CCNA – complete course by Network Chuck

**Day 1 : What is Switch ?**

* Internet is a network of computer networks.

How advance the internet get but the essence is to established communication ( term communication is sharing data and resources ) between two or more computers with one, another. To make one computer able to communicate to another computer in simple understanding, but when it comes to the medium, the process, and pathways of communication it get’s complex. And the concept of routers, switches, LAN, WAN, MAN, firewalls, modem, fiber cables, ethernet, ports, servers , ISP etc… came.

Note : WAP – Wireless Access Point

Hub :

A **hub** is a basic networking device that connects multiple devices in a LAN and operates at the physical layer. It sends a message from Device A to all devices connected to it, so even if the message is intended for Device B, every device on the hub receives it.

Switch :

A **switch** is a smart networking device that connects multiple devices in a LAN and sends data only to the intended recipient, unlike a hub which broadcasts to all devices, thereby reducing collisions, improving bandwidth, and enhancing overall network performance. It is Layer 2 device.

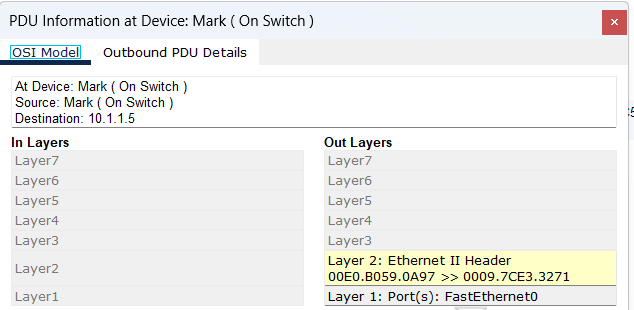
MAC : **Media Access Control**

MAC address is Layer 2 address, which is **unique hardware address** assigned to a network interface card (NIC) that identifies a device on a local network.

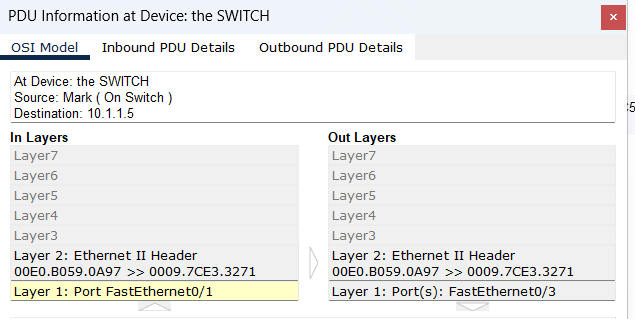
Layer 1 : Physical wire, cables, electrical wires, metal wires that send electrical signals down into the switch.

Process between sending and receiving packets in switch :

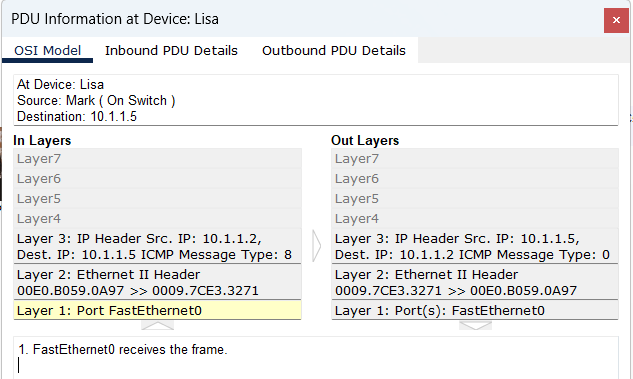
At source : 10.1.1.2



In between switch :



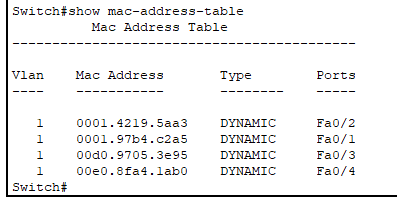
At destination : 10.1.1.5



Switch cli command :

Switch1# show mac-address-table

It show the mac address of all devices connected , when devices have interaction by ping each other.



All the messages going through the switch are called frames.

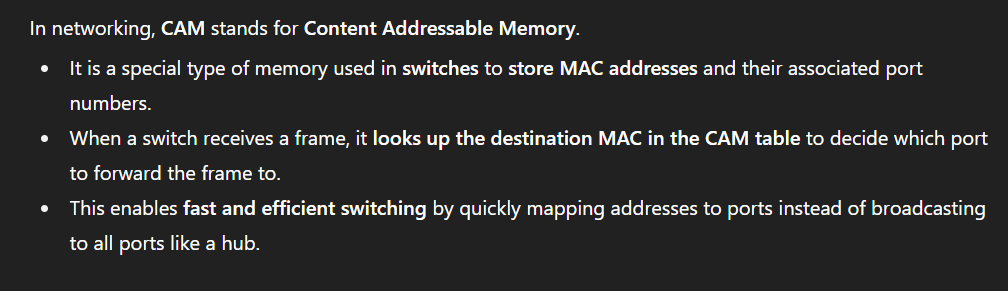
Layer 2 : includes switch , frames , mac-address

In layer 3 : at ip address level the message received called packets.

Note : A wireless connection is more like a hub , that’s why people suggest a ethernet cable connection over a wireless connection.

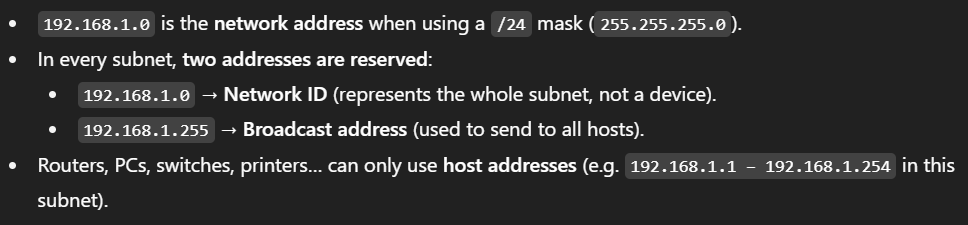
Inside switch CAM table to see the mac address assigned to connected devices.

What is CAM ?



CCNA – DAY 2 : what is router ?/ what is TCP/IP and OSI ?

Routers are layer 3 devices , their language is ip addresses. Routers help to connect different networks.



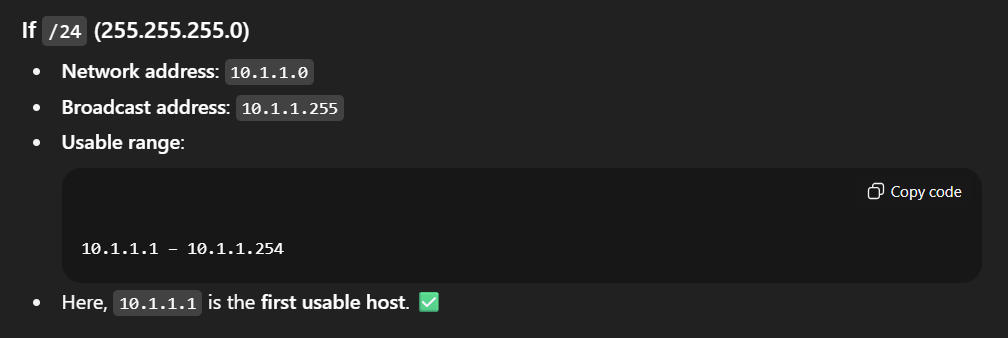
Routers cli commands :

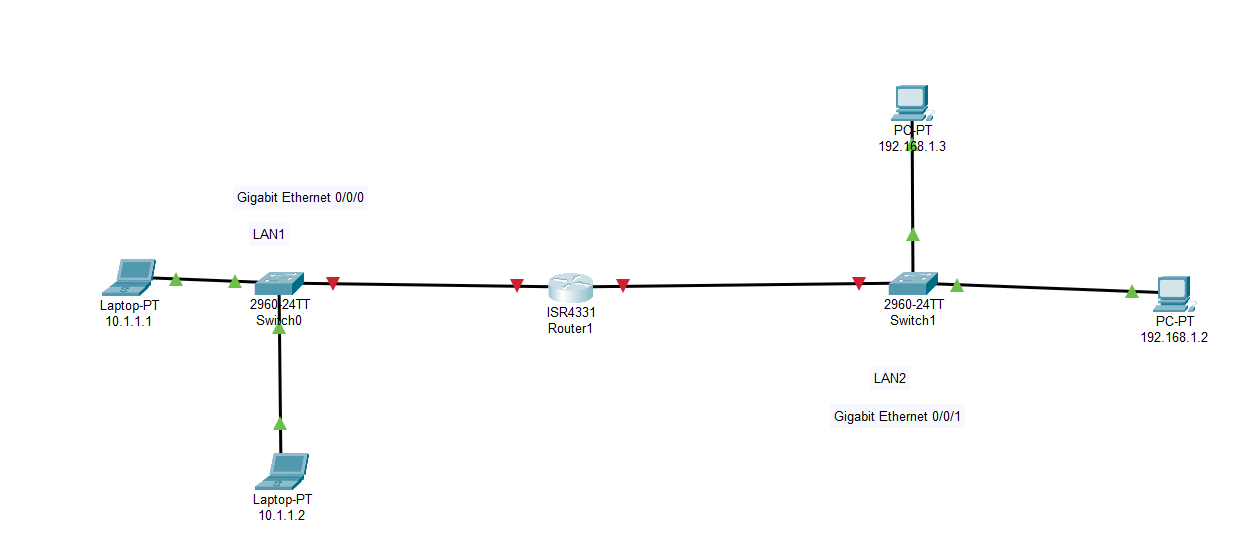
Router > enable

Router# show ip route : show ip address, subnet range in router networks

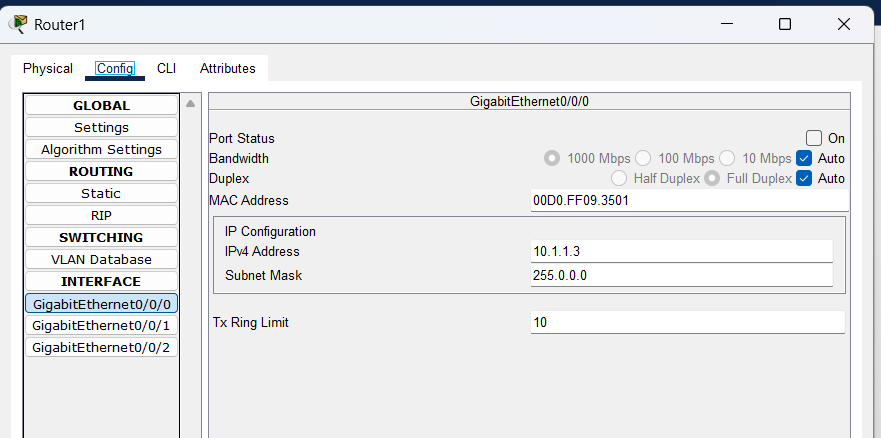


Case 2: 10.1.1.0 it is for /8 subnet mask not for /24

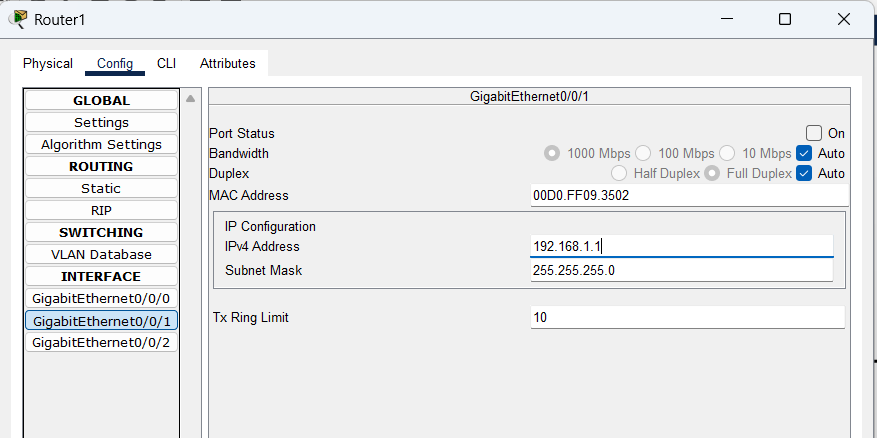


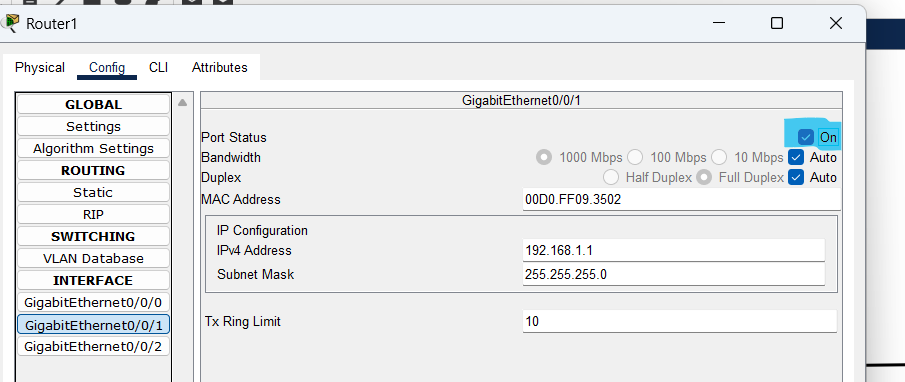


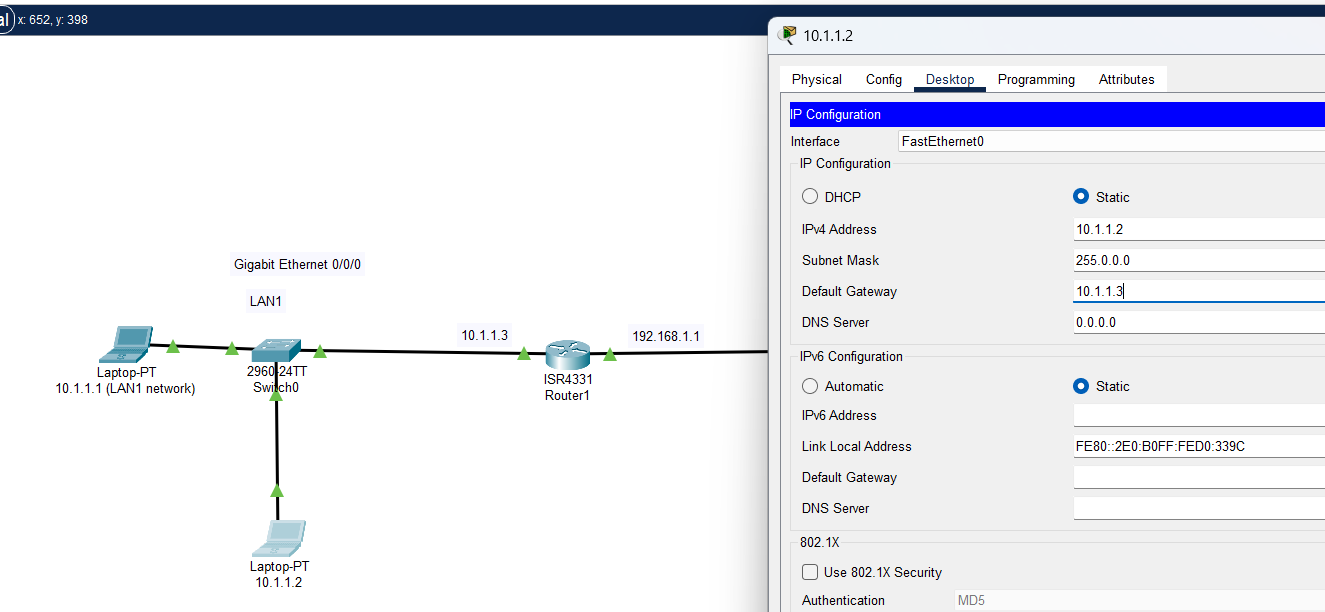
Configuring ip for LAN1 connection

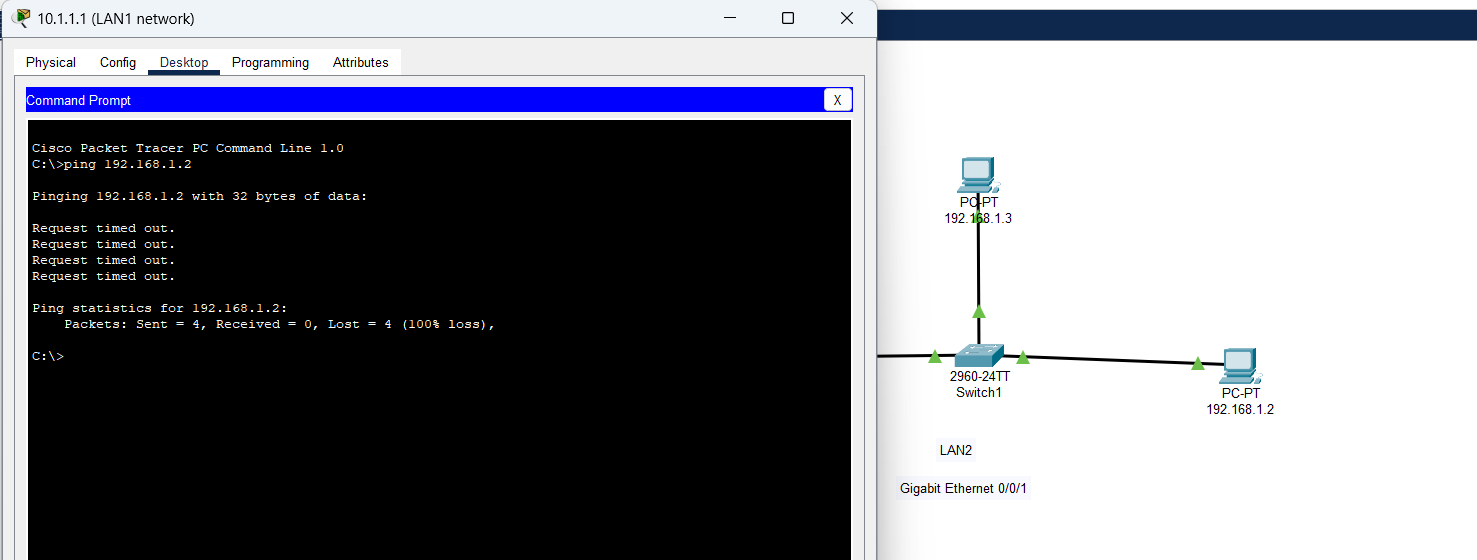


Configuring ip for LAN2 connection

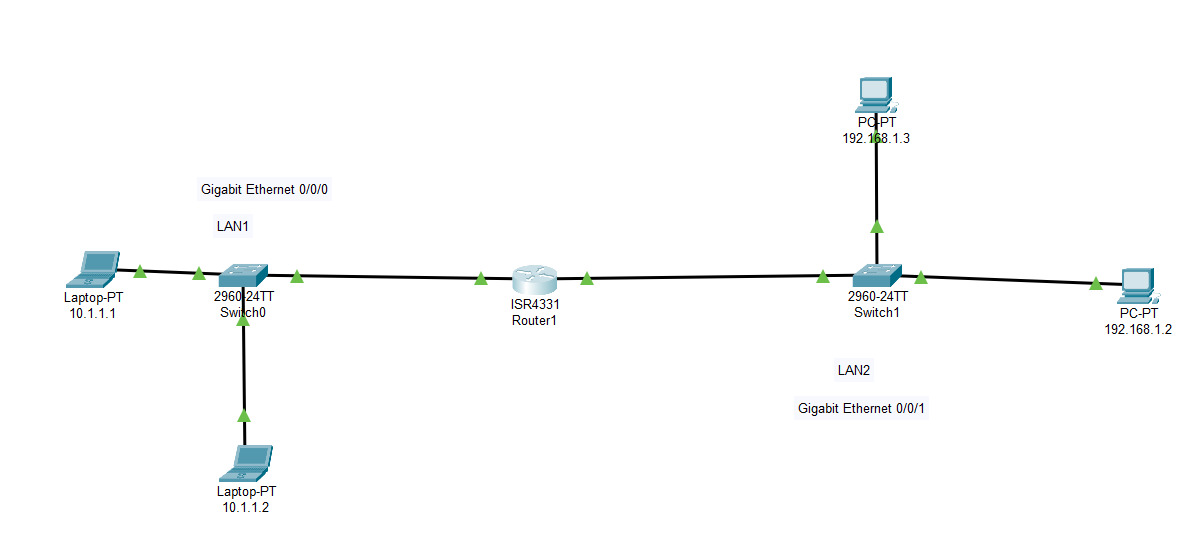


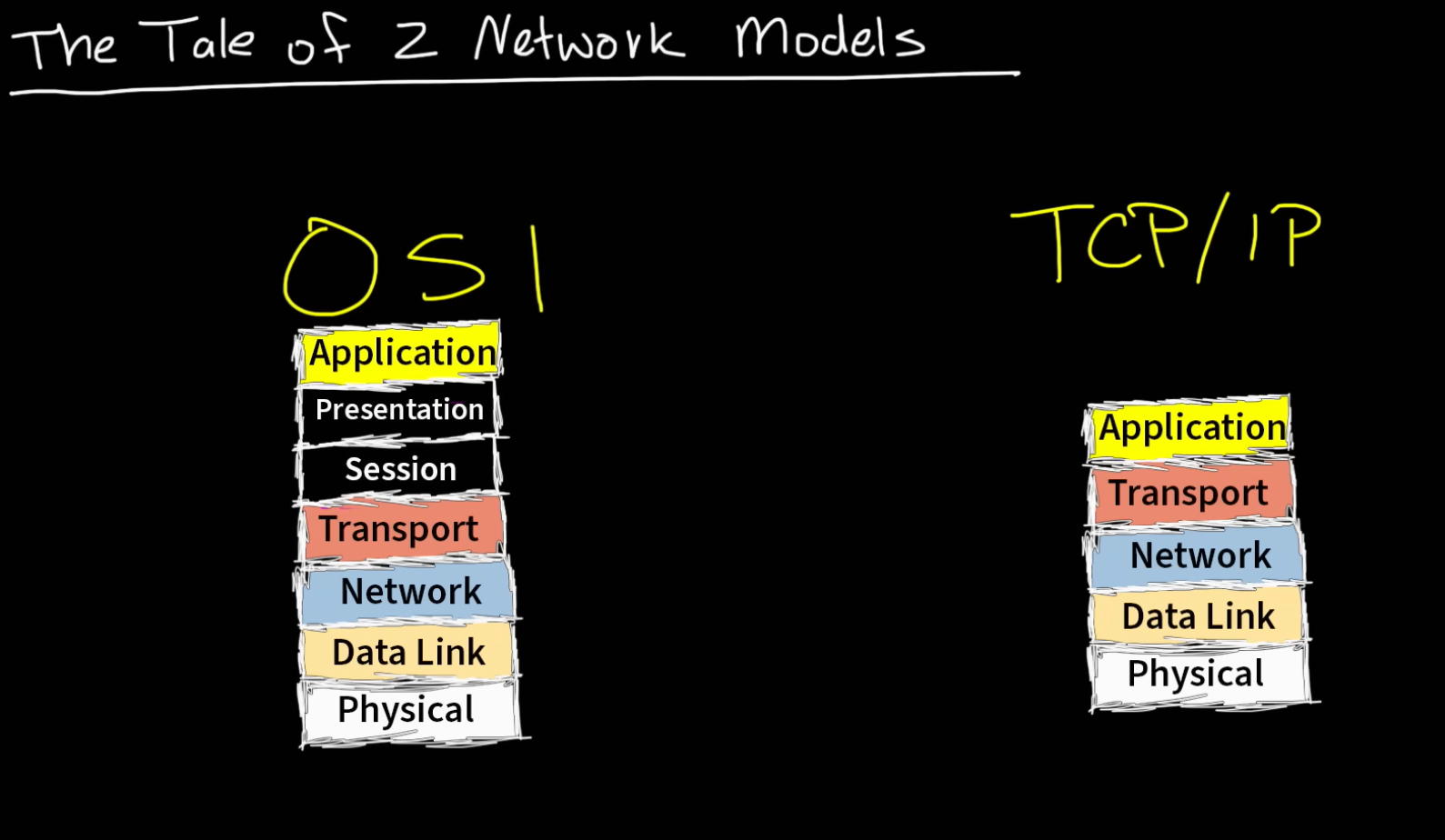












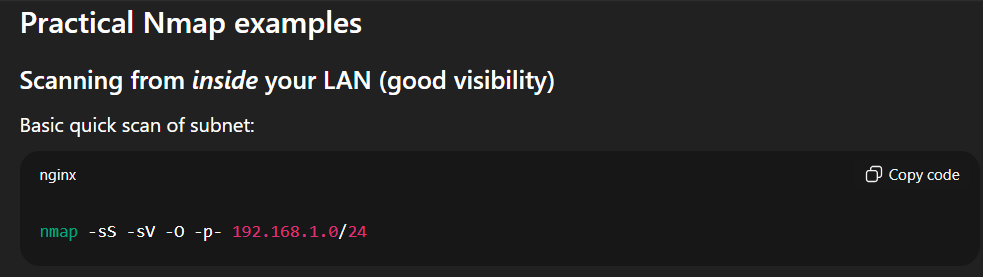
The **OSI model** is a seven-layer theoretical framework that describes how data moves across a network. Its layers are Physical, Data Link, Network, Transport, Session, Presentation, and Application. It is mainly used as a reference model to understand, design, and troubleshoot networks. It is a **theoretical reference model** with **7 layers**.

The **TCP/IP model**, on the other hand, is a four-layer practical model that is actually used in real-world networking, including the Internet. Its layers are Link, Internet, Transport, and Application. Unlike OSI, it defines real protocols such as IP, TCP, UDP, HTTP, and DNS, making it the foundation of modern networking.

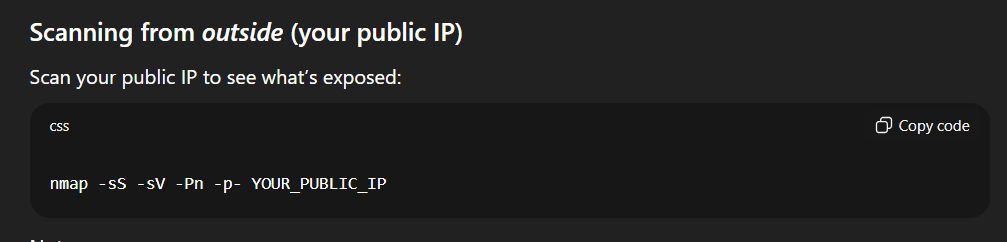
Nmap network scanning from outside of network :

nmap –script vuln <publicipof network>

nmap -sT <publicipofnetwork>

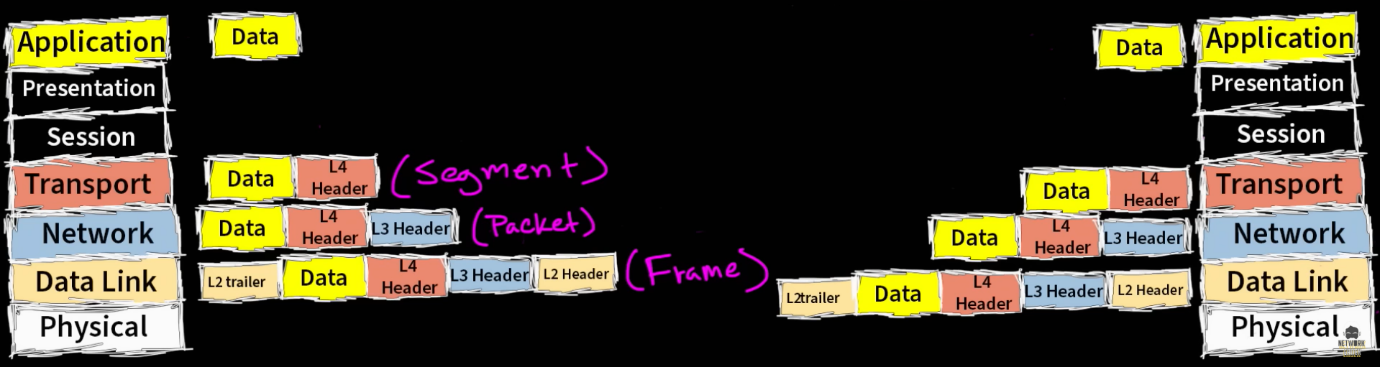


192.168.1.0 should be your private ip in home network !



What is TCP/IP and OSI layers

OSI layer :



How the OSI model works on Youtube ? ( Appilcation and Transport layers )

Application layer : Kind of portal / interface for application to communicate

over a network.

Presentation Layer : Handles two part contributing how the data will be presented , obviously in understandable form.

1. Data format = Data types 2. Encryption ( SSL )

Presentation layer would take our data and put it in a format that we understand ie HTML by web browser.

Session layers keeps the communication open or established.

Transport layer is like transporting packages or data , where all this is ready to ship from the source location. Where the transportation occurs with two commonly known protocols ( TCP , UDP ).

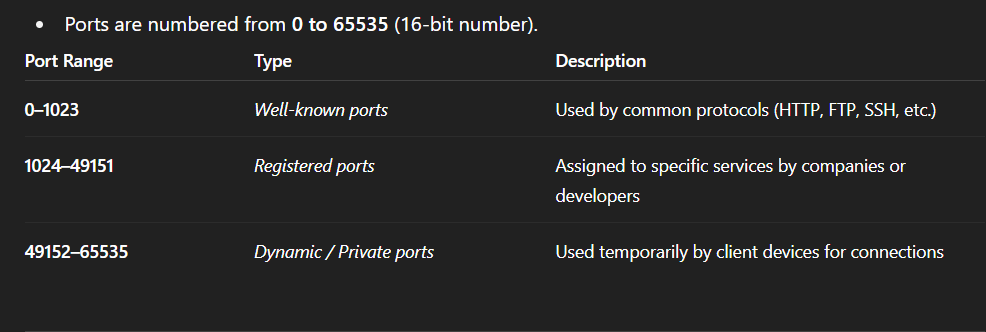
TCP = Transmission Control Protocol ( reliable perform 3 way handshake ), and wants control in every bit of communication

UDP = fast but not reliable

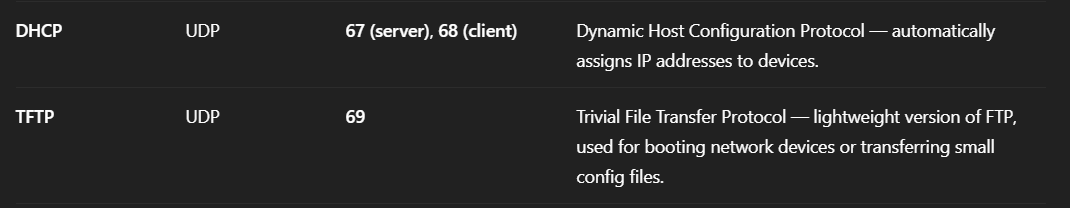
Application layers, presentation layer, and session layers are just one layer in TCP/IP mode just the application layer.

What are Ports ?

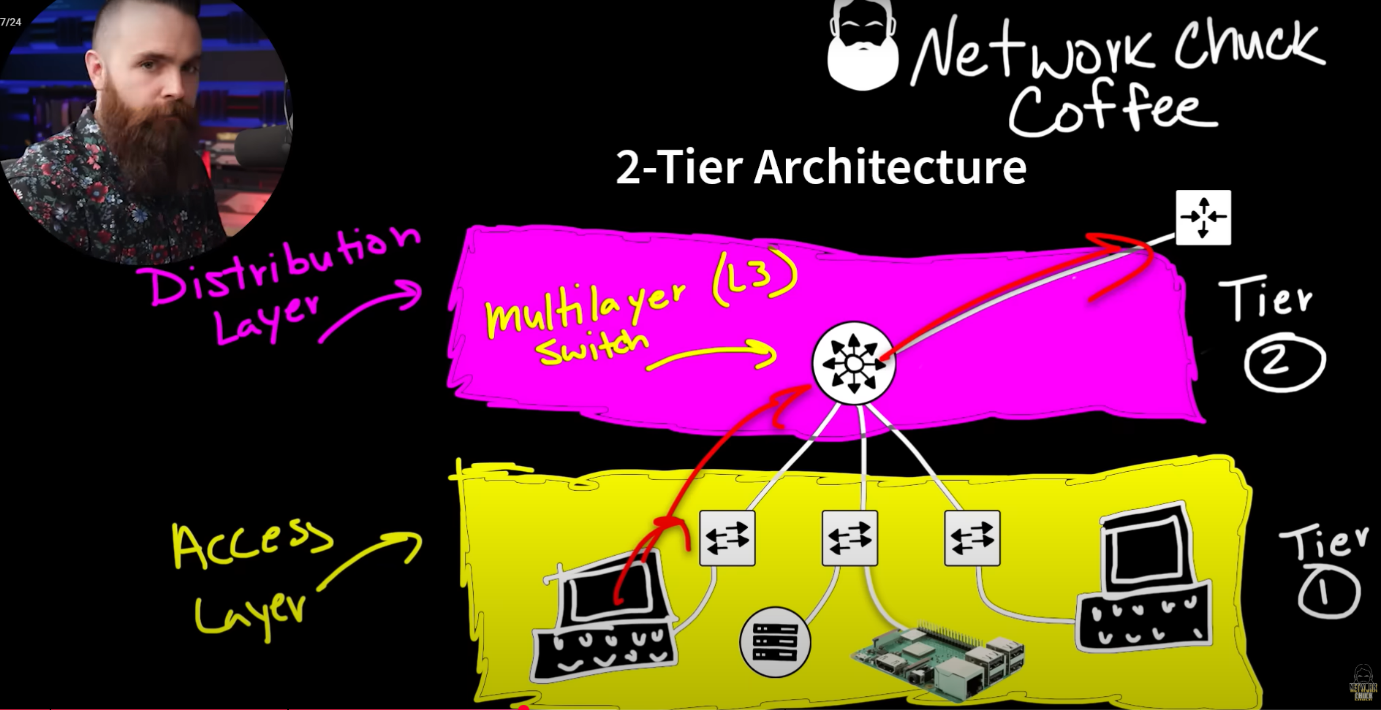
The **port number** identifies *which application/service* on that device should handle the data. Ports allows us to run multiple services on one server.

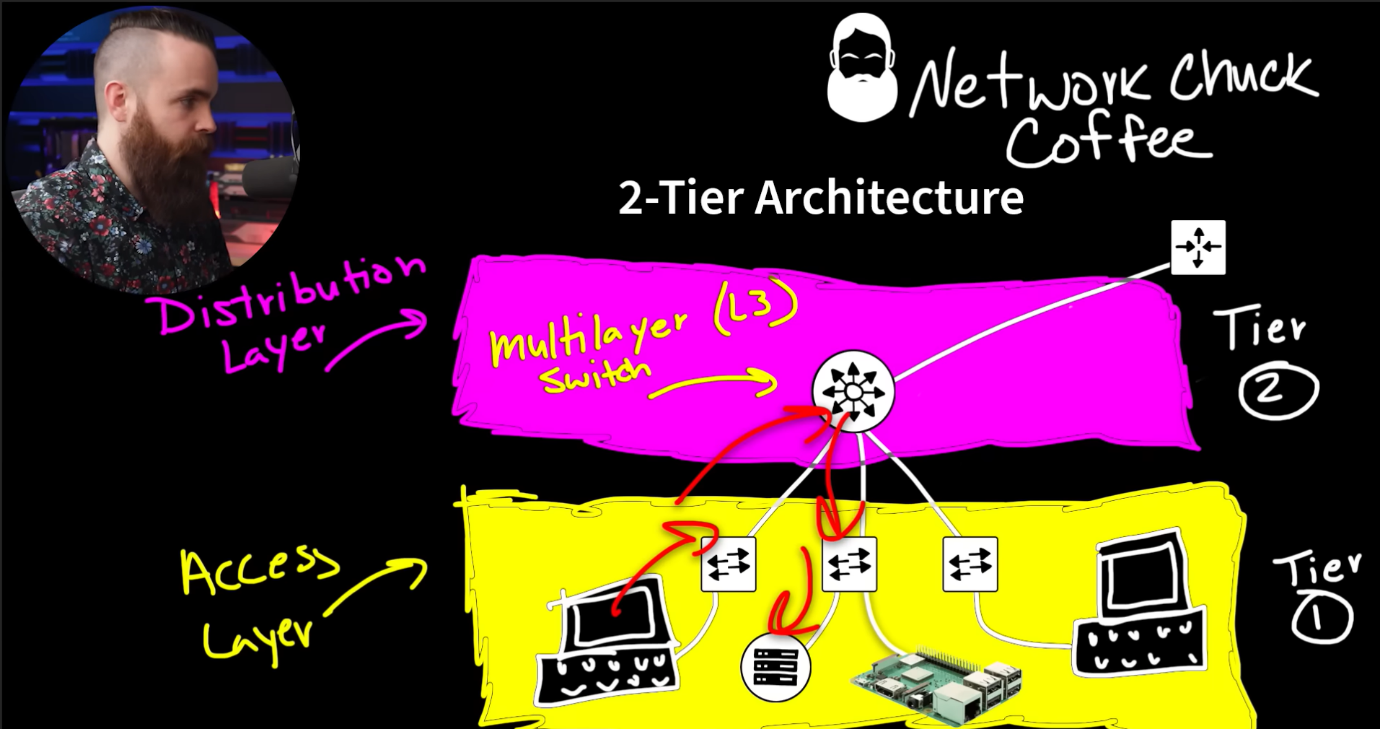


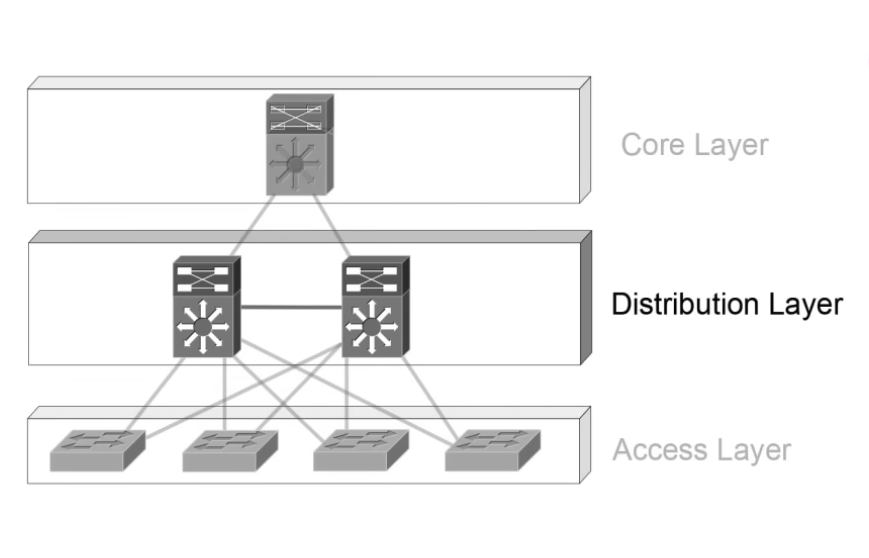




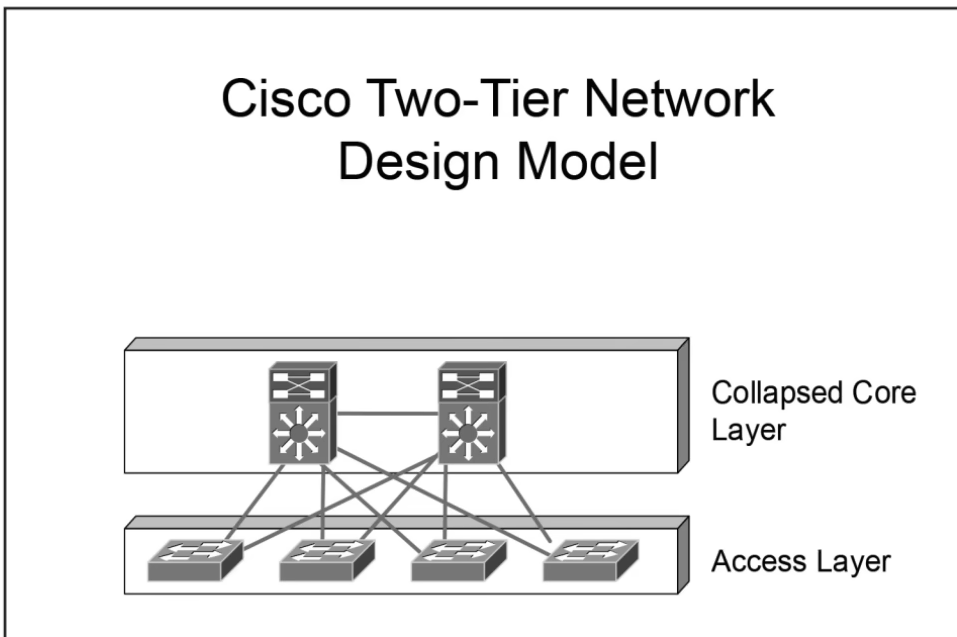
Network Design





 Tier 3

Tier 2

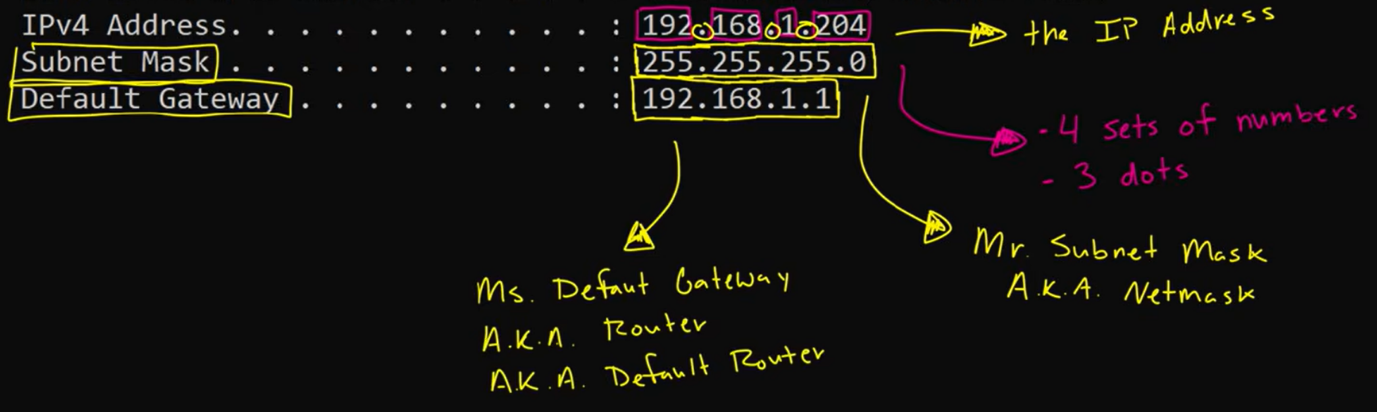


A **VLAN (Virtual Local Area Network)** is a **logical separation of a single physical network** into multiple virtual networks. Each VLAN behaves as if it were a separate LAN — its own broadcast domain — even though the same cables and switch hardware are used.

Note : Fiber optics cable uses light to transmit data.

What is an ip address ?

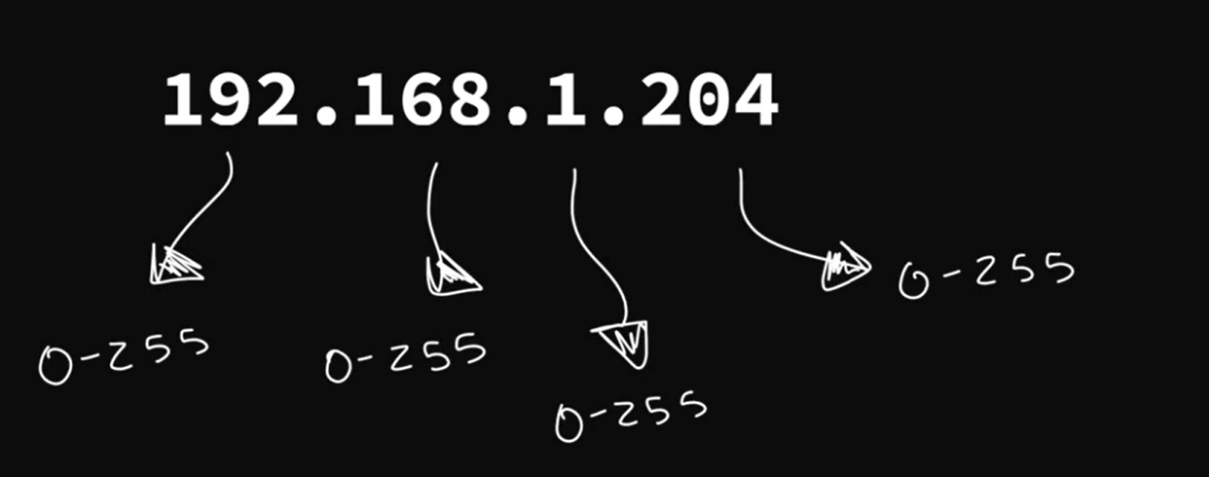
IP ( Internet Protocol ) is like name of the person or typical address of house. It allows a way to communicate between devices across the internet, basically why we need to know other’s name or address just to call, or locate them , it’s a basic presequite of communication right. It also opens up the ability to connect to the internet.

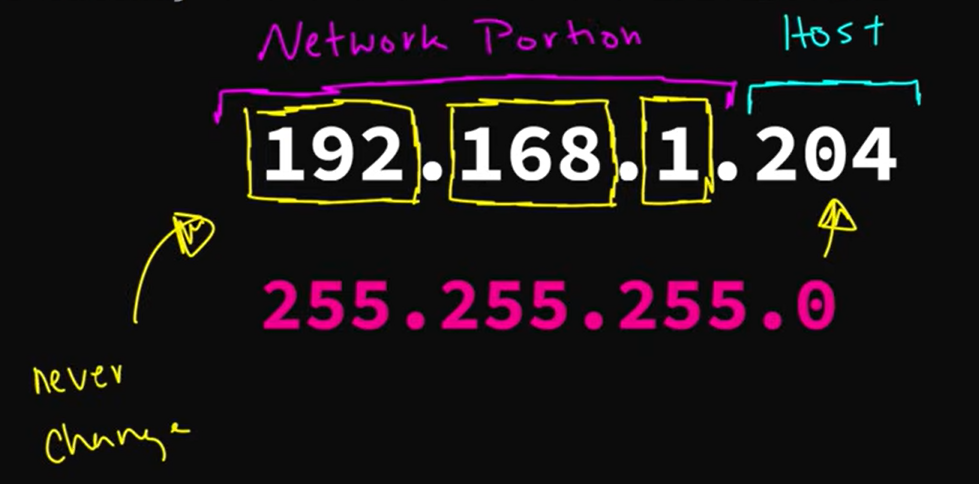


Just press win key + R and type cmd, and type command : ipconfig

And you will see your ip address also known as ipv4, you sub netmask, default gateway etc..

And router provides ip address to the devices in a network.





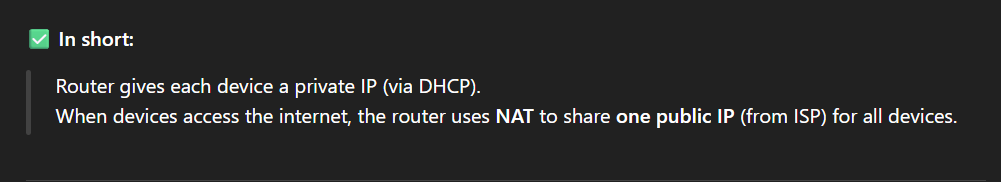
If first three octats in sub-netmask is 255.255.255.0 , then probably and mostly you ip address should look like this 192.168.1.X in your network ..

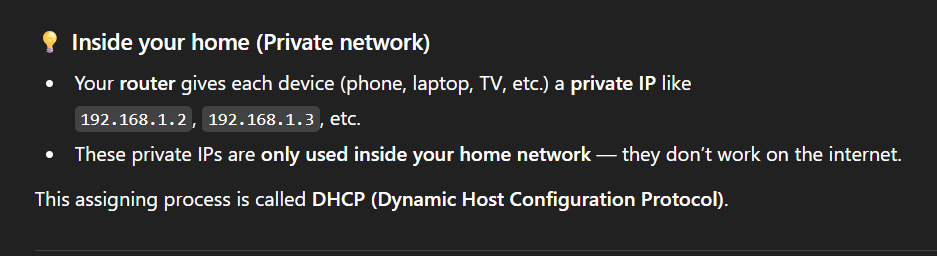
Any devices can’t assign Network address and Broadcast address, and another is default gateway ip which is obviously assign for Router itself as device in network as ip address under X range : 0-255

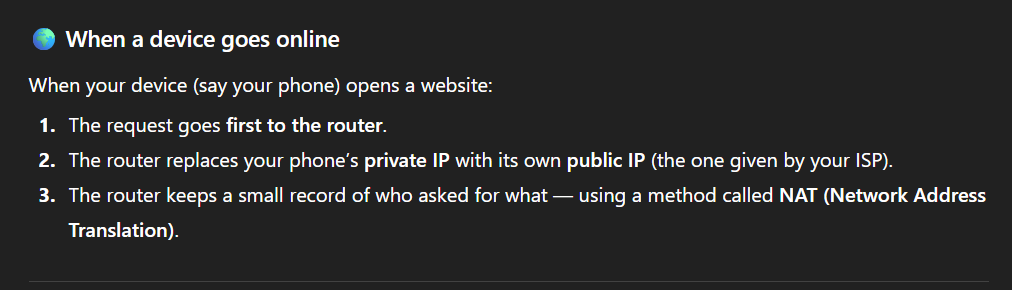
Network address : 192.168.1.0

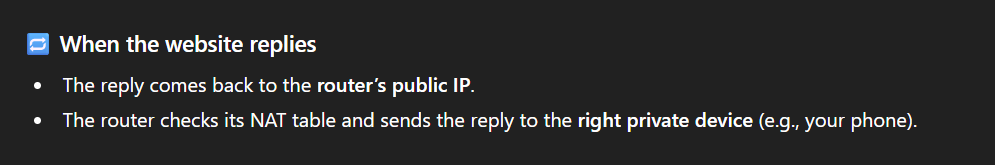
Broadcast address : 192.168.1.255

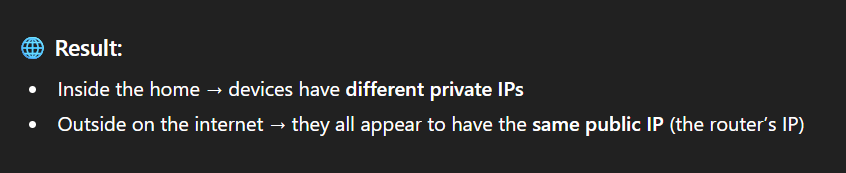
Here is an interesting thing that if the devices on a local network want to visit other different network then router will help to locate and navigate to other network address there are many examples like of google, Netflix, youtube, literally they are ip address / location on another network and our devices want to communicate with them , which both are in complete networks, so that’s why routers are so much helpful in this case.

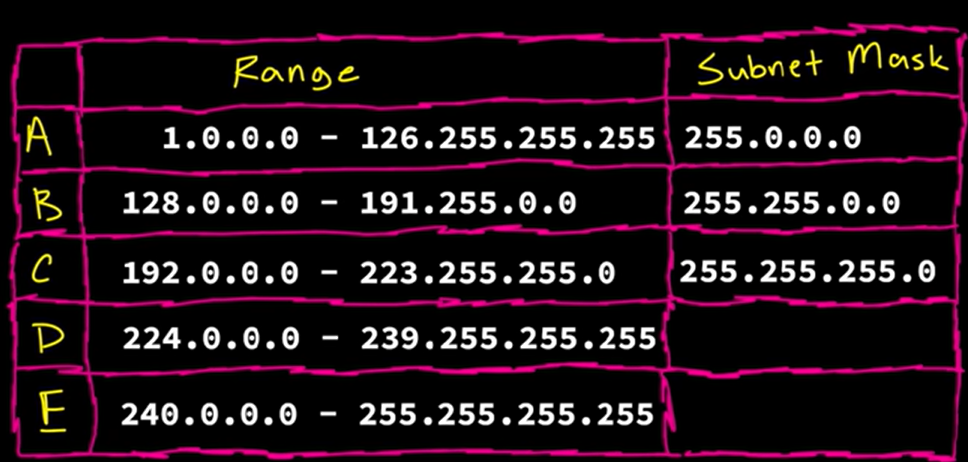






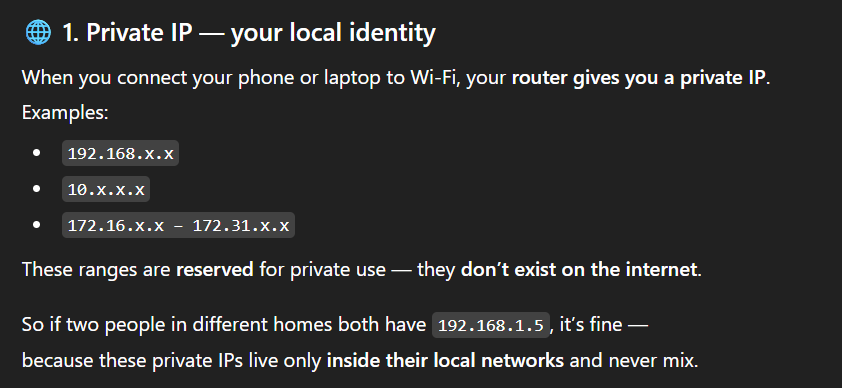


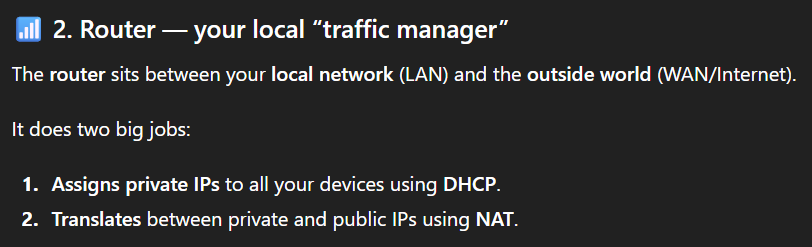


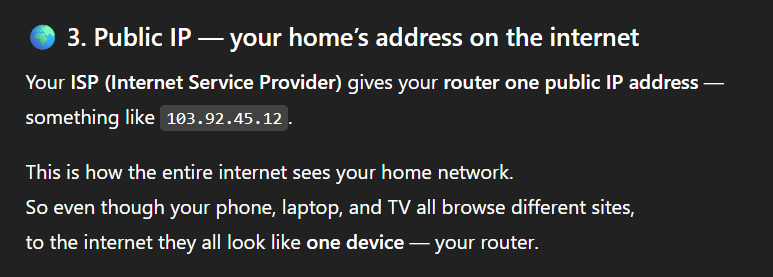


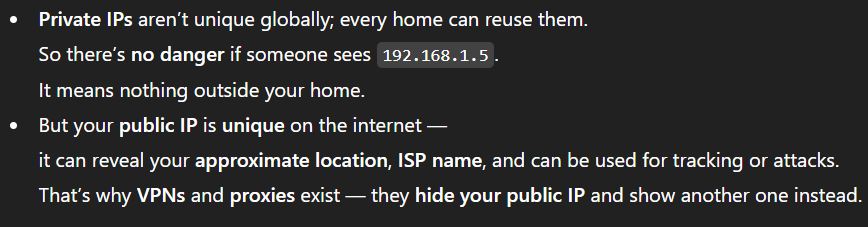
127.0.0.0 is loopback address which is the address of our own device , as localhost.











The continuous rewriting of source and destination addresses is what “Network Address Translation” means. It allows many private devices to share one public IP address, conserving the limited number of IPv4 addresses in the world. It also adds a layer of security, because external devices cannot directly see or reach your private IPs; they only interact with the router’s public interface. In this way, NAT elegantly bridges your private world and the public internet, keeping everything organized, efficient, and safe.

With **IPv4**, NAT was necessary because we ran out of public IPs.  
With **IPv6**, NAT is no longer needed — each device can have its **own unique public IP**.  
Still, routers and firewalls protect these devices, so the internet doesn’t become a free-for-all.

X.X.X.X : in total binary form it is 32 bits, so that each octats is of 8 bits.

What is Subnet Mask ?

255.255.255.0

Into binary form : 11111111.11111111.11111111.00000000

1 : network bits

2 : host bits

To see how many host can be in any network we got formula for that : 2^( of 0’s)-2

2^8-2 = 254 host in that subnet mask ! ( minus 2 because every network will have two reserved ip addresses )

Subnetting is the process of dividing a larger network into smaller more manageable subnetworks or subnets. For example breaking up current network into smaller networks ie, wireless, IoT, DMZ, User etc