



Network Topology

Proper setup of network layout.

Network Topology

This will guide you through understanding a network topology and proper setup of a network.

A network topology is made up of “**nodes**,” these are the devices in your network, such as routers, switches, and access points. This provides you with a physical and logical arrangement of how the traffic flows through your network.

The topology of our network will be one of the main deciding factors of how efficient your traffic flows.

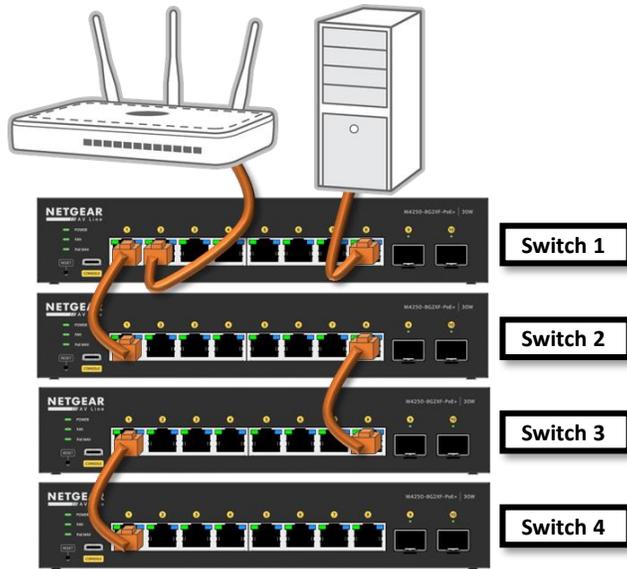
For example: Let’s say that we have 4 switches, a router and a server.

Daisy Chain Topology

In this topology we have the switches connected in a chain, this type of topology is called “**Daisy Chain**” topology where one switch connects to the next and so on.

This is not very efficient for any computers connected on switches 3 and 4 since the traffic will go through the other switches to reach the router or server.

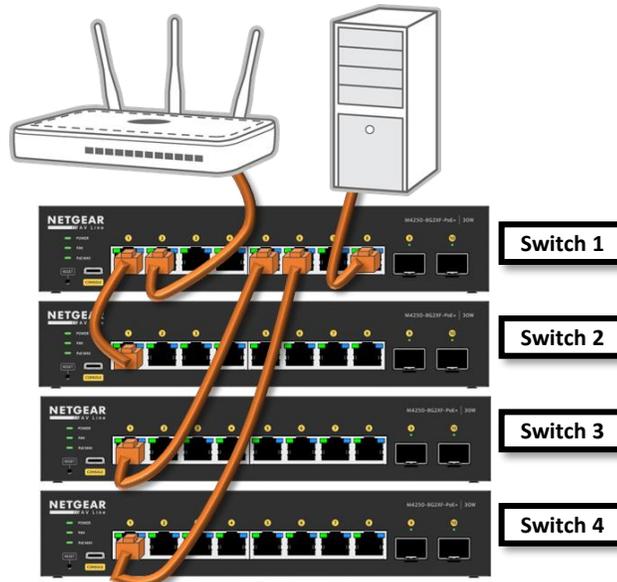
Also, If one of the switches in this chain goes down all the switches further down the chain will also lose connection.



Star Topology

In this topology “**Switch 1**” is acting as our “**Core**” switch, all other “**Edge**” switches connect directly to “**Switch 1**” and will only have one hop to access the router or server.

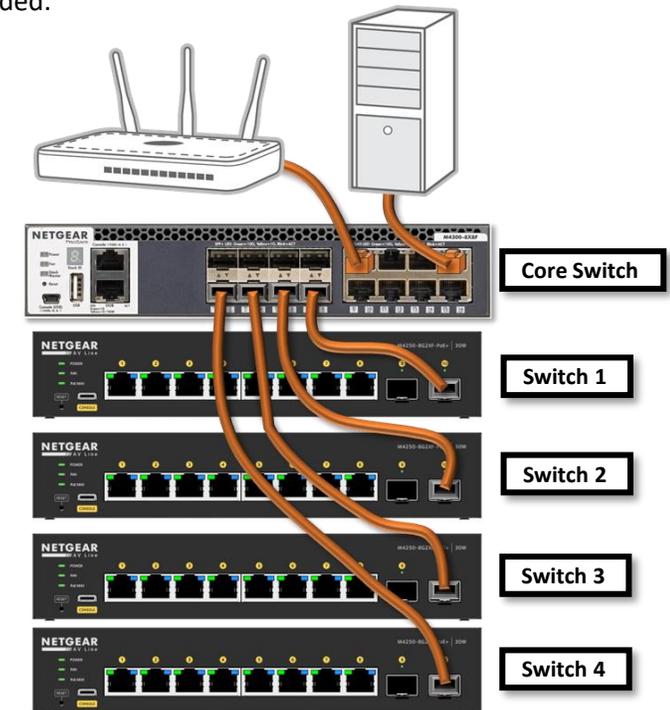
If one of the “**Edge**” switches requires a reboot, or if it goes down, it will not affect the other devices connected to the “**Core**” switch.



Advanced Star Topology

In this topology we have added a “**M4300-8X8F**” as our “**Core**” switch and we have all the “**Edge**” switches connected via the 10GB SFP+ ports.

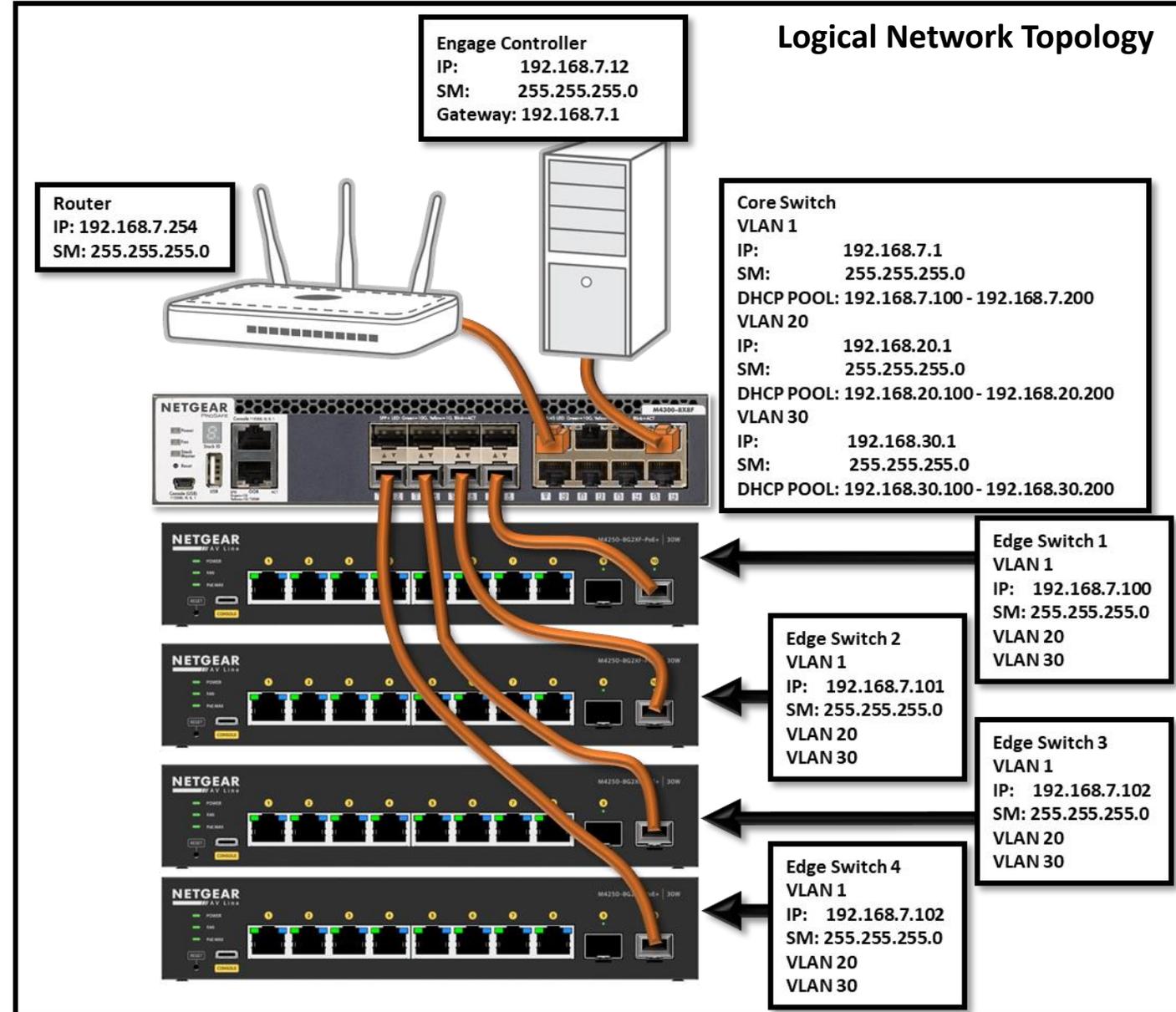
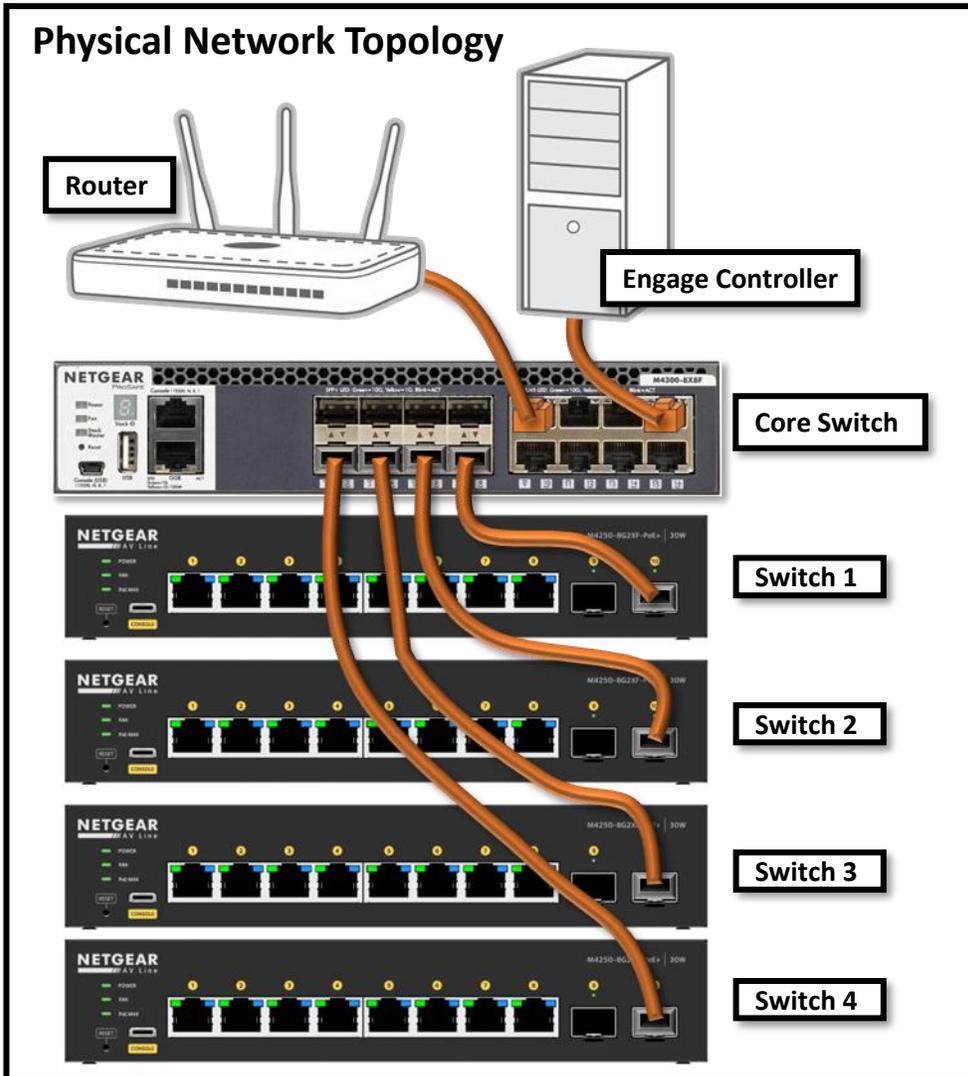
This provides all the “**Edge**” switches with a 10 Gb uplink to the “**Core**” switch and allows for the network to be easily expanded.



The topologies that we have looked at so far have been “**physical**” network topologies, there are also “**logical**” network topologies. The difference between these is that a “**physical**” topology will show the devices and how they are connected, while a “**logical**” topology will show us not only how they are connected but how the network is configured, how the traffic flows.

As you can imagine, a logical topology can make the difference between a short troubleshooting session to find the issue and having to spend hours to map out the entire network to discover the issue.

Here we can see a physical and logical topology side by side:



The first step in designing your network is to create a physical topology, this will set the layout that we need in order to design the logical layout.

When planning out your network you will need to keep in mind what you currently need, along with possible future needs.

In our example the core switch is connected to all the edge switches, we have the default VLAN 1, VLAN 20, and VLAN 30. The VLANs created on the core switch are layer 3 routable VLANs, the core switch is also the DHCP server for all the VLANs (in this scenario we disabled DHCP on the router and created a DHCP pool on the core switch for VLAN1.) The edge switches have the same VLANs, but the difference is that the edge switches have layer 2 VLANs. The routing will occur on the core switch and the VLANs will be tagged to the edge switches. Auto-Trunk will detect the NETGEAR switches and will automatically tag the VLANs to each one of the switches.

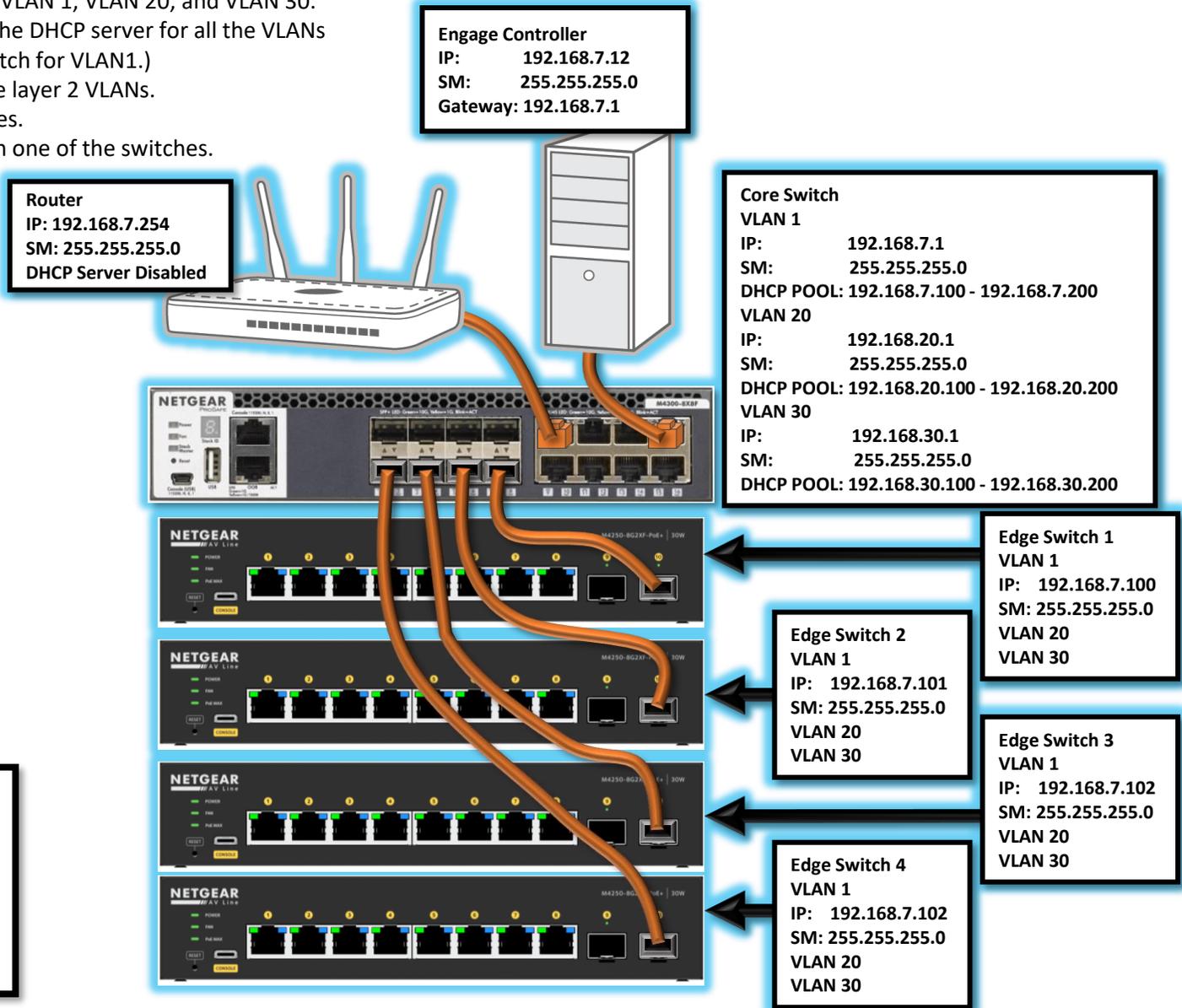
In order for VLAN 20 and 30 to be able to have access to the Internet you will need to have a default route on the core switch to forward the traffic to the IP address of the router "192.168.7.254" and the router will need the routes that will say that if you are trying to reach the "192.168.20.X" subnet go to "192.168.7.1" (the IP address of VLAN 1 on the core switch) for VLAN 20, and another route for the "192.168.30.X" subnet pointing to the IP address of VLAN 1 on the core switch.

The traffic for the VLANs will be routed through the core switch using VLAN 1 to reach the router and access the Internet, when the traffic comes back from the Internet the router needs to know where to find the subnets for the VLANs, that's why you must create the routes on the router to the core switch.

If we then want to expand our network and add another VLAN, you can create another layer 3 VLAN on the core switch, create the subnet for it and then create the route for the new subnet on the router pointing back to the core switch. You will then need to create the layer 2 VLANs on the edge switches.

If you are not using the "Auto-Trunk" feature, you will have to make sure that the uplink ports on the core and edge switches are tagged for the VLANs.

NOTE: The reason why all the switches in our topology have an IP address on VLAN 1 is because VLAN 1 is by default a routable VLAN with DHCP enabled. When the switches come up, VLAN 1 will request an IP address and if they do not receive an address within 120 seconds, they will revert to their default address "169.254.100.100" with a subnet mask of "255.255.0.0."



An issue with the topologies that we have gone over is that there is no redundancy, If the core switch goes down, the entire network goes down.

We can create a redundant network that will allow for a switch, even the core switch to go down and still allow for the devices on the network to be able to access the Internet and server.

The topology below is that of a redundant network, you have the core as 2 switches stacked and the router, server and switches connected using LAGs to each one of the core stacked switches.

This type of topology requires a bit more configuration, but it provides the redundancy that removes a single point of failure on the network.

