How do I set up one or more VLANs between a NETGEAR ProSAFE firewall and a smart switch?

Was this article helpful? Yes No

To separate guest and production networks, administrators need to segment a network and create two Layer 3 networks to achieve complete separation between them, while both networks have full access to the Internet.

As the administrator, when you create VLANs, be sure to use numbers and names that clearly identify each VLAN and its purpose. The scenario described throughout this example uses these VLAN names and network IPs:

- Existing default VLAN 1: 192.168.1.1/255.255.255.0
- Example VLAN5 as Guest: 192.168.5.1/255.255.255.0

To set up multiple VLANs, follow these high-level steps:

1. Gather the required equipment.
2. Set up the ProSAFE firewall.
3. Set up the Smart Managed Switch.
4. Assign the ports and set the port VLAN IDs.
5. Test that the VLANS are online and segregated.

These high-level steps are explained in detail in the following sections.

Required Equipment

Gather the required equipment before you attempt to configure your VLANs. Ensure that the equipment is in factory default mode to prevent configuration conflicts. For more information, visit the related link at the end of this article.

- Router that supports VLANs
- Layer 2 switch that supports VLANs
- Modem with an Internet connection
- Four Ethernet patch cables
- Two computers

To set up the ProSAFE firewall:

This example uses NETGEAR router SRX5308, but you can use any router that supports VLANs. The web interface might differ slightly for different models. If you are not using a NETGEAR product, check the documentation for that device for instructions.

1. Log in to your NETGEAR ProSAFE firewall as admin.
   The LAN Setup screen displays the VLAN ID 1 subnet IP as: 192.168.1.1/255.255.255.0, the ProSAFE Firewall's default IP.
2. Create a new VLAN.
   In the LAN Setup section, click the **Add** button and enter your settings.
   Note: This scenario creates one VLAN but you can create more.

   Example settings to create VLAN 5:

   - **Profile Name**. Guest
   - **VLAN ID**. 5
   - **Port 1**. Select the check box.
   - **IP Address.** 168.5.1
   - **Subnet Mask.** 255.255.0
   - **Start IP.** 168.5.20
   - **End IP.** 168.5.100
   - **Enable Inter VLAN Routing**. Clear the check box to disable inter VLAN routing.
     Important: If inter VLAN routing is enabled, the VLAN is accessible from other existing VLANs. When you create additional VLANS, enable and disable inter VLAN routing according to the purpose of each VLAN.

3. Click **Apply** to save.

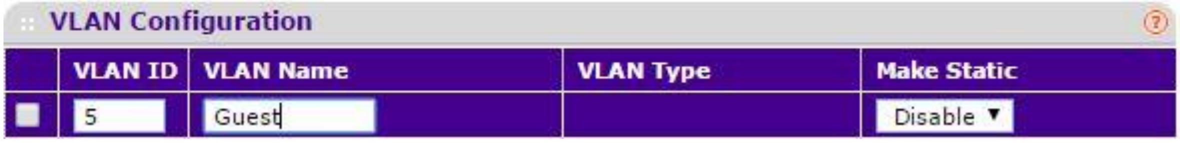
To set up the smart managed switch:

This example uses NETGEAR model M4100-D12G, but you can use any NETGEAR switch that supports VLAN configuration. The NETGEAR web interface might differ slightly for different models. If you are not using a NETGEAR switch, check the documentation for that device for instructions.

1. Connect the switch to the router and plug the computer into a spare port, such as port 6.
2. Log in to your switch's configuration utility.
3. Click **Discover** to discover the Switch Management IP. In this example, it is 192.168.1.110.
4. Enter the IP address in to your web browser.
   The login page displays.
5. Log in to the switch.
6. Select **Switching** > **VLAN** > **Basic** > **VLAN Configuration.**
   The VLAN Membership window displays.
7. In the VLAN Configuration section, enter the VLAN 5 settings and click **Add** to save.

   - **VLAN ID.** VLAN 5.

- **VLAN Name**. Guest.
- **Make Static**. Disable**.**



VLAN Configuration

	VLAN ID	VLAN Name	VLAN Type	Make Static
□	5	Guest		Disable ▼

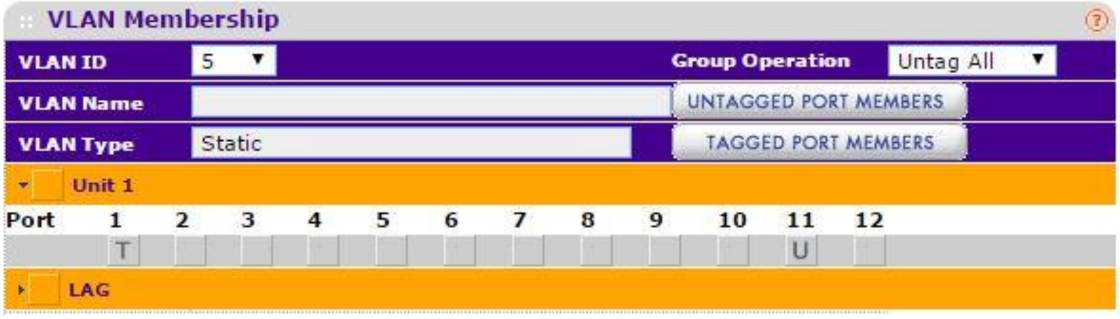
To assign the ports and set the port VLAN IDs:

This example assigns port 11 to the guest VLAN. Ports 1-10 and port 12 remain on the existing default VLAN 1.

1. Connect router port 1 to switch port 1 with an Ethernet cable.
   Port 1 on the switch is labeled as **the** trunk port (T) because it carries traffic for more than one VLAN.

2. From the switch web interface, select **Switching** > **VLANS** > **Advanced** > **VLAN Membership**.
   The VLAN Membership window displays.

3. In the VLAN Membership section, assign port 11 as an untagged (U) member of VLAN 5 by clicking the grey box under port 11, as shown in this image:

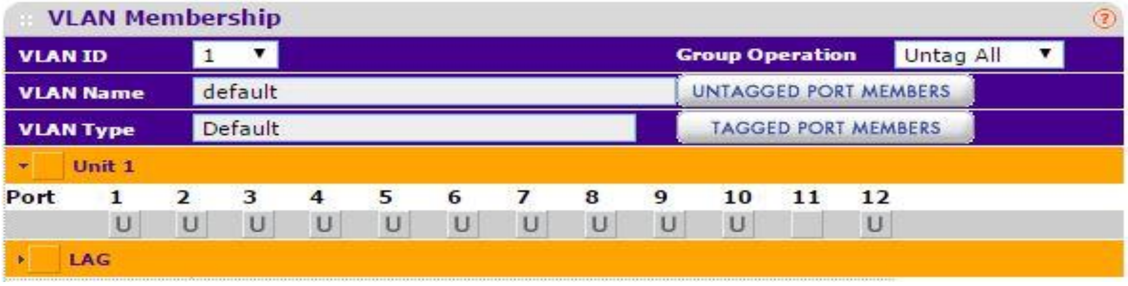


VLAN Membership

VLAN ID: 5 ▼ Group Operation: Untag All ▼
VLAN Name:
VLAN Type: Static

Port	1	2	3	4	5	6	7	8	9	10	11	12
	T										U	

4. In the VLAN Membership section, confirm that default VLAN 1 now displays that ports 1-10 and port 12 are untagged (U), as shown in this image:



VLAN Membership

VLAN ID: 1 ▼ Group Operation: Untag All ▼
VLAN Name: default
VLAN Type: Default

Port	1	2	3	4	5	6	7	8	9	10	11	12
	U	U	U	U	U	U	U	U	U	U		U

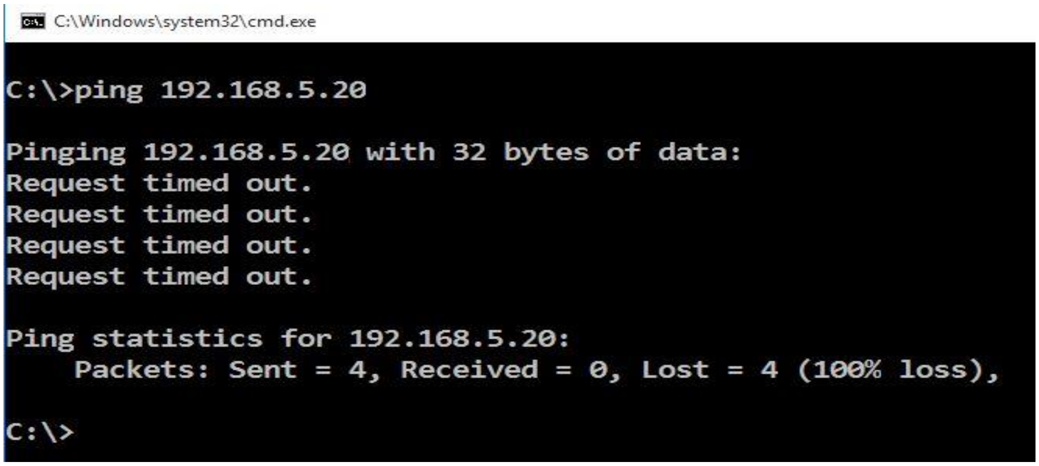
To test that the both VLANS are on line and segregated:

1. Connect the Ethernet patch cables as described here:

   - **Cable 1**. From switch port 6 to the PC that will manage the switch in VLAN 1.
   - **Cable 2**. From switch port 11 to the PC in Guest VLAN 5.
   - **Cable 3**. From the firewall (router) WAN port to your modem.

2. Confirm that the computers are connected to the Internet by navigating to any website or pinging the two remote computers. If they are not connected, double-check that each step was followed correctly and that the cables are in the correct ports.

3. Confirm that the VLANS are segregated by using a command prompt or terminal to send a ping packet from the computer connected to ports in default VLAN 1 to the PC connected to port 11 in the guest VLAN. From the computer on default VLAN 1 connected to port 6, ping the IP address of the PC in Guest VLAN 5 that received the 192.168.5.20 IP address from the ProSAFE firewall as shown in this image:



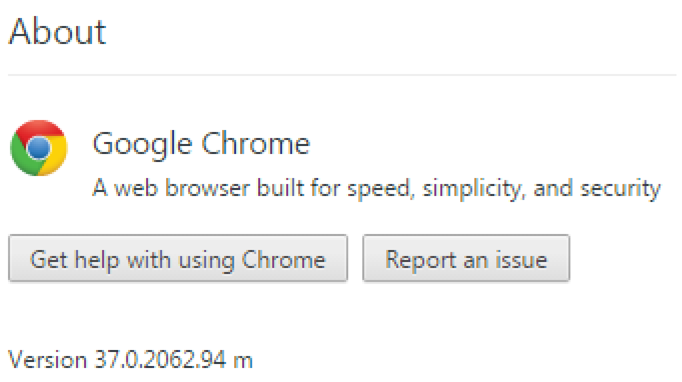
```
C:\>ping 192.168.5.20

Pinging 192.168.5.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Your connection is not private in Google Chrome browser

Was this article helpful? Yes No

You may see the following error when trying to access the web interface of your NETGEAR device when using Google Chrome. This follows a recent update to Chrome, version 37.

The exact Chrome version number is shown.



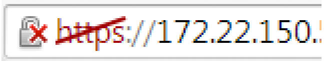
About

Google Chrome

A web browser built for speed, simplicity, and security

Version 37.0.2062.94 m

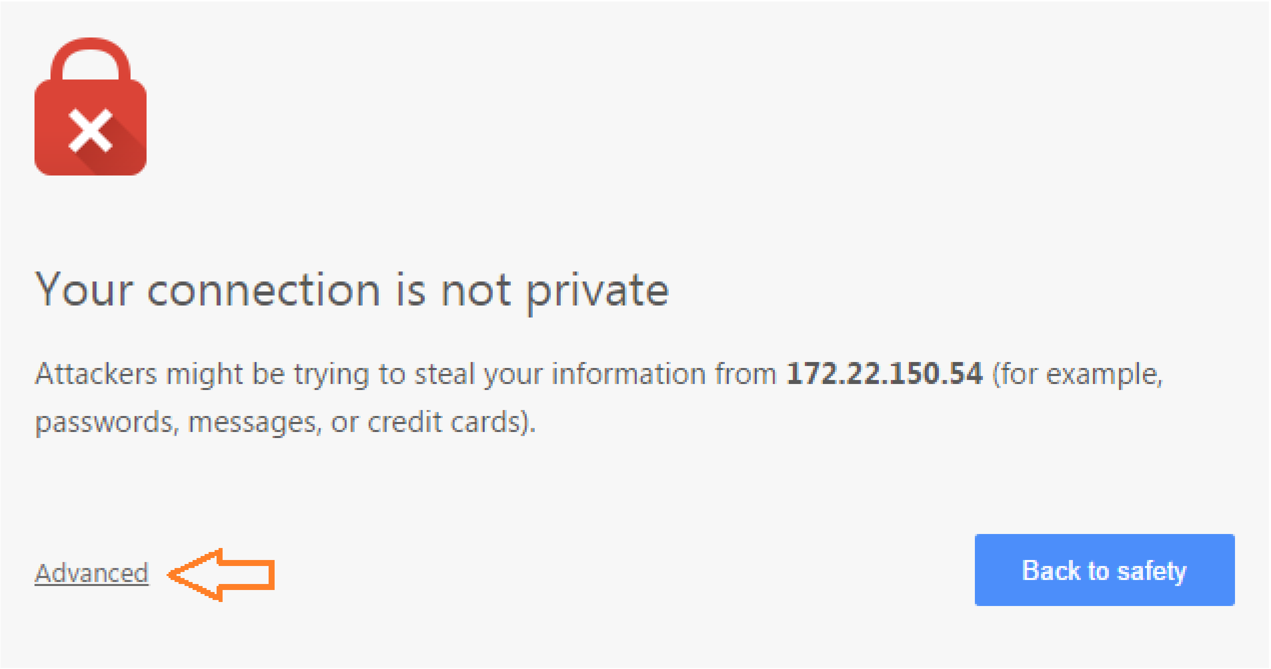
This applies to NETGEAR products using HTTPS to access Web interface. A red X is shown in Chrome.



~~https~~://172.22.150.

This is a Certificate error. This refers to how public websites trust each other. This is not important as your device is usually on a local network, behind a firewall,

This screen appears.

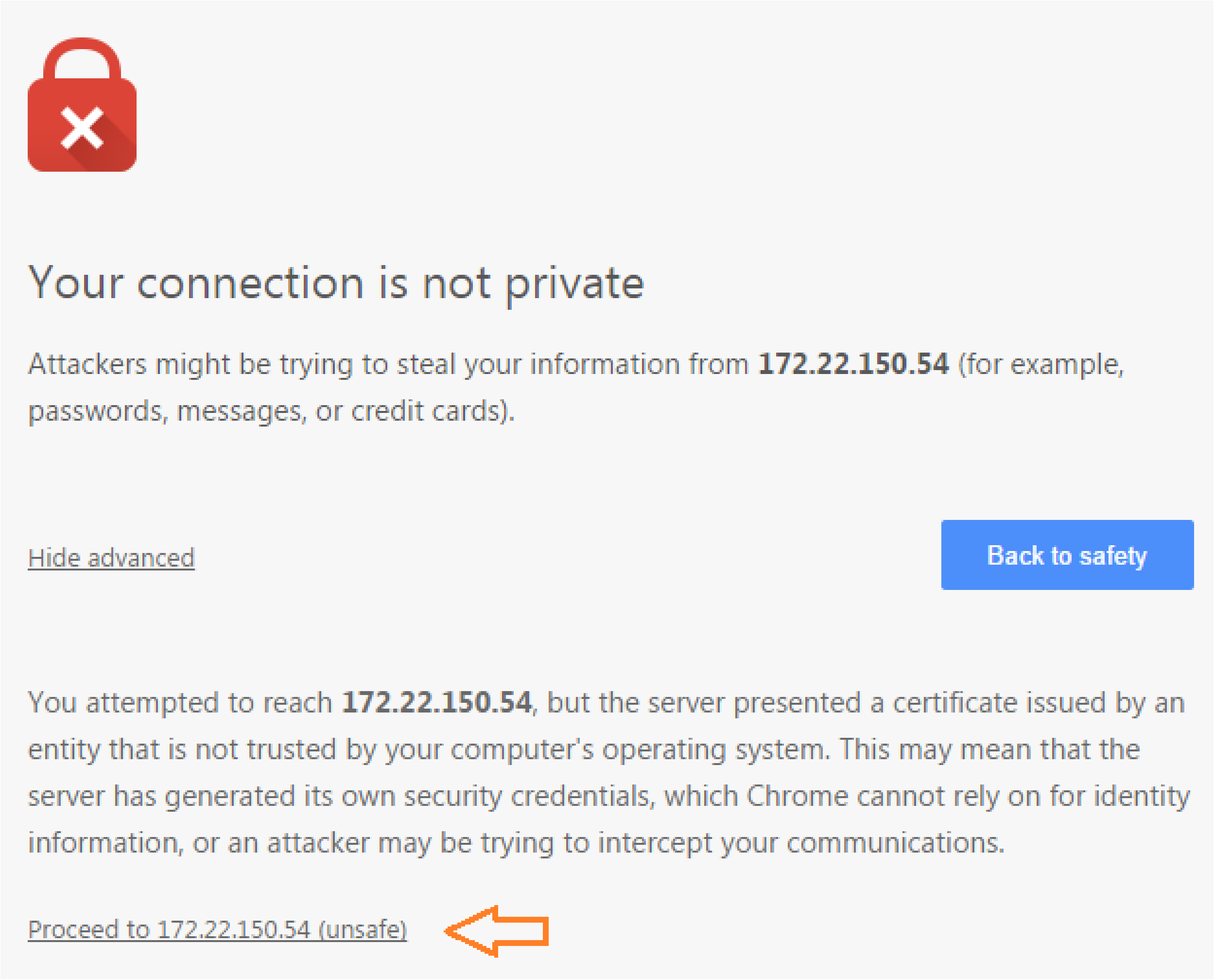


Your connection is not private

Attackers might be trying to steal your information from **172.22.150.54** (for example, passwords, messages, or credit cards).

This message does not affect accessing data on your NAS in your local network.

Click on **Advanced**, as shown by orange arrow.



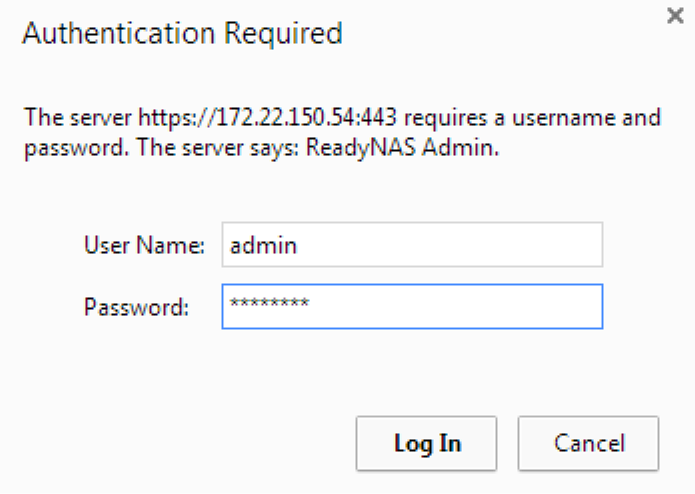
Your connection is not private

Attackers might be trying to steal your information from **172.22.150.54** (for example, passwords, messages, or credit cards).

You attempted to reach **172.22.150.54**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

Click on **Proceed**.

You will be prompted for Login Username and Password as normal.



Authentication Required

The server https://172.22.150.54:443 requires a username and password. The server says: ReadyNAS Admin.

User Name: admin

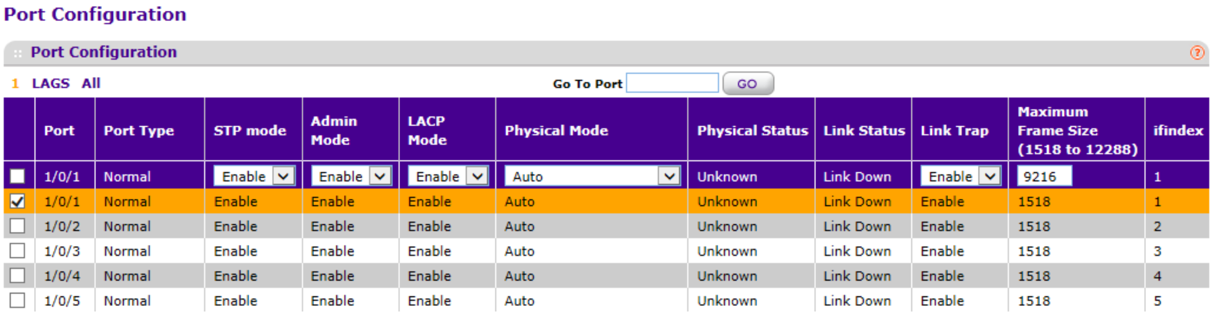
Password: ********

Configuration Using the GUI

To configure jumbo frames using the GUI:

1. Go to **Switching > Ports > Port Configuration**.
2. Select the port on which you want to enable jumbo frames.
3. In the **Maximum Frame Size** field, change the value to the required value and then click the **Apply** button.

For example, if clients are set to an MTU size of 9000, then as a good practice, set the MTU size on the switch to a slightly higher value, such as 9216, to allow for the additional header size from clients.



Port Configuration

Port Configuration

	Port	Port Type	STP mode	Admin Mode	LACP Mode	Physical Mode	Physical Status	Link Status	Link Trap	Maximum Frame Size (1518 to 12288)	ifindex
□	1/0/1	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	9216	1
☑	1/0/1	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518	1
□	1/0/2	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518	2
□	1/0/3	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518	3
□	1/0/4	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518	4
□	1/0/5	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518	5

The maximum frame size of the chosen port (1/0/1) is now changed to 9216.

Configuration Using the CLI (when supported)

To configure jumbo frames using the CLI:

1. From global mode, enter privilege/enable mode and then enter configure mode.

```
(M5300-28G) >enable
Password:********

(M5300-28G) #configure

(M5300-28G) (Config)#
```

2. Enter in to the configuration of the port on which you want to enable jumbo frames.

```
(M5300-28G) (Config)#interface 1/0/1
```

3. Configure the maximum frame size using the `mtu` command followed by the value that you want to set.

```
(M5300-28G) (Interface 1/0/1)#mtu 9216
```

How do I access the admin page of my ProSAFE Smart Managed Switch?

Was this article helpful? Yes No

To access the admin page of a Smart Switch, you first need to find the IP address of the switch. The simplest way to find the IP address of the switch is to discover it using the Smart Control Center

If you cannot use the Smart Control Center, then use one of the following methods to determine the IP address of the switch:

- If the switch is connected to a network with a DHCP server, check the list of assigned IP addresses on the DHCP server. If your internet router is also your DHCP server, you may find the list of assigned IP addresses on the admin page of your internet router (check for an "attached devices" page or similar). You need to look for the IP address that is assigned to the MAC address of the switch. You can find the MAC address of the switch on the label underneath the switch.
- If the switch is not connected to a network, connected to a network with no DHCP server, or, connected directly to your PC, then the switch will use its default IP address, 192.168.0.239. **Note**, in this case, you will need to record your computer's TCP/IP configuration settings, and then configure the computer with a static IP address of 192.168.0.210 and with 255.255.255.0 as the subnet mask. If you are unsure how to do this, see the How to set a static IP address

When you have determined the IP address of the switch, the next step is to access the admin page:

- Open a web browser.
- Type the IP address of the switch into the address bar of the web browser and press **Enter**.
- Type the admin password of the switch (the default password is *password*) and click **Login**.

Note: Ensure that your PC is connected to a port in the management VLAN.

Troubleshooting.

I still cannot find the IP address of my switch.
You can try to reset the switch to factory default settings by holding the Factory Reset button on the switch for 10 seconds. Note that this will reset the configuration of the switch to default settings. Once done, re-try the steps above.

I have found the IP address of my switch, but when I try to access it using a web browser, I do not get prompted for a password.
Check if you can ping the IP address of the switch. If you cannot ping the switch, your computer may be configured in a different IP network to the switch. Try setting your computer with a static IP in the same IP network as the switch.

I have found the IP address of my switch, but when I try to access it using a web browser, it does not accept my password.
Try the default password which is *password*. If this fails, you can reset the switch to factory default settings to restore the password to the default. Again, please note that this will erase all configured settings on the switch.

Creating a Support Case through MyNETGEAR

Was this article helpful? Yes No | 3 people found this helpful in last 30 days

To create a support case:

1. Navigate to MyNETGEAR and login with your account credentials.
2. Click **My Support** at the left sidebar.
3. Click **CONTACT SUPPORT**.

How do I troubleshoot problems with my NETGEAR PoE switch?

Was this article helpful? Yes No

This article assists in troubleshooting common Power over Ethernet (PoE) problems with NETGEAR PoE switches.

Power over Ethernet (PoE) is a networking feature defined by the IEEE 802.3af and IEEE 802.3at standards. PoE lets Ethernet cables supply power to network devices over the existing data connection.

PoE-capable devices can be power-sourcing equipment (PSE), powered devices (PDs), or sometimes both. The device that transmits power is a PSE, while the device that is powered is a PD. Here, the PSE is a PoE switch. The PDs may be devices such as VoIP phones, wireless access points, and IP cameras.

For further information on PoE, refer to https://kb.netgear.com/209/What-is-PoE-Power-over-Ethernet

Follow the guidelines in this article to help resolve problems such as:

- PD is not powering on.
- PD is powering off intermittently.
- Certain PDs are powering on while other PDs on the same PoE switch remain powered off.

PoE Standards

As mentioned above, PoE is defined by IEEE 802.3af (known as PoE) and 802.3at (known as PoE+) standards. If your PoE switch supports IEEE 802.3at, it can supply power to both 802.3at and 802.3af PDs. However, if your switch supports 802.3af only, it can only supply power to 802.3af (PoE) PDs.

PoE Budget

Your PoE switch has a PoE budget, that is, the total amount of power measured in watts that it can supply to PDs at one time. Refer to the datasheet of your switch to verify its PoE budget. You should ensure that the amount of power being drawn by your connected PDs does not exceed the PoE budget of your switch. When calculating the amount of power being drawn by your PDs, you need to check the PoE class to which the PD belongs. The PoE class of a PD determines the amount of power it will require, as seen in the below table:

Device Class	Standard	Range of Power Delivered to the Powered Device	Minimum Output at PoE Switch Port (Minimum Allocated)	Maximum Output at PoE Switch Port (Maximum Allocated)
0	PoE/PoE+	0.44W-12.95W	15.4W	16.2W
1	PoE/PoE+	0.44W-3.84W	4.0W	4.2W

Device Class	Standard	Range of Power Delivered to the Powered Device	Minimum Output at PoE Switch Port (Minimum Allocated)	Maximum Output at PoE Switch Port (Maximum Allocated)
2	PoE/PoE+	3.84W-6.49W	7.0W	7.4W
3	PoE/PoE+	6.49W-12.95W	15.4W	16.2W
4	PoE+	12.95W-25.5W	30.0W	31.6W

If for example, you have 10 PDs that are class 2, the total budget required is 70W.

Alternative Power Source

Where possible, check if the PD works with another PoE switch, or, where applicable check if the PD powers on using an external power supply. If the PD does not power on from any of these power sources, then the problem is likely with the PD.

Cabling

Check that the Ethernet cabling you are using is of good quality. It should be CAT5e or better. To be certain, try testing with different cabling to that currently in use.

Port Configuration

In the admin page of the switch, ensure that the port connected to the PD is not administratively disabled. Also, check that the PoE configuration of the port is valid (i.e. that PoE is enabled for the port, and, set to the right standard and power limit, where applicable). For further information, refer to the user manual for your switch.
Note: This does not apply to unmanaged switches and certain Web Managed Plus switches.

Firmware Update

It is possible that specific PoE-related problems may have been addressed in a firmware release. Refer to the product support page for your switch to download the latest firmware and update it. For further information, refer to the user manual for your switch and firmware release notes.
Note: This does not apply to unmanaged switches.

Reset Configuration

It is possible that a mis-configuration of the switch may cause problems. Reset the switch to factory default settings. This will erase the current configuration so you should, where necessary, make a configuration backup before completing this step.
Note: This does not apply to unmanaged switches.

Further Considerations

- If your PoE switch model is GS105PE, then refer to https://kb.netgear.com/25541/GS105PE-PoE-troubleshooting for guidance specific to this device.
- If you see symptoms where you cannot power more than one PD in a set of adjacent ports, such as scenarios outlined below, please contact NETGEAR Support. When contacting Support, it may be beneficial to reference the troubleshooting you have already carried out as described in this article.
  - On a switch with greater than 16 ports, a PD on Port 1 powers on but a PD on ports 2, 3 & 4 does not power on. Similarly, a PD on port 5 powers on but a PD on ports 6, 7 & 8 does not power on.
  - On a switch with 16 ports or less, a PD on Port 1 powers on but a PD on Port 2 does not power on. Similarly, a PD on Port 3 powers on but a PD on Port 4 does not power on.

How do I reset a smart switch to factory default settings?

Was this article helpful? Yes No | 4 people found this helpful in last 30 days

To restore a smart switch to its factory default settings, use either the **Factory Default** button or the web management interface. If you lost the password to access the smart switch, you must use the **Factory Default** button.

Important: Restoring the default settings erases all saved configurations including the password, VLAN settings, and port configurations.

To reset a smart switch using the Factory Default button:

1. Locate the recessed button that is marked **Factory Default** or **Factory Defaults** on the back or bottom panel of your device.
   Be careful not to mix it up with the **Reset** button. The Reset button restarts the switch, it does not restore it to factory default settings.
2. Insert a straightened paper clip or a similar device into the hole of the **Factory Default** button and hold for two to three seconds.

   If you press the **Factory Default** button too long, some switches change to recovery mode, signified by the LED light turning from green to amber. If this happens, power cycle the switch or press the **Reset** button to reboot the device.

   The smart switch restarts in a factory default configuration.

To reset a smart switch using the web management interface:

1. In your web browser address field, enter your smart switch IP address.
   For more information, visit What is my NETGEAR Web Managed Plus or Smart Switch Default IP Address?
   You are prompted to enter your password.
2. Enter your case-sensitive password and click **Login**.
   If you did not change the default password, the default password is password.
   The System Information screen displays.
3. Select **Maintenance** > **Reset** > **Factory Default**.
4. Select the **Check this box and click apply below to return all configuration settings to default values** check box and click **Apply**.

   The smart switch restarts in a factory default configuration.

For more information, visit:
How do I use the Smart Control Center to configure the basic settings of a smart switch?
What are the default web interface passwords for NETGEAR devices?
Password recovery for smart switches

What is a network loop?

Was this article helpful? Yes No | 9 people found this helpful in last 30 days

A network loop occurs when a network has more than one active path carrying information from the same source to the same destination. The information loops and amplifies itself using the additional path instead of stopping when it reaches its destination. Network loops might cause a slow, irregular Internet connection or network failure.

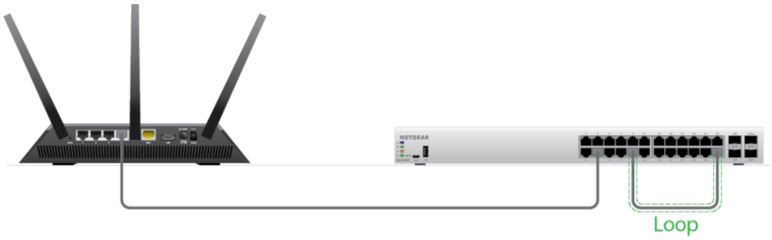
When a network loop overwhelms broadcast traffic and degrades network performance, it is called a “broadcast storm”. Some NETGEAR switches use Spanning Tree Protocol (STP) to identify and remove network loops and prevent broadcast storms.

Some common network loop examples are illustrated below, including resolutions.

Click one of the configurations below to skip to that example:

- Network switch connected to itself with an Ethernet cable
- Router connected to itself with an Ethernet cable
- Wireless device connected to a router using both WiFi and Ethernet
- Wireless device connected to a range extender using both WiFi and Ethernet
- Orbi Satellite connected to itself with an Ethernet cable

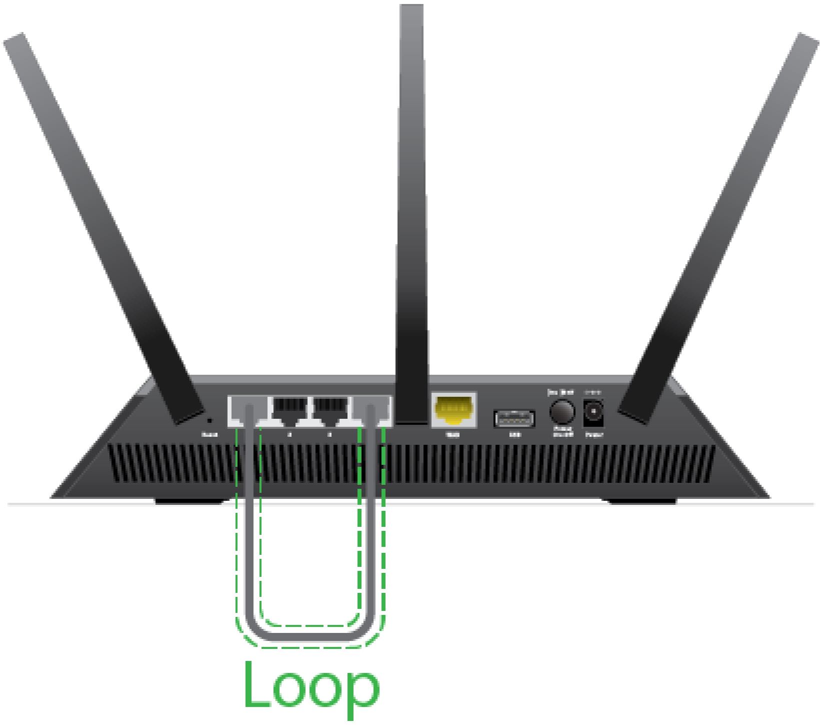
Network switch connected to itself with an Ethernet cable



Problem: Both ends of an Ethernet cable are plugged into the same network switch.

Solution: Unplug the Ethernet cable.

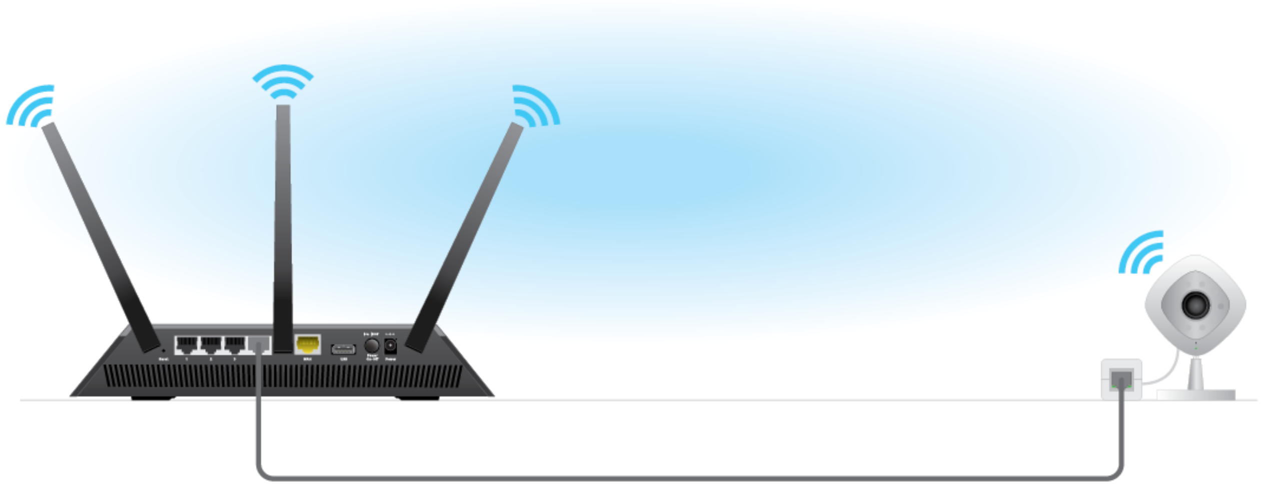
Router connected to itself with an Ethernet cable



Problem: Both ends of an Ethernet cable are plugged into the same router.

Solution: Unplug the Ethernet cable.

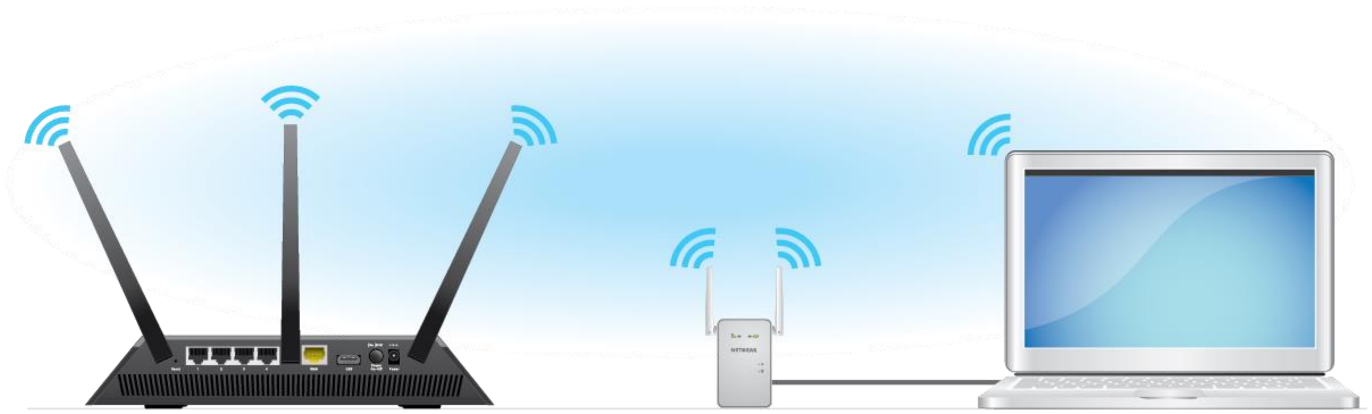
Wireless device connected to a router using both WiFi and Ethernet



Problem: A wireless device is connected to a router using both WiFi and Ethernet. The wireless device could be an IP camera, a computer, a printer, a smart home hub, or any other device that supports both wired and wireless connections.

Solution: Disconnect the Ethernet cable from your device or turn off your device’s WiFi.

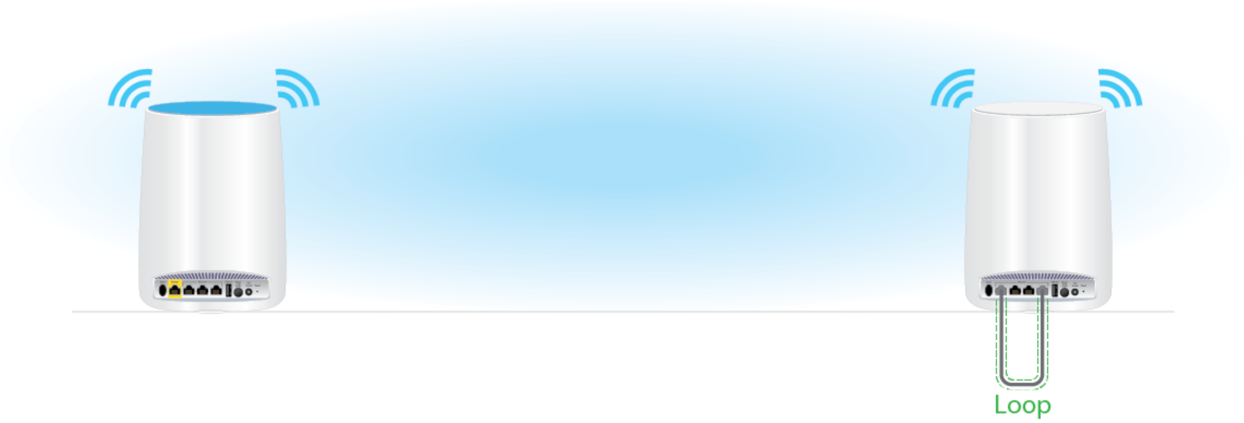
Wireless device connected to a range extender using both WiFi and Ethernet



Problem: A wireless device is connected to a wireless extender using an Ethernet cable, but the device’s WiFi is not turned off. The wireless device could be an IP camera, a computer, a printer, a smart home hub, or any other device that supports both wired and wireless connections.

Solution: Disconnect the Ethernet cable from your device or turn off your device’s WiFi.

Orbi Satellite connected to itself with an Ethernet cable



Problem: Both ends of an Ethernet cable are plugged into the same Orbi Satellite.

Solution: Unplug the Ethernet cable.

How do I create a NETGEAR Support Case?

Was this article helpful? Yes No

If NETGEAR Support does not have an article that addresses your problem, or if you need to request a replacement product, follow these steps to submit a NETGEAR support case.

To create a NETGEAR support case:

1. Visit https://www.netgear.com/mynetgear/registration/login.aspx.
2. Enter the email and password associated with your MyNETGEAR account.
   Note: If you do not have a MyNETGEAR account, see How do I create a MyNETGEAR account?.
3. Click **LOG IN**.
4. In the left sidebar, select **My Support**.
5. Click **CONTACT SUPPORT**.
6. Click on the link for your support type to jump to that section:

- Get answers about NETGEAR products before I buy
- Get help on my NETGEAR product
- Replace my defective product

Get answers about NETGEAR products before I buy

1. Select the product category that you would like to learn more about.

2. Select a NETGEAR support option.

Get help on my NETGEAR product

1. Select your registered product from the drop-down menu.
   Note: If you need to register your product, click the link below the drop-down menu or see How do I register a product on MyNETGEAR?.
2. Click **Next**.
   NETGEAR Support articles appear.
3. If the suggested articles do not address your problem, click **I cannot find an answer to my problem, I would like to contact NETGEAR support**.
4. Select a NETGEAR support option.

Replace my defective product

1. Select your registered product from the drop-down menu.
   Note: If you have not registered your product, click the link below the drop-down menu to register your product or see How do I register a product on MyNETGEAR?.
2. Click **Next**.
3. Select **Call us**.
4. Write a brief, detailed description of the problem.
5. Click **Next**.
6. Record your case number.
7. Call NETGEAR Support within 24 hours.

NETGEAR Support Remote Access Client

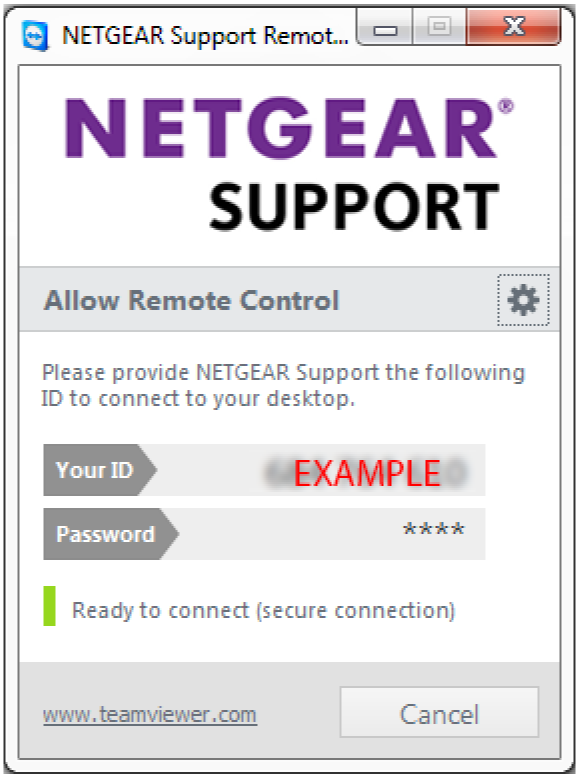
Was this article helpful? Yes No | 2 people found this helpful in last 30 days

When requested by NETGEAR Support, please download the remote access client using the download link below. Provide the 9 digit number listed in the **Your ID** field to the NETGEAR Support expert.
Windows, MacOS, and Linux versions are available.

Note: You must agree to the terms of the NETGEAR Remote Access Policy

Download client from

https://get.teamviewer.com/netgearsupport



Please provide NETGEAR Support the following ID to connect to your desktop.

Your ID EXAMPLE

Password ****

Ready to connect (secure connection)