NETGEAR®
BUSINESS

Virtual Local Area Networks (VLANs)

Easy Guide

NETGEAR®
BUSINESS

Table of Contents

Basic LAN Terms

A Local Area Network (LAN) is a group of devices physically connected by wireless or wired media to communicate, share data, and network resource. This can also be called a broadcast domain, meaning that all devices on that LAN can communicate with one another with no rules or filters.

Internet Protocol addresses (IP address) are numerical labels assigned to each device connected to a computer network that uses the Internet Protocol for communication. For example, a computer may be assigned IP addresses of 192.168.1.2 and a printer is assigned an IP address 192.168.1.3 on the same LAN network to communicate to each other.

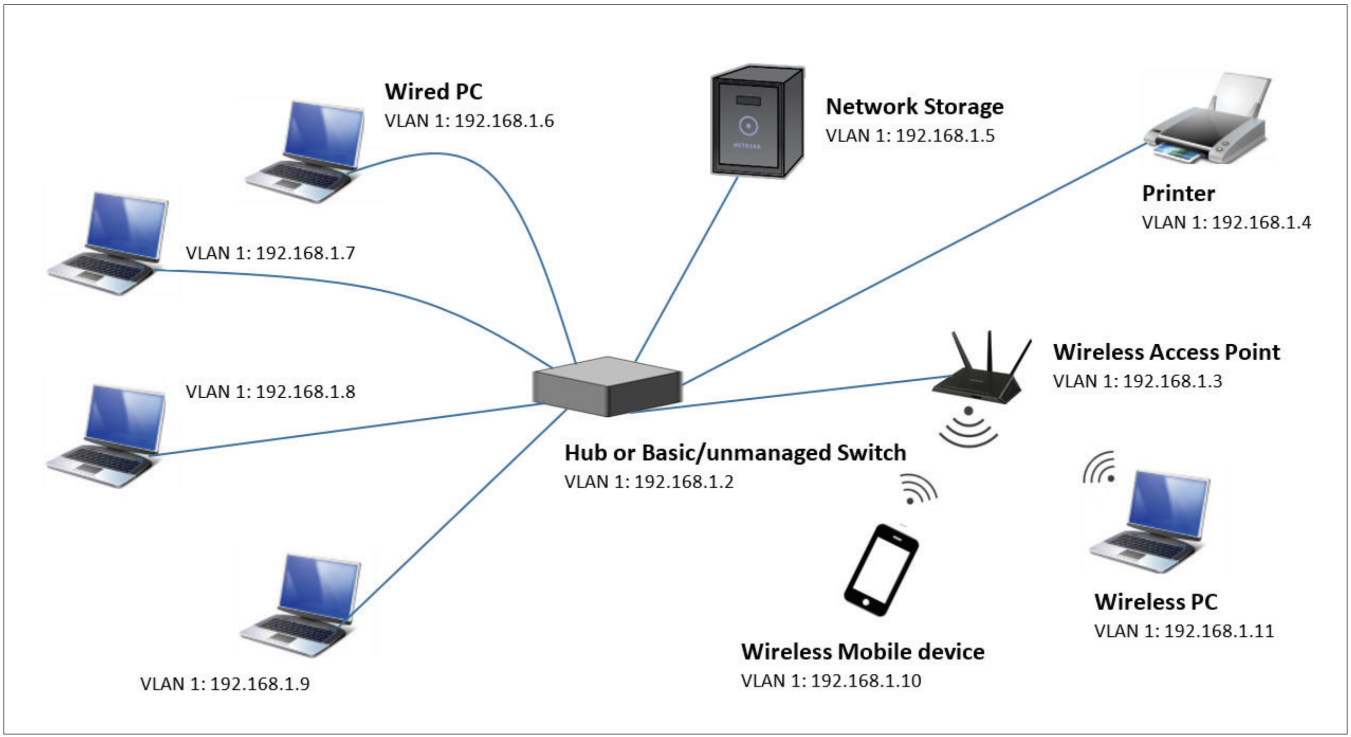
The first part that appears similar e.g. "192.168.1" is the network portion, and means both the computer and the printer is on the same LAN. The last part that appears unique is the host portion e.g "2" and "3" represent the computer and printer as two unique devices. With every assigned IP address, a subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs. One IP address may not be assigned to two separate devices/hosts on the same LAN or Subnetwork, otherwise an IP addressing conflict occurs and interferes with the network connectivity.

Subnetwork & Subnet Mask: A LAN can be broken into smaller subdivisions termed subnets. A Subnet Mask, enables each device on a LAN to know which host and network the device is a member of. With the example above, the printer and the computer have its subnet mask of 255.255.255.0 (aka /24). It means that the computer and printer is a part of the 192.168.1.0 network and has a network gateway is 192.168.1.1. The /24 subnet mask can also provide the administrator with maximum number of host and addresses it can use on this particular network (maximum of 256 addresses and can host up to 254 devices).

A LAN can be built by using basic intermediary devices like hubs, bridges, and basic switches to connect end devices (i.e. PCs, phones, printers and etc.)

As a basic the network continues to grow in complexity and size, it becomes more difficult to manage and maintain security and efficiency. In result, network disruptions and network downtime may occur.

In the example illustration below: A home network may have a network consisting of PCs, mobile devices, hub/unmanaged switch, wireless access point (WAP), network attached storage (NAS), and a printer are all connected on the same LAN:



VLAN ID	VLAN Name	Network Address	Subnet Mask	Wireless SSID	Intended Purpose	Link Type	Color code
1	VLAN_1	192.168.1.0	255.255.255.0	VLAN1_WiFi	All devices	Access	▬

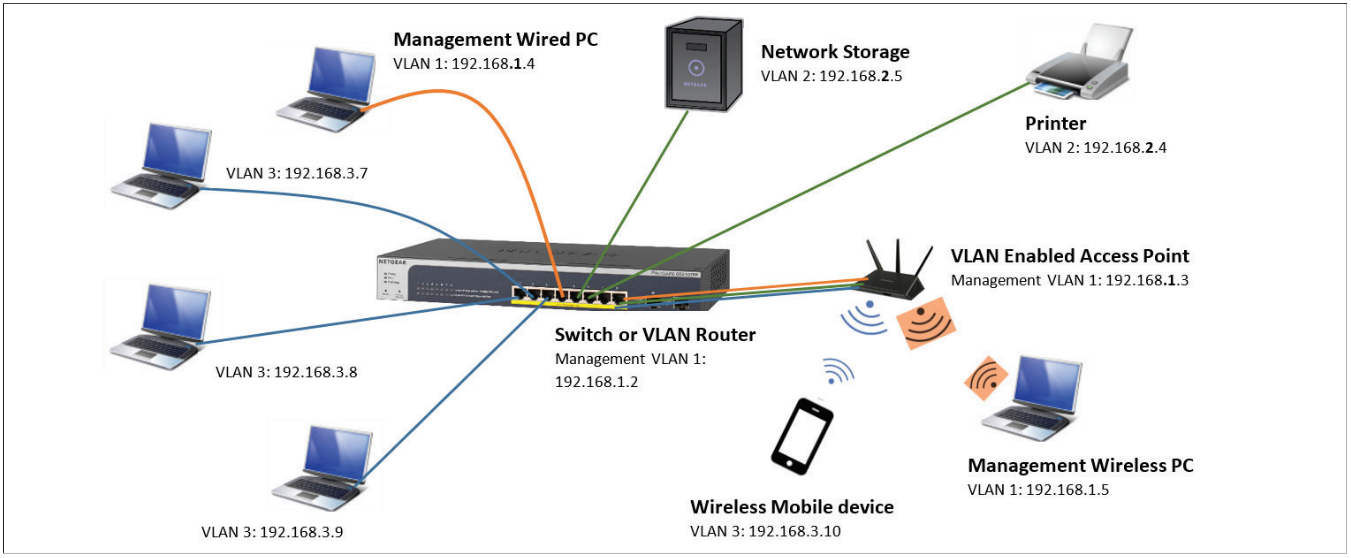
With the same above example illustration, the network may be insecure, inefficient and confusing because:

1. It is easy for unauthorized users to access and modify configurations on any device from any end point on the network as long as credentials or authentication method is open or compromised.
2. It is possible for a packet meant for only one destination to be sent to all end devices, generating unnecessary traffic, wasting resources, hindering productivity and etc.
3. It may be difficult to identify, isolate and resolve network issues during troubleshooting.

To minimize the above issues, Virtual Local Area Networks (VLANs) are introduced. Virtual Local Area Network or Virtual LAN (VLAN)

A physical LAN can be logically sub-divided into smaller LANS, without physically dividing the network. The logical networks formed are known as a Virtual LANs (VLANS). In a VLAN, devices communicate just as if they are logically connected to a physical LAN.

For example: The previous illustration above the LAN can be segmented logically by configuring three VLANs as shown below:



VLAN ID	VLAN Name	Network Address	Subnet Mask	Wireless SSID	Intended Purpose	Link Type	Color code
1	VLAN_1	192.168.1.0	255.255.255.0	VLAN1_WiFi	Management	Access	🟧
2	VLAN_2	192.168.2.0	255.255.255.0	N/A	Shared Resources	Access	🟩
3	VLAN_3	192.168.3.0	255.255.255.0	VLAN3_WiFi	Users	Access	🟦
1 2, 3	VLANs 1, 2, 3					Trunk/ all VLANs tagged	🟧 🟩 🟦

From the above illustration, the network is more secure, efficient and less confusing because:

1. It is not easy for unauthorized users to access and modify configurations on any device from any end point since VLAN_1 management network is kept separate.

2. It is easier to identify, isolate, and resolve network problems during troubleshooting.

VLANs can be configured on VLAN capable devices through management interfaces like Web User Interface (Web UI), Command Line Interface (CLI) or management software like the NETGEAR's Insight app or Cloud Portal for Insight Managed switches. Each VLAN can be configured to communicate to the Internet as well as with each other while remaining as separate logical network segments. This is known as Inter-VLAN routing. Inter-VLAN routing requires the help of a VLAN supported router or a VLAN supported smart switch. To communicate to the Internet and to other VLANs, it would require static or dynamic routes within the router to communicate to other VLANs on the network switch.

NETGEAR VLAN Terminology

VLAN ID: A VLAN ID is a numerical digit that identifies a VLAN. Normally, any number from 1 - 4095 can be assigned to identify a VLAN on a NETGEAR Switch.

VLAN membership: Can be classified by port-based, protocol based, and MAC address based.

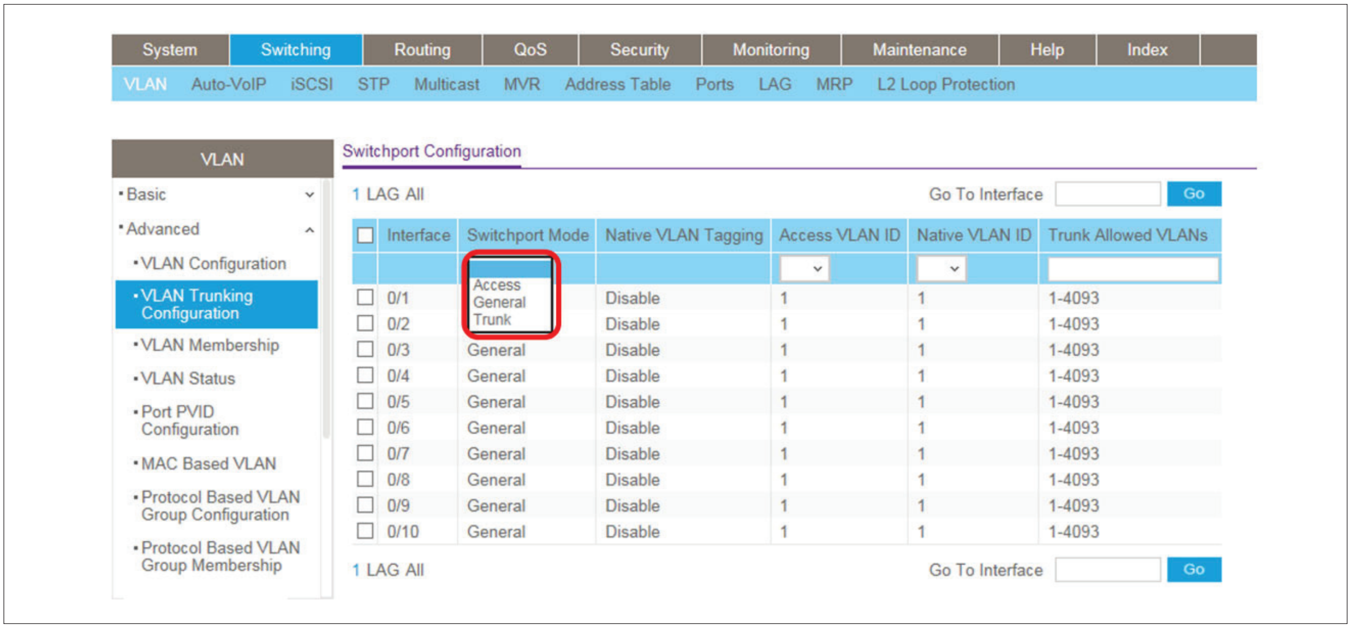
Native VLAN:

On a NETGEAR Switch, a native VLAN is by default:

- Named VLAN 1 with a VLAN ID 1
- The Management VLAN
- All ports are a member of VLAN 1
- Carrying untagged packets

All the above, except the VLAN name and ID, can be modified by a switch administrator.

Switchport modes: Switchports are the ports physically on the switch where the network cables or optics (e.g. RJ45 or Fiber) are inserted. A switchport can be configured to function in one of three modes, access, trunk or general depending on the type of device intended to be connected to it:



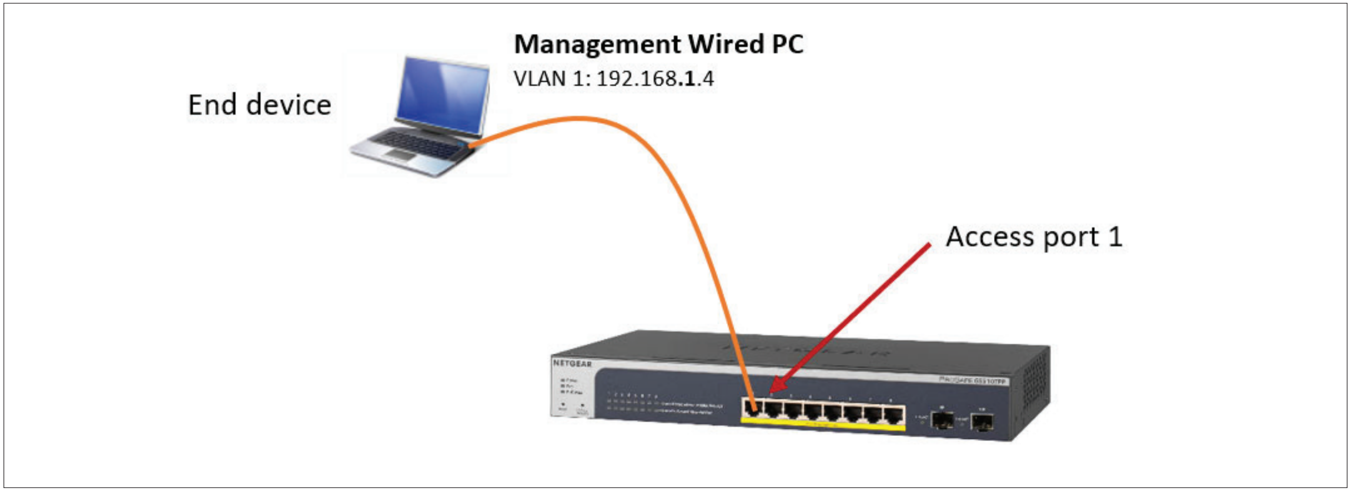
Switchport Configuration

1 LAG All — Go To Interface

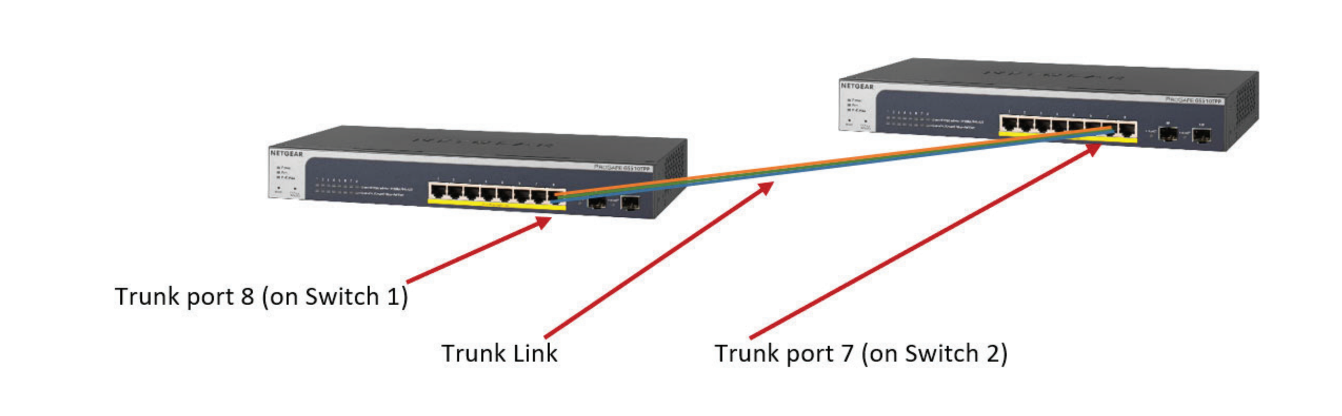
☐	Interface	Switchport Mode	Native VLAN Tagging	Access VLAN ID	Native VLAN ID	Trunk Allowed VLANs
		Access General Trunk				
☐	0/1		Disable	1	1	1-4093
☐	0/2		Disable	1	1	1-4093
☐	0/3	General	Disable	1	1	1-4093
☐	0/4	General	Disable	1	1	1-4093
☐	0/5	General	Disable	1	1	1-4093
☐	0/6	General	Disable	1	1	1-4093
☐	0/7	General	Disable	1	1	1-4093
☐	0/8	General	Disable	1	1	1-4093
☐	0/9	General	Disable	1	1	1-4093
☐	0/10	General	Disable	1	1	1-4093

1 LAG All — Go To Interface

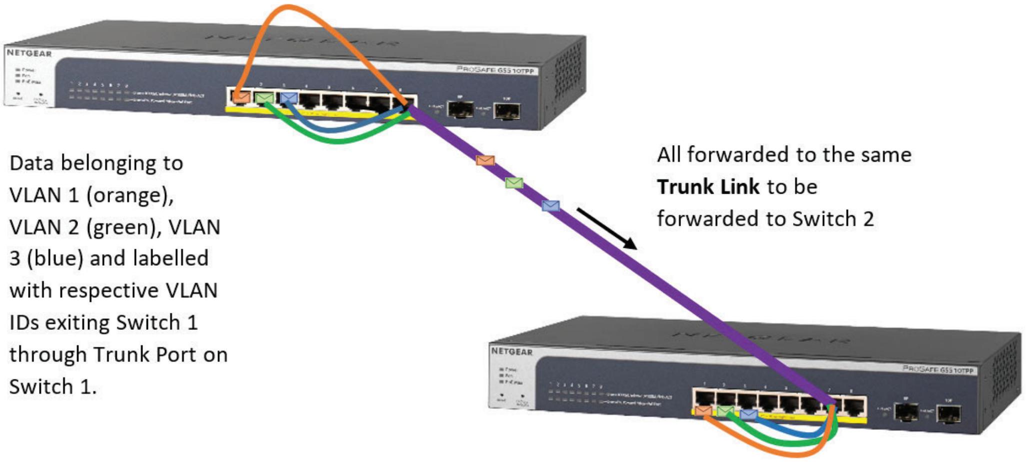
Access mode: In access mode the port becomes a member of only one VLAN. The port sends and receives untagged traffic. The access port can also receive the same VLAN ID tagged traffic, but the tag will be removed by the switchport to send untagged traffic to the device.



Trunk mode: In trunk mode, the port becomes a member of all VLANs on the switch unless specified in the allowed list on the switchport. A link connecting a trunk port from one switch to another trunk port is known as a Trunk link.



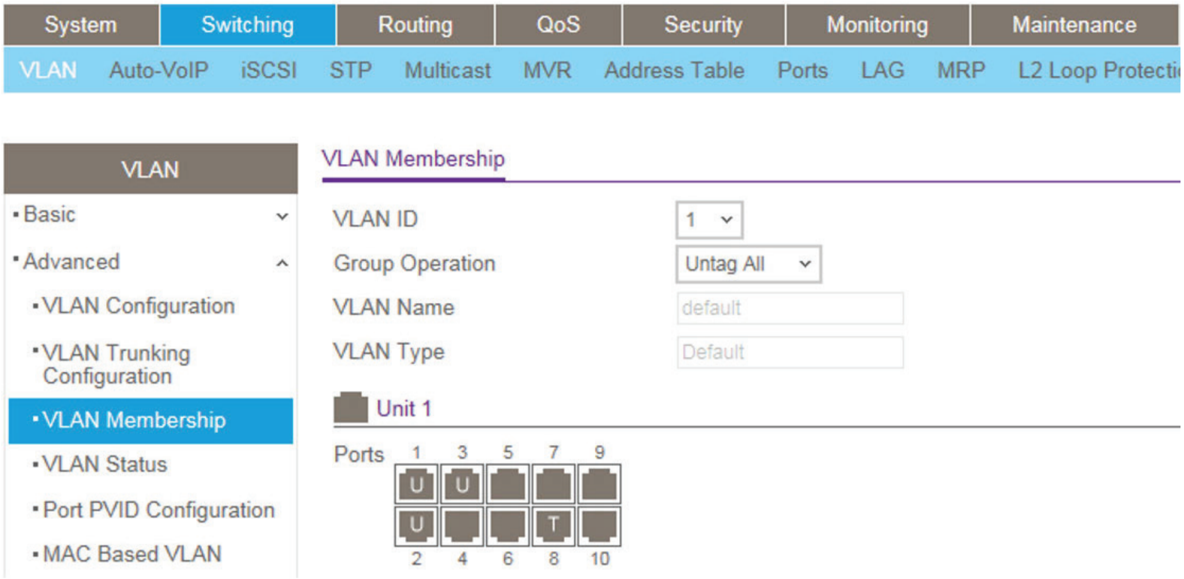
VLAN tagging (on trunk port): Tagging VLAN 2 on a trunk port ensures VLAN 2 ID is inserted into all data packets forwarded from VLAN 2 before they exit the switchport. This helps identify the data packets as belonging to VLAN 2 on the other switch.



Data belonging to VLAN 1 (orange), VLAN 2 (green), VLAN 3 (blue) and labelled with respective VLAN IDs exiting Switch 1 through Trunk Port on Switch 1.

All forwarded to the same **Trunk Link** to be forwarded to Switch 2

All the packets labelled with respective **VLAN IDs** exiting the common Trunk Link and entering Switch 2 through Trunk Port on Switch 2, then later to respective VLANs depending on VLAN ID labels (or **tag**s)



VLAN Membership

VLAN ID: 1

Group Operation: Untag All

VLAN Name: default

VLAN Type: Default

Unit 1

Ports

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

General mode: In general mode, the user can perform custom configuration of the VLAN membership, PVID, tagging, ingress filtering, and so on. The general mode is the default behavior of the switchport configuration.

PVID (Port VLAN ID): A default Port VLAN ID (PVID) of a port is the VLAN ID that will be assigned to any untagged frames entering the switch on that port.

On an access port, the VLAN ID of the VLAN assigned to that port is the Port VLAN ID.