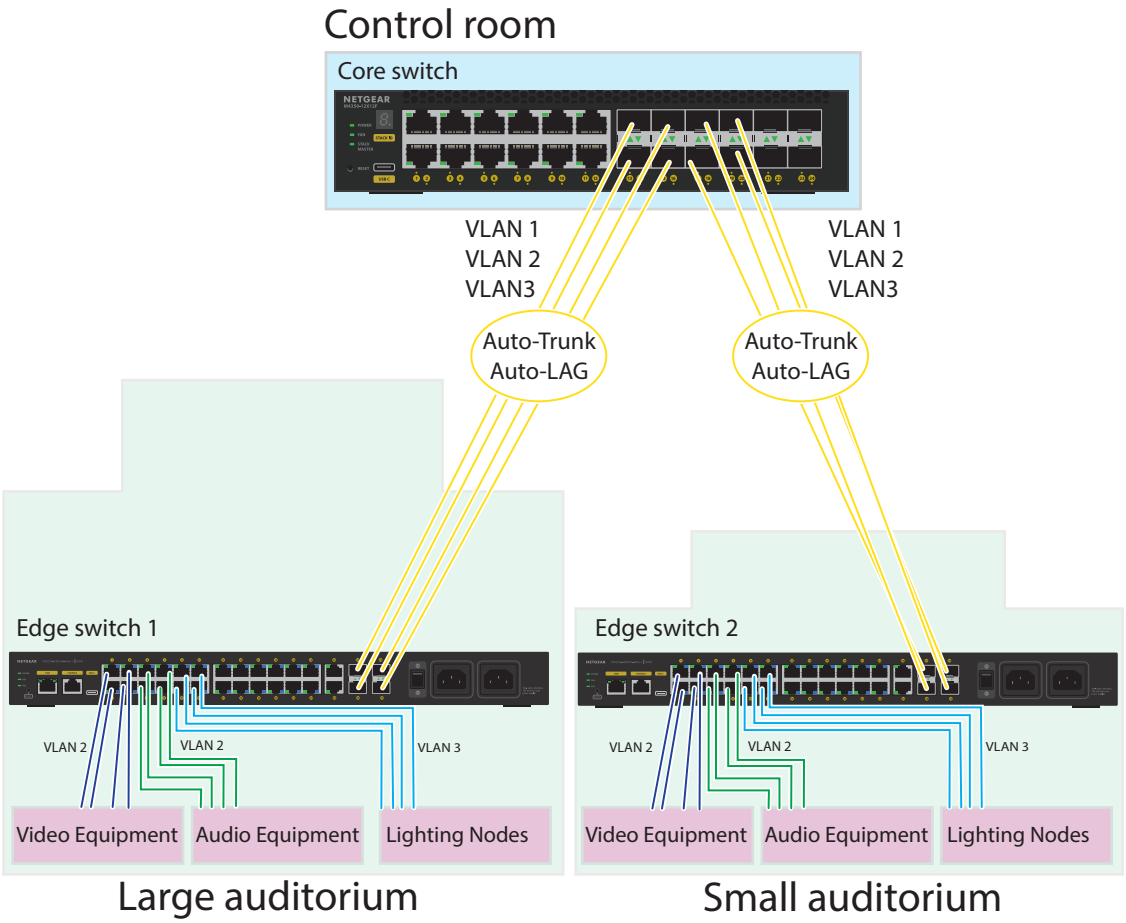


Figure 5. Three VLANs with inter-VLAN routing

The following VLANs are used in the example procedure.

Table 2. VLANs used in the example

VLAN	Type	Description
VLAN 1	Management and WiFi VLAN	Configured under the Default network profile, which uses the *Data* profile template. VLAN 1 operates in the 233.252.50.0 network as a DHCP server that assigns IP addressees in that network to the Core switch, Edge switch 1, and Edge switch 2.
VLAN 2	Video and audio VLAN	Configured under the Auditorium Sound and Video network profile, which uses the *Video with Dante audio* profile template. VLAN 2 operates as a DHCP server on the Core switch and assigns IP addresses in the 192.168.1.0 network to the video and audio equipment that is connected to Edge switch 1 and Edge switch 2.
VLAN 3	Lighting VLAN	Configured under the Auditorium Lights network profile, which uses the *Lighting* profile template. VLAN 3 operates as a DHCP server on the Core switch and assigns IP addresses in the 192.168.2.0 network to the lighting nodes that are connected to Edge switch 1 and Edge switch 2.

The following switches and ports are used in the example procedure, and VLANs 1, 2, and 3 are enabled on each switch.

Table 3. Switches and ports used in the example

Device	Model	Description
Core switch	M4350-12X12F	The switch has the following port connections: • **Port 13**: First 10G downlink to the Edge switch 1 • **Port 14**: Second 10G downlink to the Edge switch 1 • **Port 15**: Third 10G downlink to the Edge switch 1 • **Port 16**: Fourth 10G downlink to the Edge switch 1 • **Port 17**: First 10G downlink to the Edge switch 2 • **Port 18**: Second 10G downlink to the Edge switch 2 • **Port 19**: Third 10G downlink to the Edge switch 2 • **Port 20**: Fourth 10G downlink to the Edge switch 2
Edge switch 1	M4250-26G4F-PoE++	The switch has the following port connections: • **Ports 1, 2, 3, and 4**: Access ports connected to video equipment, assigned to the Video with Dante audio profile template with VLAN 2. • **Ports 5, 6, 7, and 8**: Access ports connected to audio equipment, assigned to the Video with Dante audio profile template with VLAN 2. • **Ports 9, 10, 11, and 12**: Access ports connected to lighting equipment, assigned to the Lighting profile template with VLAN 3. • **Port 27**: First 10G uplink to the Core switch • **Port 28**: Second 10G uplink to the Core switch • **Port 29**: Third 10G uplink to the Core switch • **Port 30**: Fourth 10G uplink to the Core switch
Edge switch 2	M4250-26G4F-PoE++	The switch has the following port connections: • **Ports 1, 2, 3, and 4**: Access ports connected to video equipment, assigned to the Video with Dante audio profile template with VLAN 2. • **Ports 5, 6, 7, and 8**: Access ports connected to audio equipment, assigned to the Video with Dante audio profile template with VLAN 2. • **Ports 9, 10, 11, and 12**: Access ports connected to lighting nodes, assigned to the Lighting profile template with VLAN 3. • **Port 27**: First 10G uplink to the Core switch • **Port 28**: Second 10G uplink to the Core switch • **Port 29**: Third 10G uplink to the Core switch • **Port 30**: Fourth 10G uplink to the Core switch

Inter-VLAN routing allows all devices on all VLANs to communicate with each other, regardless of the subnet the devices are operating in.

To create VLAN 2 and VLAN 3 and allow Inter-VLAN routing between all VLANs, including the default management VLAN 1:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. Configure VLAN 2 by creating the Auditorium Video and Sound network profile that uses the *Video with Dante audio* profile template:

   a. Select **Site Settings > Network Profiles**.

      The Network Profiles page displays.

   b. Click the **Create New Profile** link.

      The Create New Profile page displays the Profile Template section.

   c. From the **Profile Templates** menu, select **Video with Dante audio**, and click the **Next** button.

      The Create New Profile page displays the Profile Settings section.

   d. In the **Profile Name** field, enter **Auditorium Sound and Video**.

   e. In the VLAN ID field, enter **2**, and click the **Next** button.

      The Create New Profile page displays the Port Assignment section. However, if one or more APs are configured for the site, the Wireless Settings page displays, and you must click the **Next** button again. The WiFi options are outside the scope of this example. For more information about configuring WiFi on a network Profile, see the “Manage the WiFi Settings for a Site” chapter in the Engage Controller user manual.

   f. Do the following:

      - Click the graphical display of Edge switch 1, and then click ports **12**, **13**, **14**, and **15** several times until the ports are marked with a T (for tagged).
      - Click the graphical display of Edge switch 2, and then click ports **15**, **16**, **17**, and **18** several times until the ports are marked with a T (for tagged).

   g. Click the **Apply** button.

      The Create New Profile pop-up window displays.

h. Click the **Yes** button.

   The VLAN Routing Planner pop-up window displays.

i. Click the **Yes** button.

   Your settings are saved and the profile is added to the table on the Network Profiles page. The VLAN Routing Planner page displays.

j. Select the **Enable Routing on all Switches** check box, and click the **Apply** button.

   The VLAN Routing Planner pop-up window displays again.

k. Click the **Go to VLAN Routing** button.

   The Basic Configuration page display. In the VLAN Routing menu, the selection is VLAN ID 2.

l. Select the **DHCP Server** check box for the Core switch.

m. In the **IP Address** field, enter **192.168.1.0** and in the **Subnet Mask** field, enter **255.255.255.0**.

   This setting means that the Core switch functions as a DHCP server to assign IP addresses to all audio and video equipment that is connected to both Edge switch 1 and Edge switch 2 and that is placed in VLAN 2.

   In the DHCP Server section, the Default Router, DHCP Server Pool Start, DHCP Server Pool End, and Lease Time fields are automatically filled based on the IP address and subnet mask that you set for the DHCP server and the default settings for the lease time.

n. Click the **Apply** button.

   The Network Profiles page displays and shows VLAN 2 with routing enabled.

5. Configure VLAN 3 by creating the Auditorium Lights network profile that uses the *Lighting* profile template:

   a. Select **Site Settings > Network Profiles**.

      The Network Profiles page displays.

   b. Click the **Create New Profile** link.

      The Create New Profile page displays the Profile Template section.

   c. From the **Profile Templates** menu, select **Lighting**, and click the **Next** button.

      The Create New Profile page displays the Profile Settings section.

   d. In the **Profile Name** field, enter **Auditorium Lights**.

   e. In the VLAN ID field, enter **3**, and click the **Next** button.

      The Create New Profile page displays the Port Assignment section. However, if one or more APs are configured for the site, the Wireless Settings page displays, and you must click the **Next** button again. The WiFi options are outside the scope of this example. For more information about configuring WiFi on a network profile,

see the “Manage the WiFi Settings for a Site” chapter in the Engage Controller user manual.

f. Do the following:

- Click the graphical display of Edge switch 1, and then click ports **3**, **4**, **5**, and **6** several times until the ports are marked with a T (for tagged).
- Click the graphical display of Edge switch 2, and then click ports **5**, **6**, **7**, and **10** several times until the ports are marked with a T (for tagged).

g. Click the **Apply** button.

The Create New Profile pop-up window displays.

h. Click the **Yes** button.

The VLAN Routing Planner pop-up window displays.

i. Click the **Yes** button.

Your settings are saved and the profile is added to the table on the Network Profiles page. The VLAN Routing Planner page displays.

j. Select the **Enable Routing on all Switches** check box, and click the **Apply** button.

The VLAN Routing Planner pop-up window displays again.

k. Click the **VLAN Routing Planner** button.

The Basic Configuration page display. In the VLAN Routing menu, the selection is VLAN ID 3.

l. Select the **DHCP Server** check box for the Core switch.

m. In the **IP Address** field, enter **192.168.2.0** and in the **Subnet Mask** field, enter **255.255.255.0**.

This setting means that the Core switch functions as a DHCP server to assign IP addresses to all lighting equipment that is connected to both Edge switch 1 and Edge switch 2 and that is placed in VLAN 3.

In the DHCP Server section, the Default Router, DHCP Server Pool Start, DHCP Server Pool End, and Lease Time fields are automatically filled based on the IP address and subnet mask that you set for the DHCP server and the default settings for the lease time.

n. Click the **Apply** button.

The Network Profiles page displays and shows VLAN 3 with routing enabled.

6. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Change the management VLAN from the OOB port

The default management interface is the VLAN with ID 1. If you configure a network profile as a routing VLAN, you can set a different management VLAN than VLAN 1. However, for each site, only one VLAN can be the management VLAN.

The out-of-band (OOB) port, also called the service port, is a dedicated Ethernet port for out-of-band (OOB) management of a switch. Management 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, all ports on a switch are members of VLAN 1. If you change the management VLAN by using a network port, you are locked out from the management VLAN because the network port is no longer a member of VLAN 1. However, if you use the OOB port, you are not locked out and can continue to access the switch after changing the management VLAN.

By default, the IP address of the OOB port of a switch is assigned by the DHCP server for the site. You can also set a static IP address for the OOB port.

This example assumes the following:

- The current management VLAN is the default management VLAN with VLAN ID 1.
- You already set up a network profile to which you assigned VLAN 100.
- You are using an OOB port with IP address 10.51.100.25. (This address is just an example.)

To access a switch over its OOB port with a static IP address and change the management VLAN from the default VLAN 1 to VLAN 100:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

- **Make no changes to the network setup for the site**: Click the **Apply** button.
- **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Configure a static IP address for the OOB port:
   a. Select **Site Settings > Management VLAN and OOB**.

      The Management VLAN page displays.
   b. From the menu in the left panel, select **OOB**.

      The OOB page displays.
   c. For the switch for which you want to configure the OOB port, select the **Static** check box.

      By default, the OOB port receives IP address settings from the DHCP server.
   d. In the **IP Address** field, enter **10.51.100.25**, in the **Subnet Mask** field, enter **255.255.255.0,** and in the **Default Gateway** field, enter **10.51.100.1**.
   e. Click the **Apply** button.

      A pop-up window displays.

      Caution: When you click the Yes button, the OOB port is disconnected and you must reconnect using the new IP address settings.
   f. Click the **Yes** button.

      Your changes are saved.
5. Log in to the OOB port with its new IP address.

   You might need to change the TCP/IP settings on the your computer on which the controller is installed.
6. Change the management VLAN:
   a. Select **Site Settings > Management VLAN and OOB**.

      The Management VLAN page displays.
   b. From the **Management VLAN** menu, select **100**.
   c. Click the **Apply** button.

      A pop-up window displays.

      Caution: When you click the Yes button, the devices at the site are disconnected and must reconnect using the new IP address settings. However, your computer is not disconnected because you logged in over the OOB port.
   d. Click the **Yes** button.

Your changes are saved.

7. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Add routing and Internet access for an existing VLAN

By default, VLAN routing (layer 3 IP routing) is disabled for a network profile (VLAN) at a site. The exception is the management VLAN for the site, which is the VLAN for the default network profile.

If you enable routing for a VLAN, by default, Internet access is disabled (except for the management VLAN for the site, by default VLAN 1). However, if your network includes a PR460X Pro Router, you can, with one click, enable Internet access for all clients that are connected to the VLAN.

This example task describes how to enable routing for existing VLAN 50 that you already assigned to the Video with Q-SYS audio network profile and to enable Internet access for routing VLAN 50.

For a network that includes a PR460X Pro Router, to enable routing for an existing VLAN 50 and enable Internet access for routing VLAN 50:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. Enable routing for the Video with Q-SYS audio network profile with VLAN 50:

   a. Select **Site Settings**.

The Network Profiles page displays.

b. In the table, for the Video with Q-SYS audio network profile with VLAN 50, click the **3 dots** icon and select **Routing**.

The VLAN Routing Planner page displays.

c. Select the **Enable Routing on all Switches** check box.

You are enabling routing on all switches that use the network profile.

If you want to configure the routing, DHCP server, core switch, and IGMP Querier feature options for an individual switch that uses the network profile, click the graphical display of the switch and configure the settings by selecting one or more radio buttons for the feature options.

d. Click the **Apply** button.

The VLAN Routing Planner pop-up window displays.

e. Click the **Go to VLAN Routing** button.

The Basic Configuration page displays. Your routing settings are saved.

5. Enable access to the Internet for VLAN 50:
   a. In the **VLAN Routing** menu, be sure that the Video with Q-SYS audio network profile with VLAN 50 is selected.
   b. Turn on the **Internet Access** toggle so that it displays blue or green and is positioned to the right.
   c. Click the **Apply** button.

      Your settings are saved.
6. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Enable the mDNS gateway to share devices and services across VLANs

If your network includes a PR460X Pro Router, you can set the router as the multicast DNS (mDNS) gateway, which forwards mDNS service discovery requests and responses between VLANs. An mDNS gateway allows devices and services to be shared and discovered across different VLANs and WiFi networks without the presence of a regular DNS server.

One requirement is that inter-VLAN routing must be enabled on the VLANs where devices and services are located. By default, inter-VLAN routing is enabled. If you disabled inter-VLAN routing (see Block routing between two or more VLANs on page

70), reenable it on the VLANs that need to share services. Ports between the router and the core switch must be trunk ports that carry all relevant VLANs.

With inter-VLAN routing and the mDNS gateway enabled, devices in different VLANs can discover each other through mDNS. This method simplifies cross-VLAN access to services such as printers and displays without the need for static DNS entries or centralized name resolution.

In this example:

- Printer: Connected on a network profile that uses VLAN 1.
- Large-screen device: Connected on a network profile that uses VLAN 30.
- Clients: Connected to a network profile that uses VLAN 20.

After you configure the PR460X Pro Router as an mDNS gateway, the clients in VLAN 20 can discover and connect to the printer in VLAN 1 and the large-screen device in VLAN 30.

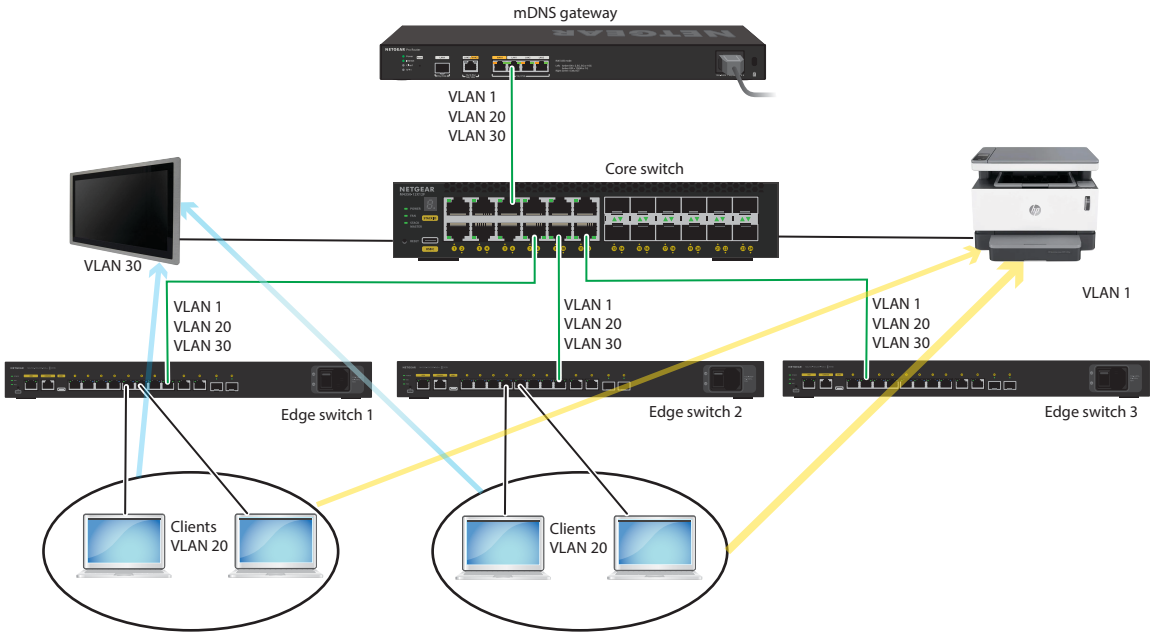


Figure 6. mDNS gateway configuration

Note: If a WiFi access point (AP) is connected to the router, a service can run either on a wired or WiFi device, but for a WiFi client to be able to access the service, the WiFi client must be connected to a WiFi network on an AP that also has the mDNS gateway feature enabled.

For a network that includes a PR460X Pro Router, to automatically enable cross-VLAN service discovery using the mDNS gateway:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. Select **Site Settings > mDNS Gateway**.

   The mDNS Gateway Configuration page displays.

5. Enable the mDNS gateway by clicking the **mDNS Gateway** toggle so that it displays blue or green and positioned to the right.

   By default, the mDNS gateway is disabled and the **Enable mDNS Gateway** toggle is gray and positioned to the left.

6. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

4

Sites

The chapter includes the following sections:

- Set up a site with a core switch as DHCP server and two edge switches, all supporting three network profiles
- Export a site and then import it in a new instance of the controller
- Change the network setup of a site

Set up a site with a core switch as DHCP server and two edge switches, all supporting three network profiles

In this example configuring, we are setting up a site named *Audio Video Lab* that supports a core switch that also functions as a DHCP server and two edge switches. All switches support three network profiles, each with their associated VLAN:

- **Data**: The default network profile with VLAN ID 1, which is also used for the control traffic.
- **Audio Dante**: A network profile to which we assign VLAN ID 20.
- **Video**: A network profile to which we assign VLAN ID 40.

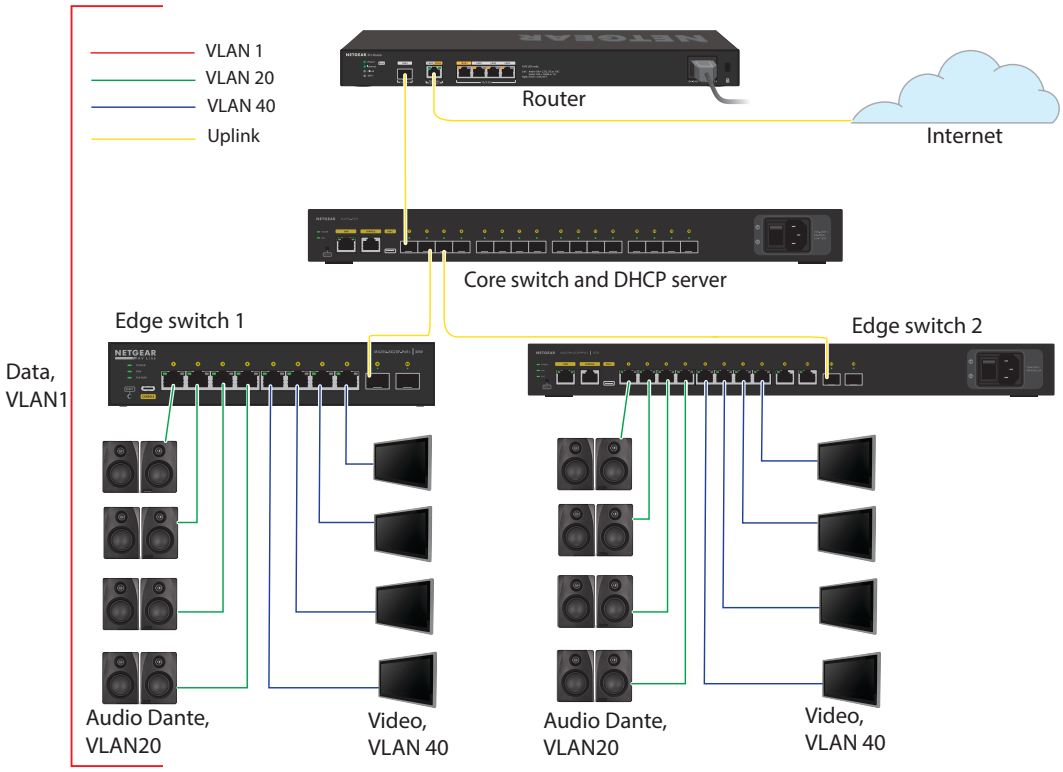


Figure 7. Core switch as DHCP server and two edge switches, supporting Data, Audio Dante, and Video network profiles

In this example configuration, the network consist of the switches and port connections that are listed in the table and that are also used in the example configuration procedure that follows. For this example, we assume that the switches are already onboarded and assigned to the default Data network profile with VLAN ID 1.

Table 4. Ports and VLANs used in the example

Device	Model	Description
Router	PR460X	The router has the following port connections: • **Port LAN5 WAN2**: 10G connection to the Internet. • **Port LAN4**: 10G connection to the Core switch.
Core switch	M4250-16XF	The switch functions as the Core switch and a DHCP server for the Audio Dante network profile. This switch has the following port connections: • **Port 1**: 10G uplink to the router. • **Port 2**: 10G downlink to the Edge switch 1. • **Port 3**: 10G downlink to the Edge switch 2.
Edge switch 1	M4250-8G2XF-PoE+	The switch has the following port connections: • **Ports 1, 2, 3, and 4**: Access ports, each connected to an audio device, assigned to the Audio Dante network profile with VLAN ID 20. • **Ports 5, 6, 7, and 8**: Access ports, each connected to a video device, assigned to the Video network profile with VLAN ID 40. • **Port 9**: 10G uplink to the Core switch.
Edge switch 2	M4250-10G2XF-PoE+	The switch has the following port connections: • **Ports 1, 2, 3, and 4**: Access ports, each connected to an audio device, assigned to the Audio Dante network profile with VLAN ID 20. • **Ports 5, 6, 7, and 8**: Access ports, each connected to a video device, assigned to the Video network profile with VLAN ID 40. • **Port 11**: 10G uplink to the Core switch.

How the ports on the Edge switches receive an IP address:

- **Ports 1, 2, 3, and 4 on Edge switch 1 and Edge switch 2**: Before you set up the Audio Dante network profile, the ports receive an IP address through the default Data network profile. After you set up the Audio Dante network profile, the ports receive an IP address from the Core switch that functions as a DHCP server for the Audio Dante network profile.
- **Ports 5, 6, 7, and 8 on Edge switch 1 and Edge switch 2**: These ports receive an IP address through the default Data network profile.

To set up the *Audio and Video Lab* site with a core switch as DHCP server and two edge switches, all supporting the Data, Audio Dante, and Video network profiles:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. Set up the *Audio Video Lab* site:

   a. Select **Controller Management**.

      The Manage Site Configurations page displays.

   b. Click the **Create New Site** link.

      The Create New Site pop-up window displays.

   c. Set the following information for the site:

      i. **Site Name**: A name for identification purposes. For this example, we are using *Audio Video Lab*.

      ii. **Site Description**: A description for identification purposes.

      iii. **New Site Admin Password**: The password, which must be eight characters or more.

      The password must be a minimum of 8 and a maximum of 16 alphanumeric characters and *cannot* contain any special characters. To make the password visible, click the eye icon.

      The controller pushes this password to each device that it onboards at the site and replaces the local device password with the site password.

      iv. **Confirm Site Admin Password**: Repeat the password.

      v. In the **New Site Admin Password Hint** field, enter a password hint.

      We are not configuring a view-only guest user password, so you can leave the associated check box cleared.

   d. Click the **Next** button.

      The windows adjusts and the Network Setup settings display.

e. Select the **Dynamic IP Address** radio button, and from the **Engage Network Interface** menu, select the computer's network interface so that it can receive a dynamic IP address from a DHCP server (or router that functions as a DHCP server) in the network.

f. Click the **Next** button.

The windows adjusts and the Wireless Setup settings display.

g. Click the **Skip >>** link to skip this step.

The Skip Wireless Setup pop-up window displays.

h. Click the **Yes** button.

Your settings are saved. The site is added to the table on the Manage Site Configurations page.

5. Add the Audio Dante network profile, assign the ports, set model M4250-16XF as the Core switch for the Audio Dante network profile, and configure its DHCP server settings:

a. Select **Site Settings > Network Profiles**.

The Network Profiles page displays.

b. Click the **Create New Profile** link.

The Create New Profile page displays the Profile Template section.

c. From the **Profile Templates** menu, select **Audio Dante**.

d. Click the **Next** button.

The Create New Profile page displays the Profile Settings section.

e. In the **Profile Name** field, enter a name for identification purposes.

f. In the **VLAN ID** field, enter **20**.

g. To add a color to the network profile for visual representation, click the box in the **Color** field, and select a color.

By default, the PTP residency time stamping toggle is enabled so that it displays blue or green and is positioned to the right.

h. Click the **Next** button.

The Create New Profile page displays the Port Assignment section.

Note: In this example, we did not add access points (APs) to the site. Therefore, the WiFi options are not displayed. If you did add APs, you can click the **Next** button to skip the WiFi configuration. If needed, you can always add a WiFi configuration later. For more information, see the "Add the global site SSID to a network profile" section or "Add a new dedicated WiFi network to a network profile" section in the NETGEAR Engage Controller User Manual.

i. Click the graphical display of model **M4250-8G2XF-PoE+** (the Edge switch 1), and click ports **1**, **2**, **3**, and **4** once.

   A flag displays for each port, indicating that the port is added to the profile as an untagged port.

j. Click the graphical display of model **M4250-10G2XF-PoE+** (the Edge switch 2), and click ports **1**, **2**, **3**, and **4** once.

   A flag displays for each port, indicating that the port is added to the profile as an untagged port.

k. Click the **Apply** button.

   The Create New Profile pop-up window displays.

l. Click the **Yes** button.

   Your settings are saved and the profile is added to the table on the Network Profiles page. The VLAN Routing Planner pop-up window displays.

m. Click the **Yes** button.

   The VLAN Routing Planner page displays.

n. Select the **Enable Routing on all Switches** check box.

o. Click the graphical display of model **M4250-16XF** (the switch that must become the Core switch).

   A pop-up window displays.

p. Select the **Core Switch** radio button, and click the **Apply** button in the pop-up window.

   Your selection is saved.

q. Click the **Apply** button at the bottom of the page.

   The VLAN Routing Planner pop-up window displays again.

r. Click the **Go to VLAN Routing** button.

   The Basic Configuration page display. In the VLAN Routing menu, the selection is VLAN ID 20.

s. Select the **DHCP Server** check box for model M4250-16XF (the Core switch).

t. In the **IP Address** field, enter **192.168.2.0** and in the **Subnet Mask** field, enter **255.255.255.0**.

   This setting means that the Core switch functions as a DHCP server to assign IP addresses to all Audio Dante equipment that is connected to both the Edge switch 1 and Edge switch 2 and that is placed in VLAN 20.

   In the DHCP Server section, the Default Router, DHCP Server Pool Start, DHCP Server Pool End, and Lease Time fields are automatically filled based on the IP address and subnet mask that you set for the DHCP server and the default settings for the lease time.

u. In the **DNS Server 1** field, type the IP address for the primary DNS server.

The choice of DNS servers depends on the scale of the network. For a large scale network, use the local DNS server. For a smaller network where no local DNS server is available, you could use Cloudflare with IP address 1.1.1.1 as the primary DNS server and Quad9 with IP address 9.9.9.9 as the secondary (or backup) DNS server.

If your network is not connected to the Internet, you do not need to set DNS servers.

v. In the **DNS Server 2** field, optionally, type the IP address for the secondary DNS server.

w. Click the **Apply** button.

The Network Profiles page displays and shows the Audio Dante profile template, VLAN ID 20, and routing enabled.

6. Add the Video network profile and assign the ports:

a. Select **Site Settings > Network Profiles**.

The Network Profiles page displays.

b. Click the **Create New Profile** link.

The Create New Profile page displays the Profile Template section.

c. From the **Profile Templates** menu, select **Video**.

d. Click the **Next** button.

The Create New Profile page displays the Profile Settings section.

e. In the **Profile Name** field, enter a name for identification purposes.

f. In the **VLAN ID** field, enter **40**.

g. To add a color to the network profile for visual representation, click the box in the **Color** field, and select a color.

By default, the PTP residency time stamping toggle is disabled so that it displays gray and is positioned to the left.

h. Click the **Next** button.

The Create New Profile page displays the Port Assignment section.

Note: In this example, we did not add APs to the site. Therefore, the WiFi options are not displayed. If you did add APs, you can click the **Next** button to skip the WiFi configuration. If needed, you can always add a WiFi configuration later. For more information, see the "Add the global site SSID to a network profile" section or "Add a new dedicated WiFi network to a network profile" section in the NETGEAR Engage Controller User Manual.

i. Click the graphical display of model **M4250-8G2XF-PoE+** (the Edge switch 1), and click ports **5**, **6**, **7**, and **8** once.

   A flag displays for each port, indicating that the port is added to the profile as an untagged port.

j. Click the graphical display of model **M4250-10G2XF-PoE+** (the Edge switch 2), and click ports **5**, **6**, **7**, and **8** once.

   A flag displays for each port, indicating that the port is added to the profile as an untagged port.

k. Click the **Apply** button.

   The Create New Profile pop-up window displays.

l. Click the **Yes** button.

   Your settings are saved and the profile is added to the table on the Network Profiles page. The VLAN Routing Planner pop-up window displays.

m. Click Select the **No** check box.

   The Network Profiles page displays and shows the Video profile template and VLAN ID 40.

7. To save the settings to the running configuration, at the top right of the page, click the **Save** button.
8. Reboot the Edge switch 1 and Edge switch 2 so that the audio devices connected to the ports that are assigned to the Audio Dante network profile receive a new IP address from the Core switch, which now serves as a DCHP server for the Audio Dante network profile with VLAN 20.

   The video devices do not receive a new IP address because they are associated with the default Data network profile, which did not change.

Export a site and then import it in a new instance of the controller

The controller is a portable application that can reside on a Windows-based computer or Mac, or on a USB thumb drive, so it can be easily moved to any network location. For a Windows-based computer, you can launch the app directly from the USB thumb drive, and save all configuration data to the same USB thumb drive. For a Mac, you can install the controller on the computer, and then copy the locally saved configuration data back to the USB thumb drive for convenience.

Importing a site configuration is useful if you set up a new installation (that is, a new instance of the controller), or you install the controller in a new folder, but want to reinstall an existing site configuration.

After you export the site, you can either import the site when you access the new controller instance for the first time, or after you already set up the new controller instance:

- Export a site and then import it when you access a new instance of the controller for the first time
- Export a site and then import it in a new instance of the controller after you set up the controller

Export a site and then import it when you access a new instance of the controller for the first time

To export a site configuration and then import it when you access a new instance of the controller for the first time:

1. On the controller instance from which you want to export the site configuration, do the following:
   a. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

      The controller application opens and displays a login page.
   b. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

      The Managed Devices page displays.
   c. Select **Controller Management**.

      The Manage Site Configurations page displays.
   d. In the table, for the site for which you want to export the site configuration, click the **3 dots** icon and select **Export**.

      The Export Site Configuration pop-up window displays.
   e. Enter a site configuration password and repeat the site configuration password.

      The site configuration password is not the same as the site password, although you could use the same password. For the site configuration password, you can

set a unique password that protects the security of the switches, configurations and site (and switches) password.

f. Click the **Apply** button.

A pop-up window opens.

g. Navigate to a location and save the site configuration.

2. On the controller instance in which you want to import the site configuration while accessing the new instance for the first time:

a. On your computer, in the folder in which you installed the controller application, click the **Engage.exe** application icon.

The initial login page displays.

The first time that you log in, no password is required. However, you then must specify a local device password to use each subsequent time that you log in.

b. In the **Login Name** field, enter admin, and click the **Login** button.

The Engage Password page displays.

c. In the New Password field, set an admin password, repeat the password in the Confirm Password field, and click the Next button.

The password must be 8 to 64 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The following special characters are allowed: ! @ # $ % ^ & * ( ). To make the password visible, click the eye icon.

d. Click the **Next** button.

The Site Setup page display.

e. Click the **Import Site Configuration** radio button.

The page adjusts.

f. Click the **Browse** button and navigate to and select the site configuration file that you want to import.

g. In the **Site Configuration Password** field, enter the password for the site configuration file.

The site configuration password is not the same as the site password (although it *could* be). When you exported the site, you defined the site configuration password.

h. Click the **Finish** button.

Your settings are saved, and the devices are being onboarded. However, if the Edit Network Setup pop-up window displays, see the following step.

If any device does not yet support the controller, the controller pushes firmware *with* controller functions to the device. This firmware update is necessary because the controller cannot manage the device without the firmware update. Because

of the firmware update, this process might take up to 10 minutes, after which the page displays the Onboarding Finished message.

Caution: During the onboarding process, do not restart the devices or change any cables. Wait until the onboarding process is finished.

i. If the devices are not being onboarded but the Edit Network Setup pop-up window displays, specify how the computer on which the controller is installed can connect to the AV network at the site by selecting one of the following radio buttons:

- **Dynamic IP Address**: From the **Engage Network Interface** menu, select the computer's network interface so that it can receive a dynamic IP address from a DHCP server (or router that functions as a DHCP server) in the network.
- **Static IP Address**: The computer requires a static IP address to connect to the site. Do the following:
  i. Assign a static IP address to the computer on which you installed the controller.

     The Network Setup page shows the steps how to assign a static IP address to the computer. You can display these steps for MacOS and Windows.
  ii. From the **Engage Network Interface** menu, select the static IP address.
- **Static IP Address + DHCP Server**: The computer uses a static IP address and lets the controller function as a DHCP server. Do the following:
  i. Assign a static IP address to the computer on which you installed the controller and configure the computer as a DHCP server.

     The Network Setup page shows both the steps how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for MacOS and Windows.
  ii. From the **Engage Network Interface** menu, select the static IP address.
  iii. In the **Start Client IP Address** field, enter the start IP address for the DHCP server address range.
  iv. In the **End Client IP Address** field, enter the end IP address for the DHCP server address range.

  Note: If you use the DHCP server option, we recommend that you restart all NETGEAR switches at the site for fastest IP address assignment by the controller's DHCP server.

j. If the Edit Network Setup pop-up window displays, after you select a radio button as described in the previous step, click the **Apply** button.

   Your settings are saved.

k. Click the **Go to Devices** button.

The Devices page displays. The page shows the following tables:

- **Managed Devices**: The table lists all onboarded devices that you can configure using the controller.
- **Discovered Devices**: The table lists all Engaged-manageable devices that the controller discovered in the network but that the controller did not onboard and that you therefore cannot yet configure using the controller.

l. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Export a site and then import it in a new instance of the controller after you set up the controller

To export a site configuration and then import it in another instance of the controller after you already set up the new instance:

1. On the controller instance from which you want to export the site configuration, do the following:
   a. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

      The controller application opens and displays a login page.

   b. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

      The Managed Devices page displays.

   c. Select **Controller Management**.

      The Manage Site Configurations page displays.

   d. In the table, for the site for which you want to export the site configuration, click the **3 dots** icon and select **Export**.

      The Export Site Configuration pop-up window displays.

   e. Enter a site configuration password and repeat the site configuration password.

      The site configuration password is not the same as the site password, although you could use the same password. For the site configuration password, you can set a unique password that protects the security of the switches, configurations and site (and switches) password.

   f. Click the **Apply** button.

A pop-up window opens.

g. Navigate to a location and save the site configuration.

2. On the controller instance in which you want to import the site configuration, do the following:

   a. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

      The controller application opens and displays a login page.

   b. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

      The Managed Devices page displays.

   c. Select **Controller Management**.

      The Manage Site Configurations page displays.

   d. Click the **Import Site** link.

      The Import Site pop-up window displays.

   e. Click the **Browse** button and navigate to and select the site configuration file that you want to import.

   f. In the **Site Configuration Password** field, enter the password that you defined when you exported the site.

      The site configuration password is not the same as the site password (although it *could* be). When you exported the site, you defined the site configuration password.

   g. Click the **Upload** button.

      The Edit Network Setup pop-up window displays.

   h. Specify how the computer on which the controller is installed can connect to the AV network at the site by selecting one of the following radio buttons:

      - **Dynamic IP Address**: From the **Engage Network Interface** menu, select the computer's network interface so that it can receive a dynamic IP address from a DHCP server (or router that functions as a DHCP server) in the network.
      - **Static IP Address**: The computer requires a static IP address to connect to the site. Do the following:

        i. Assign a static IP address to the computer on which you installed the controller.

The Network Setup page shows the steps how to assign a static IP address to the computer. You can display these steps for MacOS and Windows.

ii. From the **Engage Network Interface** menu, select the static IP address.

- **Static IP Address + DHCP Server**: The computer uses a static IP address and lets the controller function as a DHCP server. Do the following:

  i. Assign a static IP address to the computer on which you installed the controller and configure the computer as a DHCP server.

  The Network Setup page shows both the steps how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for MacOS and Windows.

  ii. From the **Engage Network Interface** menu, select the static IP address.

  iii. In the **Start Client IP Address** field, enter the start IP address for the DHCP server address range.

  iv. In the **End Client IP Address** field, enter the end IP address for the DHCP server address range.

  Note: If you use the DHCP server option, we recommend that you restart all NETGEAR switches at the site for fastest IP address assignment by the controller's DHCP server.

i. Click the **Apply** button.

Your settings are saved. The devices are being onboarded.

If any device does not yet support the controller, the controller pushes firmware *with* controller functions to the device. This firmware update is necessary because the controller cannot manage the device without the firmware update. Because of the firmware update, this process might take up to 10 minutes, after which the page displays the Onboarding Finished message.

Caution: During the onboarding process, do not restart the devices or change any cables. Wait until the onboarding process is finished.

When the onboarding is finished, the page shows the following tables:

- **Managed Devices**: The table lists all onboarded devices that you can configure using the controller.
- **Discovered Devices**: The table lists all Engaged-manageable devices that the controller discovered in the network but that the controller did not onboard and that you therefore cannot yet configure using the controller.

j. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Change the network setup of a site

You can change the network setup of a site:

To change the network setup of a site:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. Select **Controller Management**.

   The Manage Site Configurations page displays.
4. In the table, for the site that you want to edit, click the **3 dots** icon and select **Network Setup**.

   The Edit Network Setup pop-up window displays.
5. Change how the computer on which the controller is installed can connect to the AV network at the site by selecting a radio button:
   - **Dynamic IP Address**: From the **Engage Network Interface** menu, select the computer's network interface so that it can receive a dynamic IP address from a DHCP server (or router that functions as a DHCP server) in the network.
   - **Static IP Address**: The computer requires a static IP address to connect to the site. Do the following:
     a. Assign a static IP address to the computer on which you installed the controller.

        The Network Setup page shows the steps how to assign a static IP address to the computer. You can display these steps for MacOS and Windows.

     b. From the **Engage Network Interface** menu, select the static IP address.
   - **Static IP Address + DHCP Server**: The computer uses a static IP address and lets the controller function as a DHCP server. Do the following:
     a. Assign a static IP address to the computer on which you installed the controller and configure the computer as a DHCP server.

        The Network Setup page shows both the steps how to assign a static IP address to the computer and how to let the computer function as a DHCP server. You can display these steps for MacOS and Windows.

     b. From the **Engage Network Interface** menu, select the static IP address.

c. In the **Start Client IP Address** field, enter the start IP address for the DHCP server address range.

d. In the **End Client IP Address** field, enter the end IP address for the DHCP server address range.

Note: We recommend that you restart all NETGEAR switches at the site for fastest IP address assignment by the controller's DHCP server.

6. Click the **Next** button.

   The windows adjusts and the Edit Wireless Setup settings display.

7. Optionally, change the SSID name and WiFi password of the global WiFi network (SSID) for the site:

   a. For the SSID name, do one of the following:

      - **Use the site name**: Keep the associated toggle enabled so that it displays blue or green and is positioned to the right.
      - **Use a unique name**: Turn off the associated toggle so that it displays gray and is positioned to the right, and in the **SSID** field, enter the name for the WiFi network (SSID).

   b. For the WiFi password, do one of the following:

      - **Use the site password**: Keep the associated toggle enabled so that it displays blue or green and is positioned to the right.
      - **Use a unique password**: Turn off the associated toggle so that it displays gray and is positioned to the right, and in the **Password** field, enter the password for access to the WiFi network, which uses WPA-MPSK security.

   Note: You cannot change the region and country after you have enabled WiFi for a site. Therefore, the **Region** and **Country** fields are masked.

8. Click the **Apply** button.

   Your settings are saved. The altered site displays in the table on the Manage Site Configurations page.

9. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

5

LAGs, MLAGs, and switch stacks for redundancy and enhanced bandwidth

Depending on the types of switches that you connect, you can configure a link aggregation group (LAG), multi-chassis link aggregation group (MLAG), or switch stack, all of which are essential tools for setting up core switch redundancy.

The chapter includes the following sections:

What should you use: a LAG, MLAG, or switch stack?

The controller lets you set up a link aggregation group (LAG), multi-chassis link aggregation group (MLAG), and switch stack:

- **LAG**: Supported between NETGEAR fully managed switches, and between a NETGEAR fully managed switch and a third-party switch that supports LAGs.

  If you use NETGEAR fully managed switches for a LAG, the switches do not need to be of the same model. The LAG provides increased bandwidth and redundancy for a connection that can include multiple ports. By default, the Auto-LAG feature is enabled on the M4250 series and M4350 series switches, but disabled on the M4300 series switches.

- **MLAG**: Supported on M4500 series switches.

  In a ProAV environment in which you are using M4500 series switches, you can use a two-tier MLAG to set up a redundant core. You can also use MLAGs for other connections between M4500 series switches.

- **Stack**: Supported between M4300 series switches and between M4350 series switches. (You cannot mix M4300 series switches and M4350 series switches in a single stack.)

  In a ProAV environment in which you are using M4300 series and M4350 series switches, you can use a two-switch stack to set up a redundant core, but some limitations exist (see Create a two-switch stack for a redundant core on page 62).

  Note: Other than a stacking redundancy option, we do not recommend stacking in a ProAV environment. The reason is that in a switch stack, all multicast traffic is flooded through the stack, and PTP TC is not supported within a stack. A LAG or MLAG is more compatible with a ProAV environment with IGMP Plus.

  You can set up switch stack for a redundant core with two M4300 series switches or two M4350 series switches. If one of the core switches goes down or becomes unavailable, the other core switch takes over so your network remains up and running.

Why you do not need to set up LAGs between fully managed NETGEAR switches

If your network consists of fully managed NETGEAR switches, the Auto-LAG and Auto-Trunk features can automatically set up LAGs between the switches, and you do not need to create LAGs manually. (A LAG is also referred to as a port channel or an EtherChannel.)

Note: On the M4250 series and M4350 series switches, the Auto-LAG and Auto-Trunk features are enabled by default. On the M4300 series and M4500 series switches, the Auto-LAG and Auto-Tunk features are disabled by default but you can enable these features. For more information , see the NETGEAR Engage Controller User Manual.

To let switches automatically form LAGs, both the Auto-Trunk and Auto-LAG features must be enabled:

- **Auto-Trunk**: This feature lets the switch automatically enable Trunk mode on capable physical links and LAG interfaces between partner devices. A trunk can carry all active VLANs. 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.
- **Auto-LAG**: This feature automatically forms a LAG between two switches 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). 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 and Auto-LAG features, including requirements, see the "Auto-Trunk overview" and "Auto-LAG overview" sections in the NETGEAR Engage Controller User Manual.

Create LAGs between a NETGEAR core switch and third-party edge switches

If your network includes third-party switches, you must manually set up LAGs. For information about LAGs on fully managed NETGEAR switches, see Why you do not need to set up LAGs between fully managed NETGEAR switches on page 55.

These are the requirements for manually setting up a LAG between a NETGEAR switch and a third-party switch:

- At least two links must be established between the switches, and these links must support the same speed and duplex mode.
- The ports participating in the LAG must be in the general port mode.

Note: After a LAG is established, assigns VLANs on the LAG interface, not on the individual interfaces.

In this configuration example, the network includes a NETGEAR core switch and several third-party edge switches, and we are manually setting up LAGs between the core switch and the edge switches.

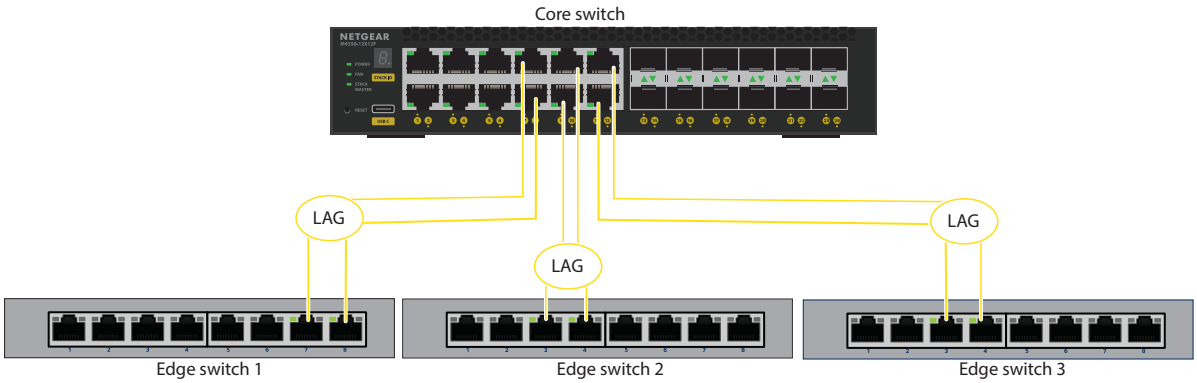


Figure 8. LAGs between a NETGEAR switch and third-party edge switches

Based on the hash mode that you select for the LAG, each switch balances traffic on the 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 cable the NETGEAR core switch to third-party edge switches and manually create LAGs:

1. Cable the switches for LAGs, using the following ports for this example:
   a. For the LAG between the Core switch and the third-party Edge switch 1, connect Core switch port 7 to a port on Edge switch 1 and connect Core switch port 8 to another port on Edge switch 1. All ports must support the same speed and duplex mode.
   b. For the LAG between the Core switch and the third-party Edge switch 2, connect Core switch port 9 to a port on Edge switch 2 and connect Core switch port 10 to another port on Edge switch 2. All ports must support the same speed and duplex mode.
   c. For the LAG between the Core switch and the third-party Edge switch 3, connect Core switch port 11 to a port on Edge switch 3 and connect Core switch port 12 to another port on Edge switch 3. All ports must support the same speed and duplex mode.

   Caution: If the third-party switch does not support STP, skip this first step; Instead, first configure the LAG and then connect the cables, otherwise a network loop occurs.
2. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
4. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:
   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
5. Configure the LAG between the Core switch and the Edge switch 1:
   a. In the Managed Devices table, for the Core switch, click the **Configure** button.

      The Overview page displays.
   b. Select **Configure > Link Aggregation**.

      The Link Aggregation Group page displays.

c. Below the graphical display of the switch, click the **Create LAG** link.

   The Create Link Aggregation Group window displays.

d. In this example, select ports **7** and **8** that must become members of the LAG by clicking the individual ports.

e. In the **LAG Name** field, enter a name, for example **Core-Edge1**.

f. From the **Hash** menu, select the hash mode for the LAG.

   We recommend that you use the default hash mode (Layer 2: destination) and only select another hash mode if you notice problems with load balancing on the LAG. If you do notice problems, try the different hash modes to see which one works best for your application.

g. From the **LAG ID** menu, select a number, for example **4**.

   The number of IDs that are available depends on the switch model.

h. If the third-party Edge switch does not support a dynamic LAG, turn on the **Static** toggle so that it displays green and is positioned to the right.

i. Click the **Apply** button.

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

6. Repeat Step 5 to configure the LAG between the Core switch and the Edge switch 2, using the following LAG configuration:
   - In this example, select ports **9** and **10**.
   - For the LAG name, enter a name, for example **Core-Edge2**.
   - For the LAG ID, select an ID, for example **5**.
7. Repeat Step 5 to configure the LAG between the Core switch and the Edge switch 3, using the following LAG configuration:
   - In this example, select ports **11** and **12**.
   - For the LAG name, enter a name, for example **Core-Edge3**.
   - For the LAG ID, select an ID, for example **6**.
8. To save the settings to the running configuration, at the top right of the page, click the **Save** button.
9. To return to the Devices page of the controller, select **Devices Management**.
10. Configure the LAGs on the third-party Edge switch 1, Edge switch 2, and Edge switch 3.

    The LAG configuration depends on the vendor and switch model. Consult the documentation for your switch model.

11. If LACP (for a dynamic LAG) is not enabled but is supported, enable it on the third-party Edge switch 1, Edge switch 2, and Edge switch 3. (By default, LACP is enabled on a NETGEAR fully managed switch.)

    The LACP configuration depends on the vendor and switch model. Consult the documentation for your switch model.

    If the third-party switch does not support LACP, the LAG becomes a static LAG. (For a dynamic LAG, both partner switches must support LACP.)
12. If the third-party switch does not support STP, connect the cables after you complete the LAG configuration.

    For a third-party switch that does not support STP, a network loop occurs if you first connect the cables and then configure the LAG.

Create a single-tier MLAG for a redundant core

In a ProAV environment, you can use a single-tier multi-chassis link aggregation group (MLAG) to set up a redundant core of M4500 series switches. A redundant core can ensure that your ProAV network continues to operate even if part of the network fails.

In this single-tier MLAG switch configuration example, two M4500 series switches function as redundant core switches, with each switch connected to multiple M4250 series edge switches. If one core switch fails, the other maintains connectivity.

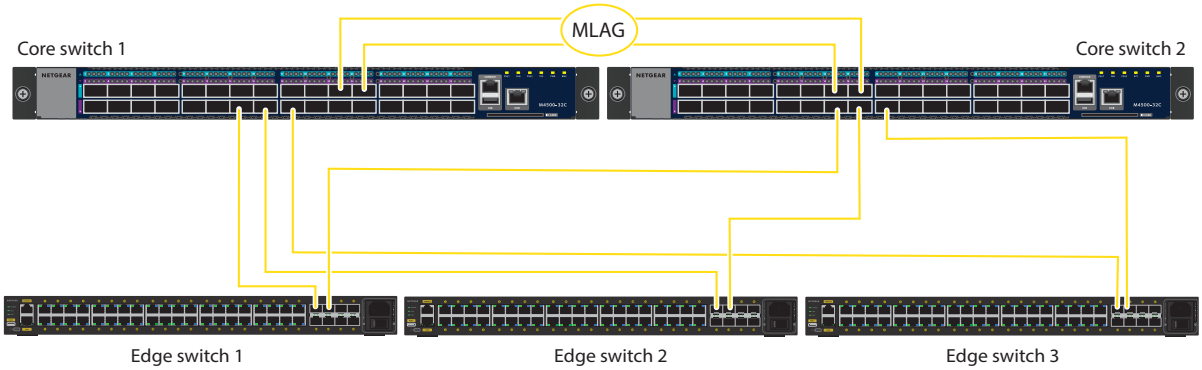


Figure 9. Core redundancy with an MLAG

To achieve network redundancy, all switches must be cabled to each other:

- Core 1 and Core 2 are connected through two cables to form a ring topology.
- Core 1 is directly connected to Edge 1, Edge 2, and Edge 3.
- Core 2 is directly connected to Edge 1, Edge 2, and Edge 3.

From the controller, you can set up and manage a single-tier MLAG with two M4500 series switches. After you configured a single-tier MLAG, the controller displays the MLAG switches as a single logical unit.

Note: You can also set up a double-tier MLAG with four M4500 series switches. For more information, see the "Set up a double-tier MLAG between four M4500 series switches" section in the NETGEAR Engage Controller User Manual.

To cable the switches for a single-tier MLAG, create a single-tier MLAG, and set the MLAG as the core switch:

1. Cable the switches for a single-tier MLAG with network redundancy:
   a. For core switch redundancy, do the following:
      - Connect port 21 on Core 1 to port 15 on Core 2
      - Connect port 23 on Core 1 to port 13 on Core 2
   b. For network redundancy with Core 1, do the following:
      - Connect port 14 on Core 1 to port 41 on Edge 1
      - Connect port 16 on Core 1 to port 41 on Edge 2
      - Connect port 18 on Core 1 to port 41 on Edge 3
   c. For network redundancy with Core 2, do the following:
      - Connect port 14 on Core 2 to port 43 on Edge 1
      - Connect port 16 on Core 2 to port 43 on Edge 2
      - Connect port 18 on Core 2 to port 43 on Edge 3
2. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
4. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

- **Make no changes to the network setup for the site**: Click the **Apply** button.
- **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

5. Set up a single-tier MLAG with the two M4500 series switches:
   a. In the Managed Devices table, click the **3 dots** icon next to the M4500 series switch you want to create the MLAG on, and select **Single-Tier MLAG**.

      The MLAG Peer Link Configuration page displays.
   b. From the **Select Switch** menu, select the other M4500 series switch to include in the MLAG.

      Both M4500 series switches must be identical models.
   c. Click the **Next** button.

      The window adjusts.
   d. In the **Assign a Domain ID** field, enter a domain ID for the MLAG.

      The name is for identification purposes only.
   e. Select the ports to define the peer link of the MLAG, and click the **Next** button.

      A message displays indicating that the port connections and port channels are successfully verified. If this message does not display, repeat this step.
   f. Click the **Submit** button.

      A pop up window displays to advise you that when you configure an MLAG, Spanning Tree Protocol (STP) is automatically disabled on the selected ports.
   g. Click the **OK** button.

      A message displays indicating that the MLAG peer link configurations are created successfully.
   h. Click the **OK** button.

      The single-tier MLAG is now created.

      In the Managed Devices table, a green X icon displays in the upper right corner of the M4500 product image to indicate the single-tier MLAG configuration. To see the details of the M4500 switches included in the MLAG tier or domain, point to the icon.
6. Set the M4500 series switches in the MLAG (that is, the *single* logical unit) as the core switch:
   a. Select **Topology**.

      The Site Topology page displays.
   b. Click the single logical unit that represents the two-tier MLAG.

A pop-up window displays details.

c. Turn on the **Core Device** toggle so that it displays blue or green and is positioned to the right.

By default, the core device option is disabled and the toggle displays gray and is positioned to the left.

The Core Switch pop-up menu displays.

d. Click the **Yes** button.

Your settings are saved.

7. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Create a two-switch stack for a redundant core

In a ProAV environment, you can use a two-switch stack to set up a redundant core, which can ensures that your ProAV network continues to operate even if part of the network fails. Other than this core redundancy option, we do not recommend stacking in a ProAV environment. A LAG or MLAG is more compatible with a ProAV environment with IGMP Plus.

Stacking is supported between M4300 series switches and between M4350 series switches. (You cannot mix M4300 series switches and M4350 series switches in a single stack.)

For a core redundancy option, the following limitations exist:

- Stacking and PTP residency time stamping (also referred to as PTPv2 transparent clock) are mutually incompatible. For a stack to be formed, you first might need to use the device UI of a participating fully managed switch to disable PTP residency time stamping for any network profiles that use it.
- Stacking and an SMPTE profile are incompatible. For example, you cannot create a redundant core and use the *Audio Video SMPTE* network profile or the *Hybrid SMPTE AES67 Core and Audio AES67 Edge* network profile.
- With MPEG video, a redundant core can work but each multicast signal is sent to the stack. To prevent flooding the stack link, we recommend that you calculate the bandwidth speed based on the sum of the traffic between the stacked switches plus 25 percent extra capacity.
- If you use a network profile with Dante audio, you can configure a redundant core if you do not activate AES67 on the Dante interfaces.

In this stacked core switch configuration example, two M4350 series switches function as redundant core switches, with each switch connected to multiple M4250 series edge switches. If one core switch fails, the other maintains connectivity.

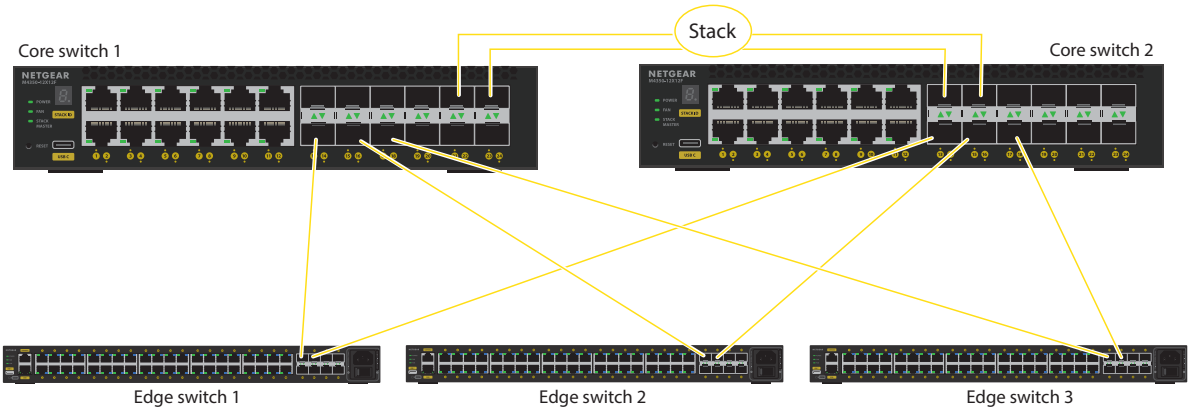


Figure 10. Core redundancy

To achieve network redundancy, all switches must be cabled to each other:

- Core 1 and Core 2 are connected through two cables to form a ring topology.
- Core 1 is directly connected to Edge 1, Edge 2, and Edge 3.
- Core 2 is directly connected to Edge 1, Edge 2, and Edge 3.

From the controller, you can set up and manage a stack of two core switches. After you configured two stacked switches, the controller displays the stacked switches as a single logical unit.

To cable the switches for redundancy, create a stack of two switches, and set the stack as the core switch:

1. Cable the switches for stacking and redundancy:
   a. For core switch redundancy, connect port 21 on Core 1 to port 15 on Core 2, and then connect port 23 on Core 1 to port 13 on Core 2.
   b. For network redundancy with Core 1, connect port 14 on Core 1 to port 41 on Edge 1, connect port 16 on Core 1 to port 41 on Edge 2, and connect port 18 on Core 1 to port 41 on Edge 3.
   c. For network redundancy with Core 2, connect port 14 on Core 2 to port 43 on Edge 1, connect port 16 on Core 2 to port 43 on Edge 2, and connect port 18 on Core 2 to port 43 on Edge 3.
2. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

3. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

4. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

5. Set up a stack with the two M4350 series switches:
   a. In the Managed Device table, for one M4350 series switch, click the **3 dots** icon and select **Stack**.

      The Create Stack pop-up window display.

   b. From the **Select Stack** menu, select the other M4350 series switch for the stack.

      Only switches that are stackable display.

   c. Click the **Next** button.

      The window adjusts.

   d. In the **Device Name** field, enter a name for the stack.

      The name is for identification purposes only.

   e. Set one of the switches as stack management switch by enabling the **Management** toggle in the graphic display for the switch so that the toggle displays blue or green and is positioned to the right.

      The **Management** toggle for the other switch is disabled, displays gray, and is positioned to the left. The other switch functions as the standby switch in the stack.

   f. In the graphical display for each switch, select the stack port or ports.

      The stack ports form the stack connection between both switches. You can assign up to eight stack ports to establish the connection between the management switch and the standby switch.

   g. Click the **Next** button.

      The window adjusts.

   h. Click the **Create** button.

      The Validate Port Connection pop-up window displays.

i. Click the **Yes** button.

The port connections are being verified. If the process is successful, the window adjusts and displays a confirmation message.

j. Click the **Reboot Now** button.

The two switches in the stack reboot. After the switches complete the reboot process, the controller displays the stacked switches as a single logical unit.

In the Managed Devices table, a green X icon displays in the upper right corner of the switch product image to indicate the stack. To see the details of the switches included in the stack, point to the icon.

6. Set the stacked M4350 series switches (that is, the *single* logical unit) as the core switch:

a. Select **Topology**.

The Site Topology page displays.

b. Click the single logical unit that represents the two stacked switches.

A pop-up window displays details.

c. Turn on the **Core Device** toggle so that it displays blue or green and is positioned to the right.

By default, the core device option is disabled and the toggle displays gray and is positioned to the left.

The Core Switch pop-up menu displays.

d. Click the **Yes** button.

Your settings are saved.

7. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

6

Security

The chapter includes the following sections:

Enable 802.1x port security for individual ports using a RADIUS server

In some managed or enterprise AV networks, you might want to use 802.1X port-based security to restrict access to only authorized devices. 802.1X requires a RADIUS server to authenticate connected devices. Without a RADIUS server, you cannot use 802.1X.

For example, in secure environments where devices must not be swapped without authorization, 802.1X can block unauthorized devices—such as someone connecting a laptop in place of a network camera.

Note: For information about a security feature that can secure WiFi access and that does not require a RADIUS server, see Import and apply a MAC ACL that allows access to WiFi clients on page 97.

802.1X is typically used in enterprise or highly managed AV networks that require centralized authentication and strict access policies. 802.1X is normally not used in standalone AV-over-IP deployments where physical port security or VLAN isolation might be sufficient.

By default, all ports are authorized and connected client devices do not need to be authorized. If you enable global 802.1x access mode, by default, all ports on the switch are set to Auto. Individual switches that are managed through the controller support 802.1x port authentication, which you manage through the AV UI that is accessible from the controller:

- **802.1x port authentication**: 802.1x authentication applies only to the individual ports for which you enable authentication on a switch and select the authentication mode.
- **Global 802.1x access authentication**: 802.1x authentication applies to all ports on a switch.

  Caution: If you globally enable 802.1x port security for all ports on a switch, be sure that you first set all uplink ports to Force-Authorized, otherwise the switch might lose access to the Internet.

The authentication mode for a port can be set to one of the following modes:

- **Auto**: Access to the port depends on the authentication exchanges between the supplicant (the client device), the authenticator (the switch), and the authentication

server (the RADIUS server). If you enable global 802.1 access mode, this is the default setting.

- **Force-authorized**: The port is set to authorized and the connected client device does not need to be authorized by the RADIUS server. This is the default setting for all ports when 802.1x is not enabled, either globally for the switch or individually for a port.

  Be sure that you keep the setting for all uplink ports to Force-Authorized, otherwise the switch might lose access to the Internet.
- **Force-unauthorized**: The port is set to unauthorized and the connected client device cannot be authorized.

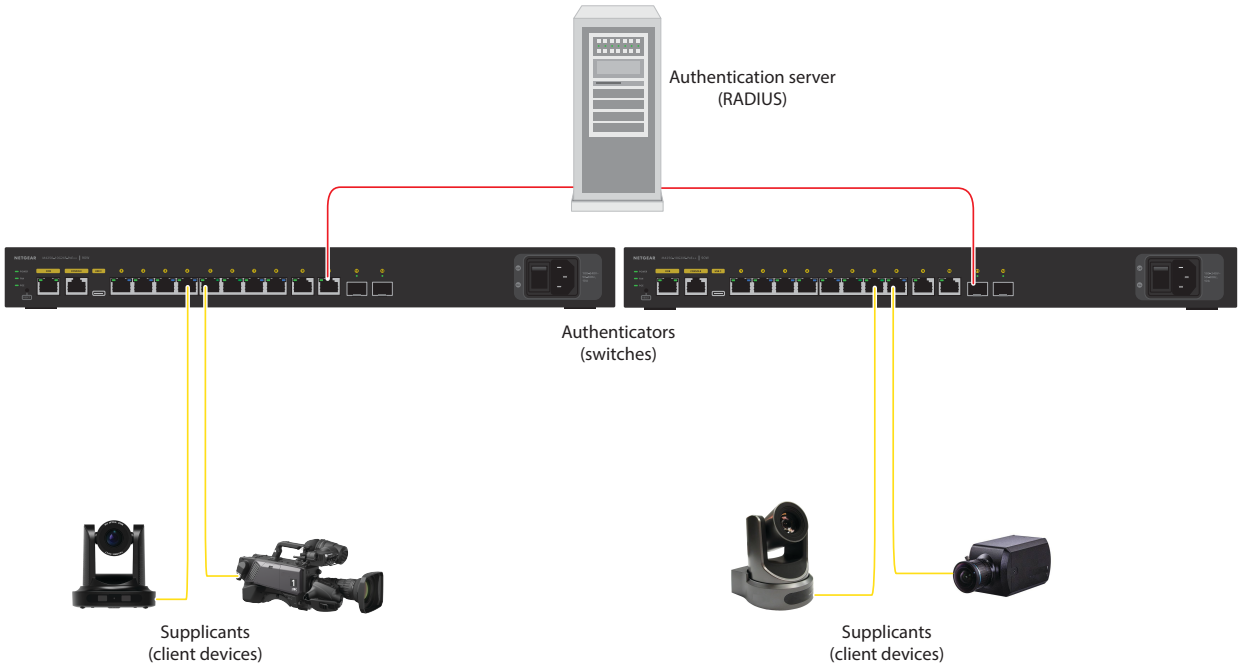


Figure 11. 802.1x port security

To enable 802.1x port security for individual ports using a RADIUS authentication server:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site**: Click the **Apply** button.
- **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Configure the basic settings for the RADIUS server:
   a. In the Managed Devices table, for the switch that you want to configure, click the **Configure** button.

      The Overview page displays.

   b. Select **Security**.

      The Security page displays.

   c. In the RADIUS Server Settings section, click the **+ Add Server** link.
   d. Configure the settings for the RADIUS server by completing the following fields:
      - **RADIUS Address**: The IP address of the RADIUS server.

        The switch must be able to reach this IP address.

      - **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.

   e. Click the **Apply** button.

      Your settings are saved.

5. For the uplink ports, make sure that the authentication mode is force-authorized:
   a. On the Security page, select the uplink ports.
   b. From the menu below the graphical display, select **Force-authorized**.

      The port is set to authorized and the connected client device does not need to be authorized by the RADIUS server. This is the default setting for all ports when 802.1x is not enabled, either globally for the switch or individually for a port.

      All uplink ports must be set to Force-Authorized, otherwise the switch might lose access to the network or Internet.

   c. Click the **Apply** button.

      Your settings are saved.

6. For the ports that you want to secure, set the authentication mode to Auto:

a. On the Security page, select the ports that you want to secure with port authentication.
b. From the menu below the graphical display, select **Auto**.

   This setting means that access to the port depends on the authentication exchanges between the supplicant (the client device), the authenticator (the switch), and the authentication server (the RADIUS server).
c. Click the **Apply** button.

   Your settings are saved.

7. To save the settings to the running configuration, at the top right of the page, click the **Save** button.
8. To return to the Devices page of the controller, select **Devices Management**.

Block routing between two or more VLANs

In most networks, by default, VLANs are isolated to prevent communication between clients on different VLANs. However, in a ProAV network that is managed through the controller, by default, inter-VLAN routing is *enabled* between all VLANs, allowing communication between clients on different VLANs. As a security measure, you can disable (block) inter-VLAN routing between two or more VLANs.

To disable routing between two or more VLANs:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Site Settings > VLAN Routing and DHCP Server**.

   The Basic Configuration page displays.

5. From the menu in the left panel, select **Advanced > Inter-VLAN Routing**.

   The Inter-VLAN Routing page displays.

6. Click the **Add Rule** button.

   The Add Rule pop-up window displays.

7. From the upper **VLAN** menu, select a single VLAN, and from the lower **VLAN** menu, select one or more VLANs.

   Your selections determine the VLANs between which inter-VLAN routing must be blocked.

8. Click the **Add** button.

   Your settings are saved. The inter-VLAN rule is added to the table, and a Deny icon displays on the left.

9. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Disable broadcast storm control for a port

By default, broadcast storm control is enabled for all ports, and we recommend that you keep it enabled. However, in an uncommon situation, you might want to disable broadcast storm control for a port.

For example, in a network with multiple switches in which you use a network profile that is based on the *Allen & Heath -- gigaACE/TG* profile template or the *CobraNet* profile template, you must disable broadcast storm control on the uplink port to prevent packets from being dropped.

To disable broadcast storm control for a port:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
4. In the Managed Devices table, for the switch with the port that you want to configure, click the **Configure** button.

   The Overview page displays.
5. Select **Configure > Port Configuration**.

   The Port Configuration page displays.
6. Select the check box for the port.
7. From the **Broadcast Storm Control** menu, select **Disable**.
8. Click the **Apply** button.

   Your setting are saved.
9. To save the settings to the running configuration, at the top right of the page, click the **Save** button.
10. To return to the Devices page of the controller, select **Devices Management**.

7

Multicast

Internet Group Management Protocol (IGMP) in IPv4 networks and Multicast Listener Discovery (MLD) in IPv6 networks are widely used multicast protocols that are supported at the network layer. IGMP and MLD are used by hosts and their adjacent routers to let hosts inform the multicast source that they want to receive, continue receiving, or stop receiving a multicast streams.

Another option is Layer 3 Protocol Independent Multicast (PIM), which is used in more complex networks where the senders and receivers are located on different subnets of a network. PIM multicast routing is generally more complicated to set up than IGMP, but allows for greater control over routing between subnets. You cannot configure PIM in the controller, but you can do in the main UI for a switch (see the information about the PIM-SM Tech Guide below).

Selecting the correct network profile in the controller is all that you need to do to enable multicast and IGMP or MLD. You do not need to configure multicast manually.

The chapter includes the following sections:

- Change the IGMP Querier selection
- Monitor multicast traffic at the network, switch, and port level

The following multicast related Tech Guide is available at the NETGEAR ProAV site:
Configuring PIM-SM

Change the IGMP Querier selection

In a VLAN with switches that participate in the IGMP Querier selection, the switch with the lowest numbered IP address is selected as the querier. Any other querier moves to the non-querier state.

The following flowchart describes the IGMP Querier selection process.

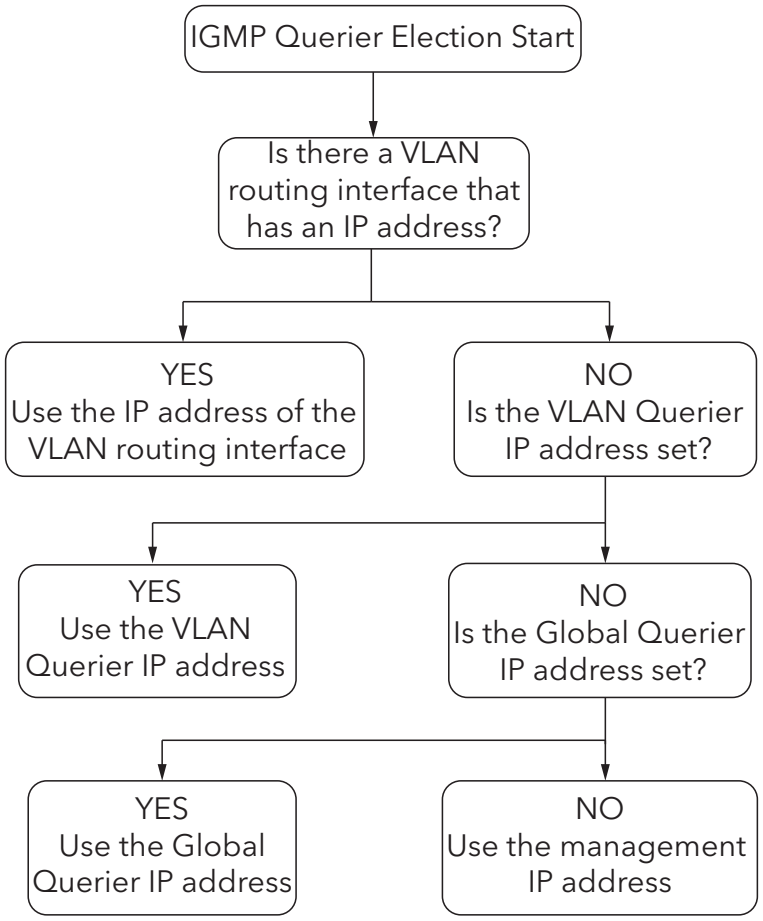


Figure 12. IGMP Querier selection flowchart

For best performance and predictability, we recommend that you configure the core switch as the IGMP Querier and that you make sure that you network includes a single IGMP Querier only. If your network includes redundant core switches (for more information, see LAGs, MLAGs, and switch stacks for redundancy and enhanced bandwidth on page 53), we recommend that you assign the lowest-numbered IP address (for example, 192.168.100.1) to the primary core switch and the second-to-lowest IP address (for example, 192.168.100.2) to the secondary core switch.

The IGMP Querier selection process uses the following IP addresses:

- **IP address present on the VLAN**: If the switch has an IP address on the VLAN, the switch uses that IP address for the IGMP selection process, even if the switch is assigned a Querier VLAN IP address.
- **No IP address present on the VLAN**:
  - **Querier VLAN IP address present**: If the switch does not have an IP address on the VLAN but is assigned a Querier VLAN IP address, the switch uses that address for the IGMP selection process.
  - **No Querier VLAN IP address present**: If the switch does not have an IP address on the VLAN and is not assigned a Querier VLAN IP address, the switch uses its management VLAN IP address for the IGMP selection process.

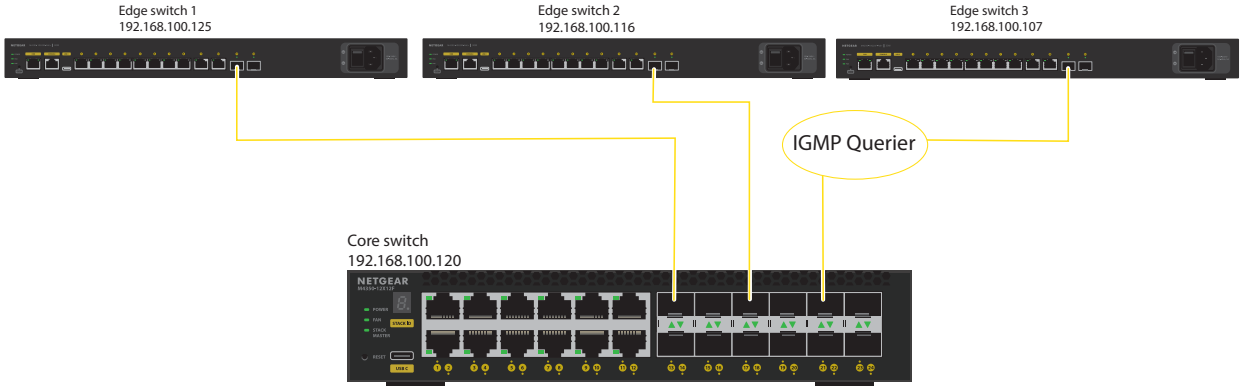


Figure 13. IGMP Querier and IP addresses

In this example, the Core switch has an IP address of 192.168.100.120 on the Default VLAN with ID 1. (This example does not include a secondary core switch.) Three edge switches are assigned IP addresses on VLAN 1:

- Edge switch 1 is assigned 192.168.100.125
- Edge switch 2 is assigned 192.168.100.116
- Edge switch 3 is assigned 192.168.100.107

If all four switches (that is, the core switch and the three edge switches) are set to participate in the IGMP election process, Edge switch 3 is elected as the IGMP Querier because it has the lowest numbered address on VLAN 1. In the following example task, the IGMP Querier is changed to the Core switch by changing the IP address of the Core switch to a lower-numbered IP address.

To change the IGMP Querier selection on VLAN 1 from the Edge switch 3 to the Core switch:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. Site **Settings > VLAN Routing and DHCP Server**.

   The Basic Configuration page displays. (In the menu in the left pane, Basic is selected by default.)

5. From the **VLAN Routing** menu, select **Default**.

   1 displays as the VLAN ID.

6. For the Core switch, select the **Static** check box.

   In the **IP Address** field, enter **192.168.100.1**. This IP address is now the lowest-numbered IP address in VLAN 1.

7. Click the Apply button.

   A warning pop-up window displays.

8. Click the **Yes** button.

   Your settings are saved.

9. Select **Site Settings > IGMP Querier**.

   The IGMP Querier page displays.

   The Core switch now displays as QUERIER and the Edge 3 switch as NON-QUERIER.

10. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Monitor multicast traffic at the network, switch, and port level

You can monitor multicast traffic in the controller at the network level, switch and VLAN level, and port connection level (that is, the connection between two ports). The information that is displayed includes bit rate, dropped packets, and physical errors.

For information about monitoring multicast *groups*, see the "Display the multicast groups in your network" section in the NETGEAR Engage Controller User Manual.

For information about displaying which switch is the IGMP Querier, see the "Configure an IGMP querier for a routing VLAN" section in the NETGEAR Engage Controller User Manual.

To monitor multicast traffic at the network level, switch and VLAN level, and port connection level:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
4. **Network level**. To monitor bit rate, dropped packets, and physical errors at the network level:
   a. Select **Network Monitoring > Network Statistics**.

      The Network Statistics page displays, showing bit rate, dropped packets, and physical errors.
   b. To narrow down the information that displays or search for a device name, device model, network profile, or VLAN ID, click in the field in the table header, and select the check box for one or more options, and then click the **Apply** button.

The information in the table adjusts.

c. To search for a port, in the **Port** field, type the port number in the format *unit number/slot number/port number*.

The information in the table adjusts.

d. To filter on switch type, interface medium, link state, interface type, or link type, do the following:

i. At the right of the page, click the **<** (left arrow) icon.

The Filter icon displays.

ii. Click the **Filter** icon.

The Filter pop-up window displays.

iii. Select one or more check boxes, and click the **Apply** button.

(To clear your selection, clear the check boxes, and click the **Apply** button.)

iv. To close the Search window, at the top right of the window, click the **x**.

e. To group the information in the table by switch type, port, VLAN IDs, or link speed, do the following:

i. At the right of the page, click the **<** (left arrow) icon.

A menu with icons displays.

ii. Click the **Group By** icon.

The Group By pop-up window displays.

iii. Select the **Switch Type**, **Port**, or **VLAN ID**, or **Link Speed** radio button, and click the **Apply** button.

The information in the table adjusts. By default, the Switch Type radio button is selected.

iv. To close the pop-up window, at the top of the window, click the **x**.

f. To reset all counters, at the top right of the page, click the **Reset All Counters** link.

g. To export the information that displays in the table, at the top right of the page, click the **Export** link, and save the .csv file on your computer.

5. **Switch and VLAN level**. To monitor bit rate, dropped packets, and physical errors at the switch level:

a. Select **Topology**.

The Site Topology page displays. The default topology type is Tree View, unless you set another default type.

b. At the right of the page, click the **<** (left arrow) icon, and select the **topology** icon.

The Topology Views pop-up window displays.

c. Select the **Physical Topology** radio button, and close the Topology Views window by clicking the **x** at the top right of the window.

d. Click a device.

A pop-window displays.

e. From the **Select VLAN** menu, select a **VLAN**, and turn on the **Watch List** toggle so that it displays blue or green and is positioned to the right.

Information for the switch and VLAN displays, showing bit rate, dropped packets, and physical errors.

f. To close the pop-up window, at the top right of the window, click the **x**.

6. **Port connection level**. To monitor bit rate, dropped packets, and physical errors at the port connection level:

a. Click a connection dot between two devices.

A pop-up window with a table displays information about the port numbers and port speeds and connection statistics, including bit rate, dropped packets, and physical errors.

b. To add the ports or LAGs that form the connection between the devices to the monitor, click the **Add to Monitor** button.

The Show Monitoring toggle is automatically enabled so that it displays blue or green and is positioned to the right.

c. To close the pop-up window, click the **x**.

The Site Topology page now displays the monitor, which is a table that shows information about traffic bit rates, physical errors, and dropped packets for the ports that you added in the previous substeps.

d. The clear the counters for a port or LAG, click the **Clear Counters** button.

To remove a port or LAG from the monitor, click the **trashcan** (Delete) icon, and in the Delete Watch List pop-up window that displays, click the **Delete** button.

e. To hide the monitor, turn off the **Show Monitoring** toggle so that it displays gray and is positioned to the left.

f. To set threshold for bandwidth utilization, packets errors, and packets drops, do the following:

i. Click the **Set Threshold** link.

The Threshold pop-up window displays.

ii. To set a percentage for bandwidth utilization, physical errors, and packets drops, move each slider to the desired position.

The settings applies to the entire network.

iii. Click the **Apply** button.

Your settings are saved. The pop-up window closes.

g. To reset all counters on all devices, do the following.
   i. Click the **Reset all counters** link.
      A Warning pop-up window displays.
   ii. Click the **Yes** button.
      The pop-up window closes.

8

Services

The chapter includes the following sections:

The following DHCP service related Tech Guide is available at the NETGEAR ProAV site:

Configuring DHCP Reservations Using Engage

Change the STP root bridge in the network

If you have redundant connections between network devices, loops can exist, which can bring devices down and create problems in the network. The purpose of Spanning Tree Protocol (STP) is to eliminate loops in the network by electing one switch as the root bridge, which is the switch that can forward packets, and moving the other switches to the non-root state, which prevents the switches from forwarding packets. By default, Rapid STP (RSTP) is enabled on the switches.

Note: In a ProAV network, we recommend that you do not change STP to Multiple STP (MSTP) because IGMP+ might no longer function as designed.

In a network with switches that participate in STP root bridge selection, the switch with the lowest bridge ID is elected as the root bridge. The bridge ID is made up of the priority value and the MAC address.

By default, most switches, including NETGEAR switches, are assigned a priority of 32,768, which is the IEEE standard default. As a result, the switch with the lowest MAC address is typically selected as the STP root bridge. All other switches become non-root switches and calculate the shortest path to the root bridge. The shortest path is based on port cost, which considers interface speed, not just physical distance or hop count.

We recommend that you set the core switch as the root bridge by changing the STP priority the core switch to the primary mode with priority 0. If your network includes redundant core switches (for more information, see LAGs, MLAGs, and switch stacks for redundancy and enhanced bandwidth on page 53), we recommend that you assign the one but lowest-numbered priority (for example, 8192) to the secondary core switch.

Note: STP priorities are set in increments of 4,096. The lowest priority is 0, the next lowest priority is 4,096, and the one after that is 8,192, and so on.

Table 5. Default STP network redundancy values in the AV UI

Mode in the AV UI	Associated Bridge Priority Value
Primary mode	0
Neutral mode	32768
Backup mode	8192

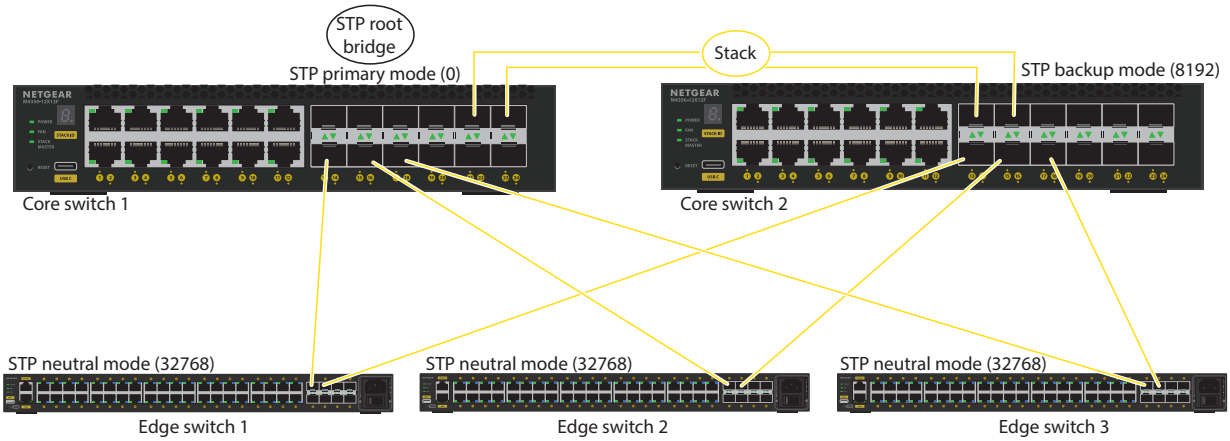


Figure 14. STP root bridge in the network

In this example, we change the STP priority of the core switch to the primary mode with priority 0, and the STP priority of the secondary core switch to the backup mode with priority 8,192. The results is that the core switch becomes the STP root bridge, and the redundant core switch becomes the backup STP root bridge.

To change the STP priority of the primary and secondary core switches and display links that are blocked by STP to prevent loops (if any such links are present):

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site**: Click the **Apply** button.
- **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

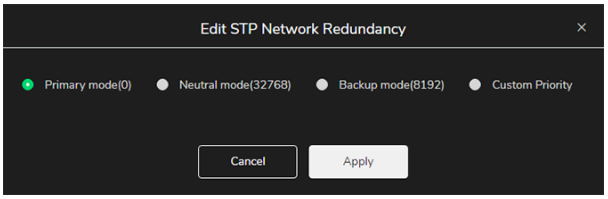
4. Change the STP priority of the primary core switch:
   a. In the Managed Devices table, for the primary core switch, click the **Configure** button.

      The Overview page displays.

   b. In the Device Details section, below to the STP Network Redundancy field, click the **pencil** icon.

      The Edit STP Network Redundancy window displays.

   c. Select the **Primary mode (0)** radio button.



   d. Click the **Apply** button.

      Your settings are saved. The window closes. The Overview page displays again.

   e. Select **Devices Management**.

      The Devices page of the controller displays.

5. Change the STP priority of the secondary core switch:
   a. In the Managed Devices table, for the secondary core switch, click the **Configure** button.

      The Overview page displays.

   b. In the Device Details section, below to the STP Network Redundancy field, click the **pencil** icon.

      The Edit STP Network Redundancy window displays.

   c. Select the **Backup mode (8192)** radio button.

   d. Click the **Apply** button.

      Your settings are saved. The window closes. The Overview page displays again.

   e. Select **Devices Management**.

      The Devices page of the controller displays.

6. To save the settings to the running configuration, at the top right of the page, click the **Save** button.
7. To return to the Devices page of the controller, select **Devices Management**.
8. Display links that are blocked by STP to prevent loops (if any such links are present):
   a. Select **Topology**.

      The Site Topology page displays. The default topology type is Tree View, unless you set another default type.
   b. At the right of the page, click the **<** (left arrow) icon.

      A menu with icons displays.
   c. Click the **topology** icon.

      The Topology Views pop-up window displays.
   d. Select the **Physical Topology** radio button.

      The topology adjusts.
   e. Enable the **Show STP** toggle.

      The toggle displays blue or green and is positioned to the right.

      A connection between two devices that displays with a dashed line indicates a link that is blocked by STP.

      If no dashed lines display, STP did not detect any loops and did not block any links.

Import a list of devices for DHCP address reservation

For you to be able to import a list of devices into the controller for which you want to reserve DHCP addresses, you first must enable routing for a VLAN and then configure a DHCP server for the routing VLAN.

In this example, we assume that you already created VLAN 100 when you set up a new network profile with the name Broadcast AVB but did not make VLAN 100 the management VLAN.

The example procedure describes how you can enable routing on VLAN 100, configure a DHCP server for VLAN 100, and finally import the following spreadsheet in CSV format with host names, MAC addresses, and IP addresses for DHCP reservation:

host	MAC address	IP address
Edge1_Studio	44:a5:6e:61:40:b0	192.168.100.150
Edge2_Control	44:a4:5e:31:39:b2	192.168.100.151
Edge3_Equipment	44:a3:4e:11:28:b4	192.168.100.152

The CSV file must include the table headings in the order that is shown above. On each row, the first column must include the host name, the second column the MAC address, and the third column the IP address.

To enable routing for VLAN 100, configure a DHCP server for VLAN 100, and then import the contents of the CSV file for DHCP address reservation:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
4. Enable routing for VLAN 100:
   a. Select **Site Settings > VLAN Routing and DHCP Server**.

      The Basic Configuration page displays. (In the menu in the left pane, Basic is selected by default.)
   b. At the top right of the Basic Configuration page, click the **Enable New VLAN Routing** link.

      The VLAN Routing Planner pop-up window displays.
   c. Select the radio button for the **Broadcast AVB** network profile, which uses VLAN 100.
   d. Click the **Apply** button.

      The VLAN Routing Planner page displays.
   e. Select the **Enable Routing on all Switches** check box.

This selection enables routing on all switches that use the Broadcast AVB network profile.

f. Click the **Apply** button.

Your settings are saved.

5. Enable and configure the DHCP server for VLAN 100:

a. Remain on the Basic Configuration page.

(If you are not on the Basic Configuration page, select **Site Settings > VLAN Routing and DHCP Server**.)

b. In the table, select the **DHCP Server** check box for the switch on which you want to enable the DHCP server.

We recommend that you use the core switch as the DHCP server.

c. In the **IP Address** and **Subnet Mask** fields, type the **192.168.100.5** as the IP address and **255.255.255.0** as the subnet that must be assigned to the DHCP server.

This configuration assumes that the switch is a DHCP client that is assigned 192.168.100.5 as the IP address and 255.255.255.0 as the network mask. If you now use the switch itself as a DHCP server, you can use the same IP address and subnet mask that were assigned before, but the IP address and subnet mask then become static, and the DHCP client function of the switch is disabled.

In the DHCP Server section, the Default Router, DHCP Server Pool Start, and DHCP Server Pool End fields are automatically filled based on the IP address and subnet mask that you set for the DHCP server.

d. In the DHCP Server section, configure the DHCP pool and DNS server setting:

- **Default Router**: The IP address of the router for the DHCP pool. By default, this IP address is the same address as the VLAN IP address (192.168.100.5).
- **DHCP Server Pool Start and DHCP Server Pool End**: Type **192.168.150** as the pool start IP address en **192.168.100.199** as the pool end IP address.

  When you set the IP address of the default router to 192.168.100.5, the pool start address was automatically set to 192.168.100.6 and the pool end address was automatically set to 192.168.100.254.
- **DNS Server 1**: Type the IP address for the primary DNS server.

  The choice of DNS servers depends on the scale of the network. For a large scale network, use the local DNS server. For a smaller network where no local DNS server is available, you can use Cloudflare with IP address 1.1.1.1 as the primary DNS server and Quad9 with IP address 9.9.9.9 as the secondary (or backup) DNS server.
- **DNS Server 2**: Optionally, type the IP address for the secondary DNS server.

- **Search Domain**: The domain name for the DHCP server. This name is a fully qualified domain name (FQDN). For example, type Broadcast_AVB_Domain.
- **Lease Time**: Type the time in minutes that the IP address is leased to the client. The default is 240 minutes.

e. Click the **Apply** button.

A warning pop-up window displays.

f. Click the **Yes** button.

Your settings are saved.

6. Import the contents of the CSV file for DHCP address reservation:
   a. Remain on the Basic Configuration page.

   (If you are not on the Basic Configuration page, select **Site Settings > VLAN Routing and DHCP Server**.)

   b. From the menu in the left panel, select **Advanced > DHCP Address Reservation**.

   The DHCP Address Reservation page displays.

   c. Click the **Import** button.

   The Import IP Reservation List pop-up window displays.

   d. Click the **Browse** button, navigate to the CSV file, and select it.
   e. Click the **Import** button.

   The address reservations are added and the DHCP Address Reservation page displays again.

   The page shows the Edge1_Studio switch, Edge2_Control switch, and Edge3_Equipment switch, each with their associated MAC address and IP address.
7. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

9

Topologies and Monitoring

The chapter includes the following sections:

- Recommended AV network topologies
- Set monitoring thresholds for bandwidth utilization, physical errors, and packets drops for a link
- Add a topology location image and place devices on the image

Recommended AV network topologies

We recommend that you use a star topology for an AV network. A star topology reduces latency and makes the network better predictable.

For an AV network that uses an SMPTE or AES67 network profile, and where PTPv2 is enabled, you must use a star topology. That is, do not use another type of topology.

We also recommend that you do not use a bus topology in an AV network, nor in an audio-only network with Dante.

Set monitoring thresholds for bandwidth utilization, physical errors, and packets drops for a link

Using the physical topology, you can set monitoring thresholds from 0 percent to 100 percent for a link between two network devices:

- **Bandwidth utilization**: Monitor the transmit (Tx) bitrate and received (Rx) bitrate for the port at each end of a link.
- **Packets errors**: Monitor the transmit (Tx) packets errors and received (Rx) packet errors for the port at each end of a link.
- **Packets drops**: Monitor the transmit (Tx) packets drops and received (Rx) packet drops for the port at each end of a link.

These monitoring thresholds let you identify connection problems where the bandwidth utilization is too high or where too many packets errors and packet drops occur.

Note: The thresholds are for monitoring only, that is, the actual traffic is not affected by the thresholds.

To set a monitoring threshold for bandwidth utilization, physical errors, and packets drops for connections for the port at each end of a link:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. Select **Topology**.

   The Site Topology page displays. The default topology type is Default and the default topology view is Tree View.

5. At the right of the page, click the **<** (left arrow) icon.

   A menu with icons displays.

6. Click the **topology** icon.

   The Topology Views pop-up window displays.

7. Select the **Physical View** radio button.

   The topology adjusts.

8. To close the Topology Views window, at the top right of the window, click the **x**.

9. To monitor the port at each end of a link, do the following:

   a. Click a connection dot between two devices.

      A pop-up window with a table displays information about the port numbers and port speeds and connection statistics.

   b. Add the ports or LAGs that form the connection between the devices to the monitor, by clicking the **Add to Monitor** button.

      The Show Monitoring toggle is automatically enabled so that it displays blue or green and is positioned to the right.

   c. To close the pop-up window, click the **x**.

      The Site Topology page now displays the monitor, which is a table that shows information about traffic bit rates, physical errors, and dropped packets for the ports that you added in the previous substeps.

10. To set a threshold for bandwidth utilization, packets errors, and packets drops, do the following:
    a. Click the **Set Threshold** link.

       The Threshold pop-up window displays.
    b. To set a percentage for bandwidth utilization, physical errors, and packets drops, move each slider to the desired position from 0 percent to 100 percent.

       The settings applies to the entire site.
    c. Click the **Apply** button.

       Your settings are saved. The pop-up window closes.
11. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

Add a topology location image and place devices on the image

For a site, you can add a topology location image such as map or floor plan and place devices on the map or plan. For example, the map could display a large auditorium, small auditorium, and control room, along with the devices that are located at the auditoriums and control room.

Note: The topology location is for monitoring only.

To add a topology location image and move devices on the image:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

- **Make no changes to the network setup for the site**: Click the **Apply** button.
- **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Topology**.

   The Site Topology page displays. The default topology view is Tree View, unless you already changed the default topology view.

5. At the right of the page, click the **<** (left arrow) icon.

   A menu with icons displays.

6. Click the **topology** icon.

   The Topology Views pop-up window displays.

7. Select the **Abstract View** radio button.

   The topology adjusts.

8. In the **BG Image** field, click the **Upload** button, and then navigate to and select a background image such as a map or floor plan.

   The Upload Image pop-up window display the selected image.

9. As an option, turn, resize, or crop the image, and when you are done, click the **flag** button at the right.

   The image is set as the background image on the Site Topology page.

10. To move a device on the image, select the device and move it to the desired location.
11. To save the settings to the running configuration, at the top right of the page, click the **Save** button.

10

Access points and WiFi

The chapter includes the following sections:

The following access point and VLAN related Tech Guide is available at the NETGEAR ProAV site:

Configuring Access Points with Multiple VLANs

Add WiFi with WPA3/WPA2 - PSK security to your network

The information in this section applies only if your network includes access points (APs). In this section, SSID is the same as a WiFi network.

If you let the controller onboard one or more APs, you must set up a global site SSID. This is the default WiFi network that is associated with the Default network profile with VLAN ID 1, broadcasts on the 2.4 GHz and 5 GHz radios (but not on the 6 GHz radio, if supported by the APs), and uses WPA2 - MPSK as security.

You can either add the global site SSID when you set up the controller or add it when you onboard the first AP at a site. After setup, you cannot delete the global site SSID or change the type of WiFi security. However, you can add another SSID and apply it to the Default network profile and other profiles.

In this example procedure, we are adding an SSID with WPA3/WPA2 - PSK security. This type of security is very common and supports both WPA3 devices and legacy WPA2 devices. WPA2 - PSK (which uses AES) is less secure than WPA3 - PSK (which uses SAE).

To set up a WiFi network that uses WPA3/WPA2 - PSK security:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
4. Select **Site Settings > Wireless**.

   The SSID page displays.
5. Click the **+ Add New SSID** link.

   The Create New SSID page displays.

6. In the **SSID** field, type the WiFi network name.

   The SSID is the WiFi network name. Type a name for the SSID with a maximum of 32 characters. You can use a combination of alphanumeric and special characters, except for quotation marks (") and a backslash (\).

   For a WiFi device to be able to connect to the AP, the SSID on the WiFi device must match the SSID of the AP.
7. Select the WLAN Status **Enable** radio button, which enables the SSID after you complete and save the SSID configuration.
8. Select the Radio Band **2.4 GHz** and **5 GHz** check boxes.

   Note: Even if the AP supports the 6 GHz radio band, if you select the 6 GHz check box, the WPA3/WPA2 - PSK security is not available. If you want to use the 6 GHz band, you can use WAP3 - PSK security. However with WAP3 - PSK security, some legacy WiFi devices do not detect WPA3 and support only WPA2. Therefore, if your network also includes WPA2 devices, a better option is to use WPA3/WPA2 - PSK security.
9. Specify the WiFi security by selecting **WPA3/WPA2 - PSK** from the **Security** menu.

   This option enables WiFi devices that support either WPA3 or WPA2 to join the WiFi network.
10. Set a passphrase in the **Passphrase** field by entering a phrase of 8 to 63 characters.
11. From the **VLAN ID** menu, select the VLAN to which the WiFi network must be assigned.
12. Click the **Save** button.

    Your changes are saved.
13. To save the settings to the running configuration, at the top right of the page, click the **Save** button.
14. Make sure that a WiFi client can connect to the new WiFi network, and check to see that the WiFi client displays on the Tree View page of the site topology by doing the following:
    a. Select **Topology**.

       The Site Topology page displays. The default topology type is Tree View.
    b. At the right of the page, click the **<** (left arrow) icon.

       A menu with icons displays.
    c. Click the **topology** icon.

       The Topology Views pop-up window displays. By default, the Tree View radio button is selected, and the topology displays as a tree.
    d. Turn on or the **Show Wireless Clients** toggle.

The toggle displays blue or green and is positioned to the right.

The WiFi client displays.

15. If the WiFi client does not display or cannot connect to the new WiFi network, check the following:

    - If the WiFi-enabled computer or mobile device is already connected to another WiFi network in the area, ask the user to disconnect it from that WiFi network and connect it to the correct WiFi network. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
    - If the WiFi-enabled computer or mobile device is trying to connect to the network with its old settings (before the user changed the settings), ask the user to update the WiFi network selection in the WiFi-enabled computer or mobile device to match the current settings for the network.
    - Does the user try to connect using the correct WiFi network name (SSID) and password?
    - If applicable, make sure that the WiFi adapter device driver is updated to the latest version on the WiFi-enabled computer or mobile device.

Import and apply a MAC ACL that allows access to WiFi clients

The information in this section applies only if your network includes access points (APs). In this section, SSID is the same as a WiFi network.

You can import an existing access control list (ACL) that is based on up to 512 MAC addresses. You can import the list into any MAC ACL, but the MAC addresses on the list are available only for the MAC ACL into which you import the list. That is, if you want to use the same list in another MAC ACL, you must also import the list into that MAC ACL.

The file with MAC addresses must be in the following format:

- Entries in the file must be MAC addresses only in hexadecimal format with each octet separated by a hyphen, for example 00:1A:2B:3C:4D:5E.
- You must separate entries with a comma, or place entries on separate lines.
- The file must be in text format (that is, with a `.txt` extension).

The following is an example of a MAC ACL that you can import, assuming that the ACL is in a file with a `.txt` extension:

```
00:1A:2B:3C:4D:5E
```

```
00:1A:3B:4C:5D:6E
00:1A:4B:3C:2D:1E
00:3A:1B:5C:6D:2E
00:2A:6B:5C:4D:3E
```

You can use a MAC ACL to control which WiFi devices can access a WiFi network. You can apply a MAC ACL to more than one WiFi network.

To import an existing MAC ACL for WiFi clients and enable the ACL for a WiFi network:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. For the AP for which you want to import and enable the ACL, click the **3 dots** icon, and select **Launch Wi-Fi UI**.

   The SSID page displays.

5. Import the ACL for a group:

   a. Select **Management > Configuration > Security > ACLs > Wireless Clients**.

      The page shows all MAC ACL.

   b. Click the group name for the MAC ACL that you want to set up by importing an existing ACL.

      The MAC ACL page displays, showing the settings for the selected MAC ACL.

      Devices in the Available Stations table are automatically detected by the controller and are common to all MAC ACLs, which allows you to add a device to more than one MAC ACL. A neighboring station displays as Neighbor and a connected station displays as connected.

   c. Select the ACL Policy **Allow** radio button.

A WiFi device for which you import the MAC address into the ACL is allowed access to the WiFi network, but all other WiFi devices are denied access to the WiFi network.

d. Replace or merge the MAC addresses in the import list with the MAC addresses in the Trusted Stations table (if any are already in the table) by selecting one of the following radio buttons:

- **Replace**: MAC addresses in the Trusted Stations table are replaced with the ones in the import list.
- **Merge**: MAC addresses in the Trusted Stations table are merged with the ones in the import list.

e. Click the **Browse** button and navigate to and select the import file.

The MAC addresses on the import list are placed in the Trusted Stations table.

f. Click the **Apply** button.

Your settings are saved.

WiFi devices in the Trusted Stations table can access the WiFi network to which you apply the ACL. WiFi devices in the Untrusted Stations table cannot access the WiFi network to which you apply the ACL.

6. Apply the ACL to an SSID (WiFi network):

a. Select **Management > Configuration > Wireless > Basic > Wireless Settings**.

The page that displays lets you select an SSID.

b. Click the **>** button to the left of the SSID.

The settings for the selected SSID display.

c. Scroll down and click the **> Advanced** tab.

The page expands.

d. Select the **MAC ACL** check box.

Select the **Local MAC ACL** radio button, and from the **Select Group** menu, select the MAC ACL that you defined earlier.

Caution: If you are accessing the controller UI over a WiFi connection, make sure that your device is allowed access to the SSID. Otherwise, your device is denied access to the controller UI after you click the **Apply** button.

e. Click the **Apply** button.

Your settings are saved.

11

Troubleshooting with the Engage controller

This chapter provides troubleshooting steps that might allow you to resolve problems on your own.

The chapter includes the following sections, and we recommend that you perform the troubleshooting steps in the order that the sections are presented:

- 1. Check and update firmware as needed
- 2. Check for a network loop
- 3. Check the port status, port errors, and port statistics
- 4. Check the status of the fiber modules
- 5. Perform a cable test
- 6. Check the logs
- Optional step: Contact the NETGEAR Pro AV Design support team
- Optional step: Set your devices to factory defaults from the OOB port

Note: If you make too many custom changes to a profile and contact us for assistance, we might not be able to provide assistance. We might ask you to remove your custom changes and revert to the profile template. After all, each profile template is *certified by the manufacturer*.

1. Check and update firmware as needed

One of the main causes of network problems is inconsistent firmware versions across devices in your network. If you run into problems, an essential troubleshooting step is to check the firmware version of the devices in your network and update the firmware as needed.

Caution: Updating firmware might cause a temporary network interruption.

To check and update firmware as needed:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
4. In FW Version column of the Managed Devices table, check to see if a download cloud icon is present.

   A download cloud icon indicates that new firmware is present for the device.
5. If new firmware is present, do the following to update your device, or all devices of the same model:
   a. Click the **download cloud** icon.

      The Update Firmware pop-up window displays.
   b. Leave the **Online** radio button and **Reboot Automatically** radio button selected.
   c. Do one of the following:

- If the device model is the only one present in your network, click the **Continue** button.

  The FW Version column of the Managed Devices table displays Waiting and after a short while, the firmware update progress bar displays.

  The Update Firmware pop-up window displays again to confirm a successful firmware update, and after a short pause, the device restarts.
- If multiple devices of the same model are present in your network, click the **Group Update** button.

  The Maintenance page displays. Do the following:

  i. For the type or model of device (in the Firmware Name column), click the **3 dots** icon and select **Update Now**.

     The Update Firmware pop-up window displays.

  ii. Leave the **Online** radio button and **Reboot Automatically** radio button selected.

  iii. Click the **Continue** button.

     The Status column displays Updating. The Update Firmware pop-up window displays again to confirm a successful firmware update, and after a short pause, the devices restart.

2. Check for a network loop

Network loops create problems such as interruptions (outages), broadcast storms, and congestion and might bring down one or more devices or even your entire network. If a network loop occurs, the LEDs of all ports that are connected to devices blink rapidly.

We highly recommend that you use Spanning Tree Protocol (STP) in your network and set the core switch as the STP root bridge For more information, see Change the STP root bridge in the network on page 82 and the NETGEAR Engage Controller User Manual..

To check for a network loop and, if present, remove the loop:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. Check to see if a network loop is present:
   a. Select **Topology**.

      The Site Topology page displays. The default topology type is Tree View, unless you set another default type.

   b. At the right of the page, click the **<** (left arrow) icon.

      A menu with icons displays.

   c. Click the **topology** icon.

      The Topology Views pop-up window displays.

   d. Select the **Physical Topology** radio button.

      The topology adjusts.

   e. Enable the **Show STP** toggle.

      The toggle displays blue or green and is positioned to the right.

      A connection between two devices that displays with a dashed line indicates a link that is blocked by STP because STP detected a network loop.

   If no dashed lines display, STP did not detect any loops and did not block any links.

5. If a network loop is present, check the ports one after the other by doing the following:
   a. In the Managed Devices table, for one of the switches on which the network loop is observed, click the **Configure** button.

      The Overview page displays.

   b. Select **Port configuration**.

      The Port Configuration page displays.

   c. For each port that is connected to a device, do one of the following:

      - **You can see the switch LEDs**: From the **Admin Mode** menu, select **Disable**, and the check to see that the LEDs stop blinking rapidly.

If the LEDs start to function normally, the port connection caused the network loop.

- **You cannot see the switch LEDs**: Ping the device that is connected to the port:
  i. Select **Diagnostics > Troubleshoot**.

     The Troubleshoot page displays

  ii. In the **IP Address/Host Name** field, specify the IP address of the port on the connected device.

     Various ways exist to determine the IP address of the port on the connected device:

     - Go to **Topology > Site Topology**, and click a device to display the IP address.
     - Go to **Topology > Site Neighbors**, and in the IP address column, determine the IP address.
     - Go to **Devices**, click the **Configure** button for a device, and on the Overview page, point to a port to display the IP address.

  iii. Turn on the **Ping** toggle so that it displays green and is positioned to the right.

  iv. Click the **Run Tests** button.

     If the switch receives an abnormal ping response, the port is likely causing the network loop; If the switch receives a normal ping response, the port does not cause the network loop.

.

3. Check the port status, port errors, and port statistics

You can check the port status and check for port errors using the controller and the AV UI that is accessible from the controller.

If errors are discovered, you can remedy the situation. Often this means checking the cable connection and, if needed, reestablishing a proper connection.

To check the port status and check for port errors in the controller UI, and display port statistics for an individual switch in AV UI that is accessible from the controller:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.

4. Check the port status and check for port errors in the controller UI:

   a. Select **Network Monitoring > Network Statistics**.

      The Network Statistics page displays.

   b. If your network includes multiple devices, to narrow down the information that displays or search for a device name, device model, network profile, or VLAN ID, do the following:

      - **Device name**: Click in the **Device Name** field, select the check box for one or more device names, and then click the **Apply** button.
      - **Device model**: Click in the **Device Model** field, select the check box for one or more device models, and then click the **Apply** button.
      - **Network profile**: Click in the **Network Profile** field, select the check box for one or more profile names, and then click the **Apply** button.
      - **VLAN ID**: Click in the **VLAN ID** field, select the check box for one or more VLAN IDs, and then click the **Apply** button.

   c. To search for a port, in the **Port** field, type the port number format *unit number/slot number/port number*.

      The information in the table adjusts.

   d. Check the fields in the following table for normal port operation or port errors.

      Table 6. Normal port operation or port errors

Field	Normal condition	Error condition
Link State	Up	Down
Link Speed	Maximum speed that the device at the other end is capable off	Below maximum speed

Table 6. Normal port operation or port errors (Continued)

Field	Normal condition	Error condition
Drop Packets	None or a minimum number	Large number, but for best diagnosis, observe over a period of 10 minutes.
Physical Errors	No errors at all	If errors occur, they are physical port errors on the device or endpoint, cable errors, or transceiver module errors.

e. To observe dropped packet over a period of 10 minutes, click the **Reset All Counters** button to set the statistics to zero, wait 10 minutes, and then look again at the number of dropped packets.

5. Access the AV UI from the controller and check for port statistics for an individual device:
   a. Select **Devices**.

      The Managed Devices page displays.

   b. In the Managed Devices table, for the device for which you want to check port statistics, click the **Configure** button.

      The Overview page displays.

   c. 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 7. Inbound traffic

Field	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.
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 8. Outbound traffic

Field	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.

6. To return to the Devices page of the controller, select **Devices Management**.

4. Check the status of the fiber modules

You can check the status of the fiber modules (also referred to as transceiver modules) and check for transmit faults, loss of signals, fault status, and, if available, diagnostic information.

If errors are discovered, you can remedy the situation. Often this means checking the SFP port, fiber module, and cable connections and, if needed, cleaning the SFP port and fiber module and reestablishing proper connections.

To check the status of the fiber modules:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

- **Make no changes to the network setup for the site**: Click the **Apply** button.
- **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Network Monitoring > Fiber Modules**.

   The Fiber Modules page displays.

5. To narrow down the information that displays or search for a switch name, switch model, network profile, or VLAN ID, do the following:
   - **Device name**: Click in the **Device Name** field, select the check box for one or more switch names, and then click the **Apply** button.
   - **Device model**: Click in the **Device Model** field, select the check box for one or more switch models, and then click the **Apply** button.

   The information in the table adjusts.

6. To search for a port, in the **Port** field, type the port number format *unit number/slot number/port number*.

   The information in the table adjusts.

   The table provides a lot of information for each fiber module. The following fields are of particular interest when you are troubleshooting fiber modules.

Table 9. Fiber module troubleshooting

Field	Normal condition	Error condition
Link State	Up	Down
Link Speed	Maximum speed that the fiber module and device at the other end is capable off	Below maximum speed
Output Power (dBm)	Minimal attenuation (not below -10dBm)	Excess attenuation (below -10dBm)
Input Power (dBm)	Minimal attenuation (not below -10dBm)	Excess attenuation (below -10dBm)
TX Fault	No faults	Faults occurred
LOS	No loss of signal	Loss of signal occurred
Fault Status	No faults	Faults occurred
Diagnostics Info	No diagnostics information	Diagnostics information present

5. Perform a cable test

When you access the AV UI from the controller, you can test and display information about the cables that are connected to switch ports.

Note: This option is not supported on the M4500 series switches.

To perform a cable test:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
4. In the Managed Devices table, for the device for which you want to perform a cable test, click the **Configure** button.

   The Overview page displays.
5. Select **Diagnostics > Cable Test**.

   The Cable Test page displays.
6. Select the ports for which you want to test the attached cables.
7. Click the **Test Selected Ports** button.

   A cable test is performed on the selected ports. The cable test might take up to 30 seconds to complete. If the port forms an active link with a device, the cable status is Normal.

   The following table describes the test results that might display in the Cable Test Results section.

Field	Description
Port	The port on which the test was performed
Test Results	**Normal**: The cable is working correctly. **Open**: The cable is disconnected or has a faulty connector. **Short**: An electrical short occurred in the cable. **Cable Test Failed**: The cable status could not be determined. The cable might in fact be working. **Untested**: The cable is not yet tested. **Invalid cable type**: The cable type is unsupported. **No cable**: No cable is detected.
Fault Distance	The estimated distance in meters from the end of the cable to the failure location. The failure location is displayed only if the cable status is Open or Short.

8. To return to the Devices page of the controller, select **Devices Management**.

6. Check the logs

You can check the network logs for fully managed switches and the Pro Router, and if your network includes access points (APs), you can check the AP logs.

To check the switch, router, and AP logs:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
4. Display a switch or router log:
   a. Select **Network Monitoring > Network Logs**.

The Network Logs page displays.

You can narrow down the information that displays or search for a device name.

b. To display the log details for a device, in the Log Details column, click the **log** icon.

The Log Details pop-up window displays.

c. Check the time of the log entries when the event occurred.

5. Display an AP log:

a. Select **Network Monitoring > Access Point**.

The Access Point page displays.

You can narrow down the information that displays, search for an AP name or model, or filter by AP model.

b. To display the log details for a device, in the Log Details column, click the **log** icon.

The Log Details pop-up window displays.

c. Check the time of the log entries when the event occurred.

Optional step: Contact the NETGEAR Pro AV Design support team

The controller provides data collection tools that let you collect and package information for the ProAV Design support team. If you would like help, collect and download the data, then email it to the ProAV Design support team.

To collect and download data and send it to the ProAV Design support team:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

The controller application opens and displays a login page.

2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

The Managed Devices page displays.

3. If you set up more than one site, from the **Site** menu, select the site.

The Edit Network Setup pop-up window displays.

Do one of the following:

- **Make no changes to the network setup for the site**: Click the **Apply** button.
- **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

The Managed Devices page adjusts.

4. Select **Support**.

   The Support page displays.

5. In the table with devices at the site, select the check box for each device that you want to be included in the file, or select the check box in the table header so that all device are selected.

   By default, the check box in the table header is selected.

6. Above the table, select one or all of the following check boxes:
   - **Controller Log File**: Selected by default.
   - **Site Configuration File**: Selected by default.
   - **Switch Log File**: Selected by default. If this option is cleared, select the check box, and select one or more switches.
   - **AP Log File**: Not selected by default. If you select the check box, also select one or more access points.
7. By default, the **CPU Packet Capture** check box is enabled. Select the check box to disable CPU packet capture.
8. Click the **Download File** button.

   The Download File pop-up window displays.

   If you enabled the **CPU Packet Capture** check box, you can adjust the time of the capture duration between 5 and 30 seconds. By default, the capture duration is set to 5 seconds.

9. Click the **Confirm** button.

   The file or files are generated as a zip archive file. The controller automatically generates topology screenshots and includes them in the ZIP file.

10. Save the zip archive file to your computer.
11. Address an email to ProAVDesign@netgear.com, attach the zip archive file, describe the symptoms in the email, and send the email.

    A member of the NETGEAR ProAV support team will contact you.

Optional step: Set your devices to factory defaults from the OOB port

If your network consists of less than five or six switches and access points and you run into difficulties, it could be easier to reset all switches and access points to factory defaults rather than to perform extended troubleshooting, which could be time-consuming. Reconfiguring network profiles could go fast in most cases.

We recommend that you use the OOB port to reset your devices to factory defaults so that you do not lose connectivity or are locked out from the controller during the reset process. In this example procedure, we are using an IP address of 10.51.100.25 and a subnet mask of 255.255.255.0 for the OOB port. The IP address of the default gateway 10.51.100.1.

⚠ **Caution:** Resetting your devices to factory default causes a major network interruption.

To configure the OOB port and then reset all your devices to factory defaults:

1. On your computer, in the folder in which you installed the controller application, double-click the **Engage** application icon, or double-click the **Engage** shortcut.

   The controller application opens and displays a login page.
2. In the **Login Name** field, enter **admin** as the user name, in the **Password** field, enter the controller password that you set up the first time that you logged in, and click the **Login** button.

   The Managed Devices page displays.
3. If you set up more than one site, from the **Site** menu, select the site.

   The Edit Network Setup pop-up window displays.

   Do one of the following:

   - **Make no changes to the network setup for the site**: Click the **Apply** button.
   - **Change the network setup for the site**: See the information in Change the network setup of a site on page 51. When you are done, click the **Apply** button.

   The Managed Devices page adjusts.
4. Configure a static IP address for the OOB port:
   a. Select **Site Settings > Management VLAN and OOB**.

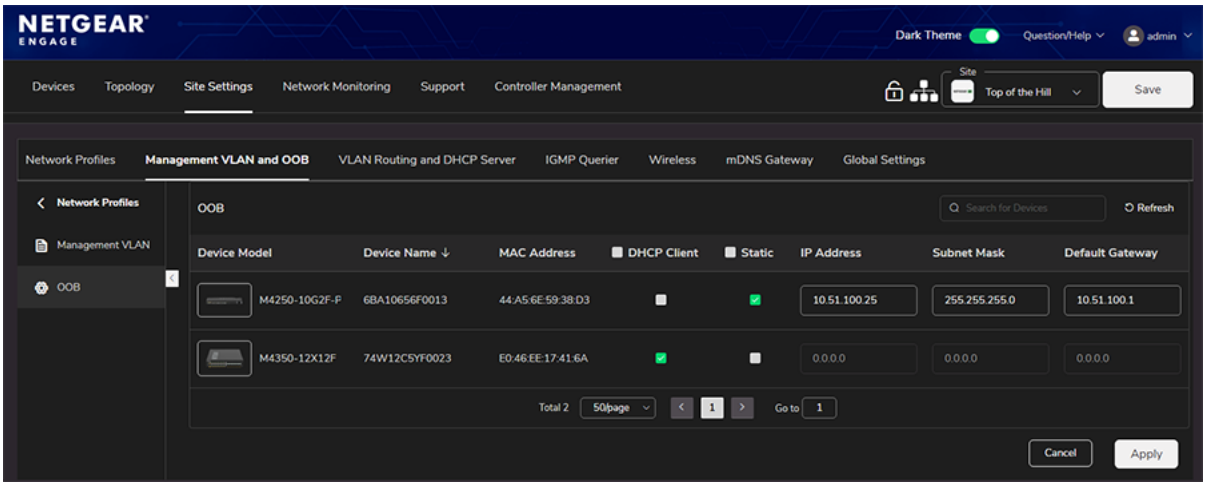
      The Management VLAN page displays.
   b. From the menu in the left panel, select **OOB**.

      The OOB page displays.

c. For the switch for which you want to configure the OOB port, select the **Static** check box.

   By default, the OOB port receives IP address settings from the DHCP server.

d. In the **IP Address** field, enter **10.51.100.25**, in the Subnet Mask field, enter **255.255.255.0,** and in the **Default Gateway** field, enter **10.51.100.1**.



e. Click the **Apply** button.

   A pop-up window displays.

   Caution: When you click the Yes button, the OOB port is disconnected and you must reconnect using the new IP address settings.

f. Click the **Yes** button.

   Your changes are saved.

5. Log in to the OOB port with its new IP address.

   You might need to change the TCP/IP settings on the your computer on which the controller is installed.

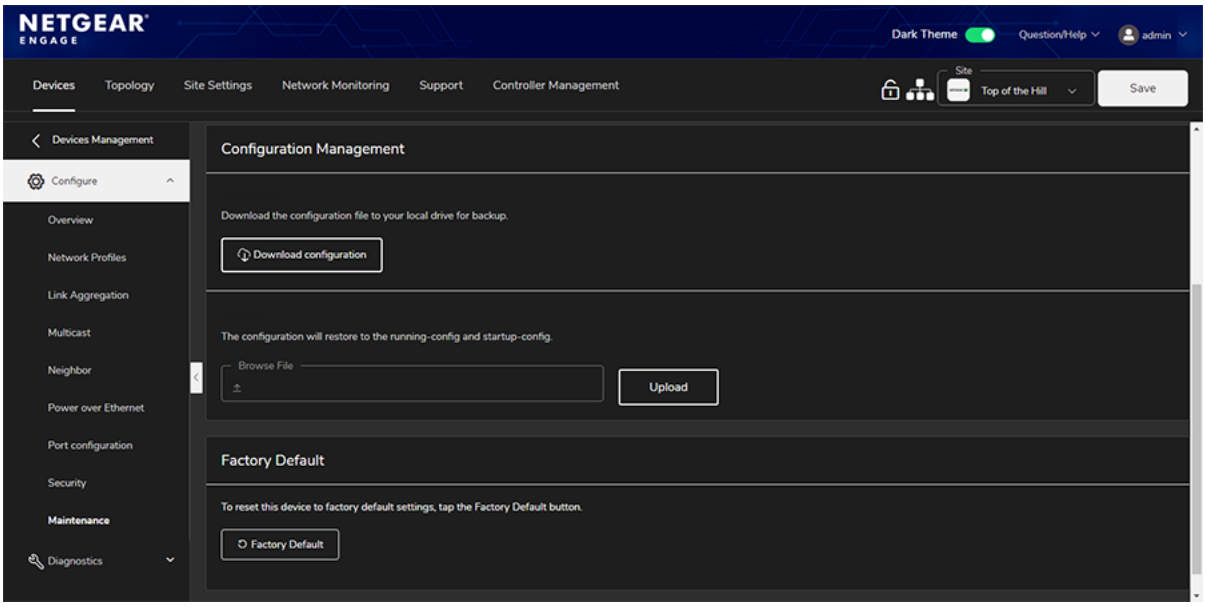
6. Reset a device to factory defaults:

   a. In the Managed Devices table, for the device that you want to set to factory defaults, click the **Configure** button.

      The Overview page displays.

   b. Select **Maintenance**.

The Maintenance page displays.



c. 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.

d. 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 and the switch receives an IP address from the DHCP server in the network, the controller can rediscover the switch. If the switch requires a static IP address, you first must set the IP address of the switch before the controller can rediscover the switch.

7. To return to the Devices page of the controller, select **Devices Management**.
8. Repeat Step 6 for the next device that you want to reset to factory defaults.

After a few minutes, the devices that you reset to factory defaults display in the Discovered Devices table, and you start the onboarding process for these devices. It might take up to 10 minutes for an access point to display in the Discovered Devices table.

For more information about onboarding and configuring, see the NETGEAR Engage Controller User Manual.