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.

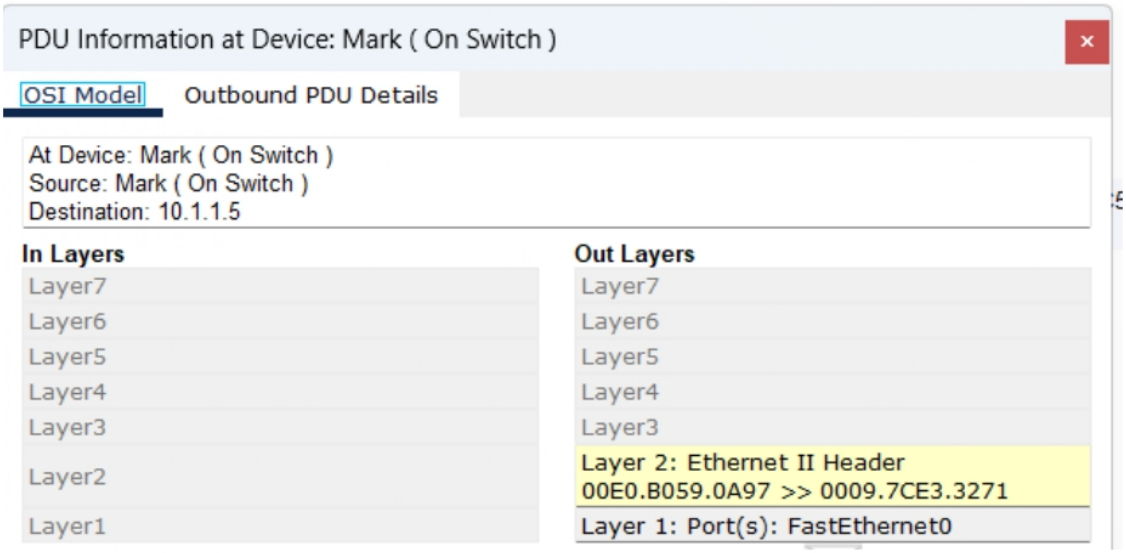
MAC : **Media Access Control**

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.

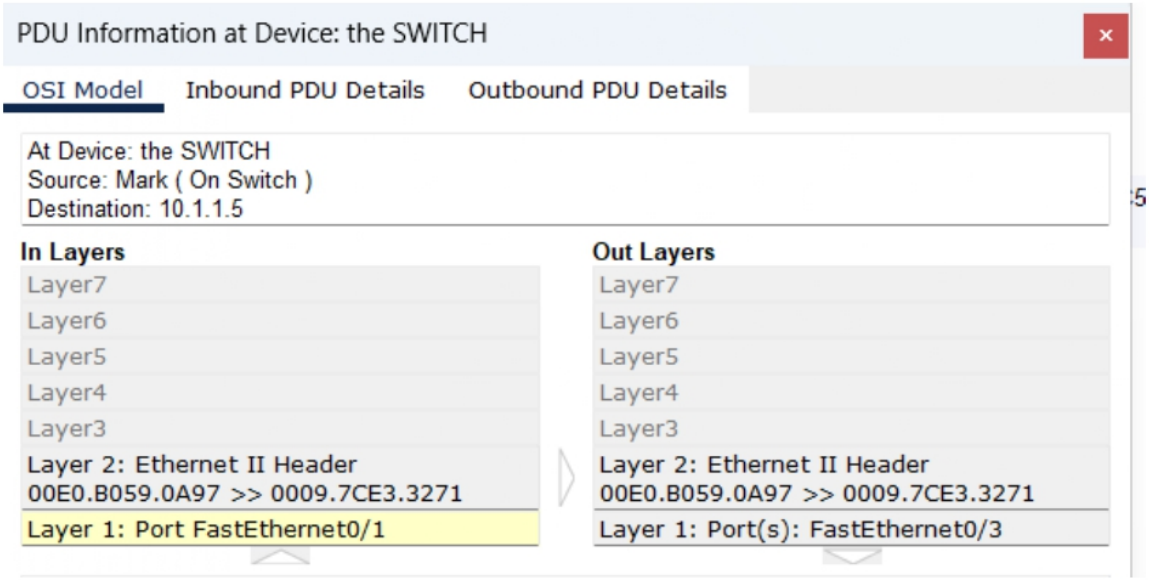
Layer 1 : Physical wire, cables, electrical wires, metal wires that send electrical signals down into the switch.

Process between sending and receiving packets in switch :

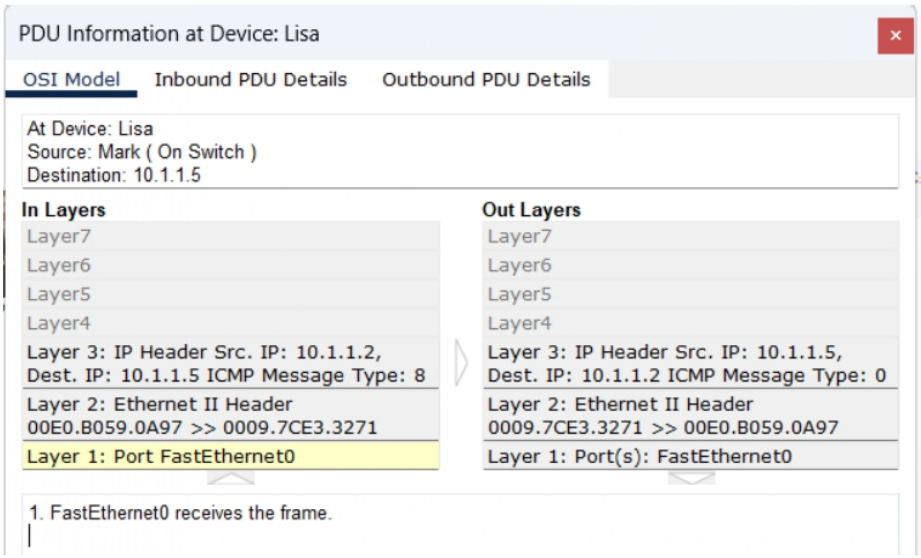
At source : 10.1.1.2



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.

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.4219.5aa3    DYNAMIC     Fa0/2
   1    0001.97b4.c2a5    DYNAMIC     Fa0/1
   1    00d0.9705.3e95    DYNAMIC     Fa0/3
   1    00e0.8fa4.1ab0    DYNAMIC     Fa0/4
Switch#
```

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 ?

In networking, **CAM** stands for **Content Addressable Memory**.

- It is a special type of memory used in **switches** to **store MAC addresses** and their associated port numbers.
- When a switch receives a frame, it **looks up the destination MAC in the CAM table** to decide which port to forward the frame to.
- This enables **fast and efficient switching** by quickly mapping addresses to ports instead of broadcasting to all ports like a hub.

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.

- `192.168.1.0` is the **network address** when using a `/24` mask (`255.255.255.0`).
- In every subnet, **two addresses are reserved**:
  - `192.168.1.0` → **Network ID** (represents the whole subnet, not a device).
  - `192.168.1.255` → **Broadcast address** (used to send to all hosts).
- Routers, PCs, switches, printers... can only use **host addresses** (e.g. `192.168.1.1 - 192.168.1.254` in this subnet).

Routers cli commands :

Router > enable

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

🔹 **Case 1:** `192.168.1.0`

This one is usually seen with a `/24` mask (`255.255.255.0`).

- **Network address:** `192.168.1.0`
- **Broadcast address:** `192.168.1.255`
- **Usable host range:**

```
192.168.1.1 - 192.168.1.254
```

👉 So `192.168.1.0` is the **network ID**, not a usable host.

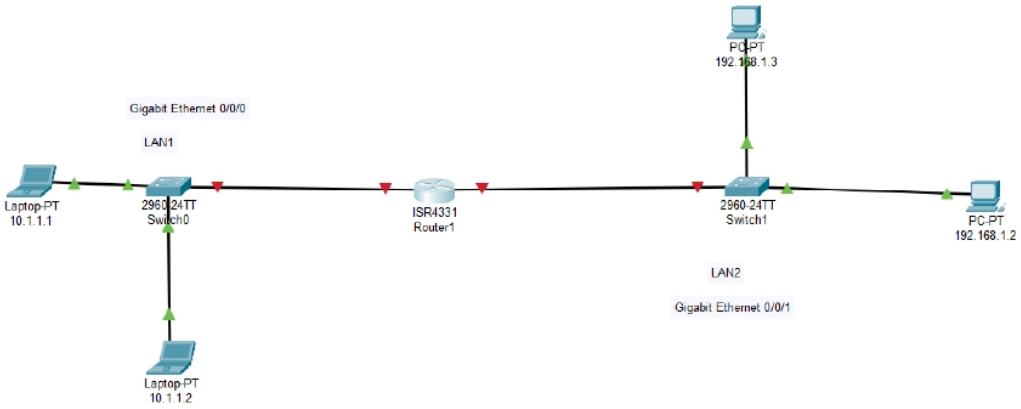
Case 2: 10.1.1.0 it is for /8 subnet mask not for /24

If `/24` (255.255.255.0)

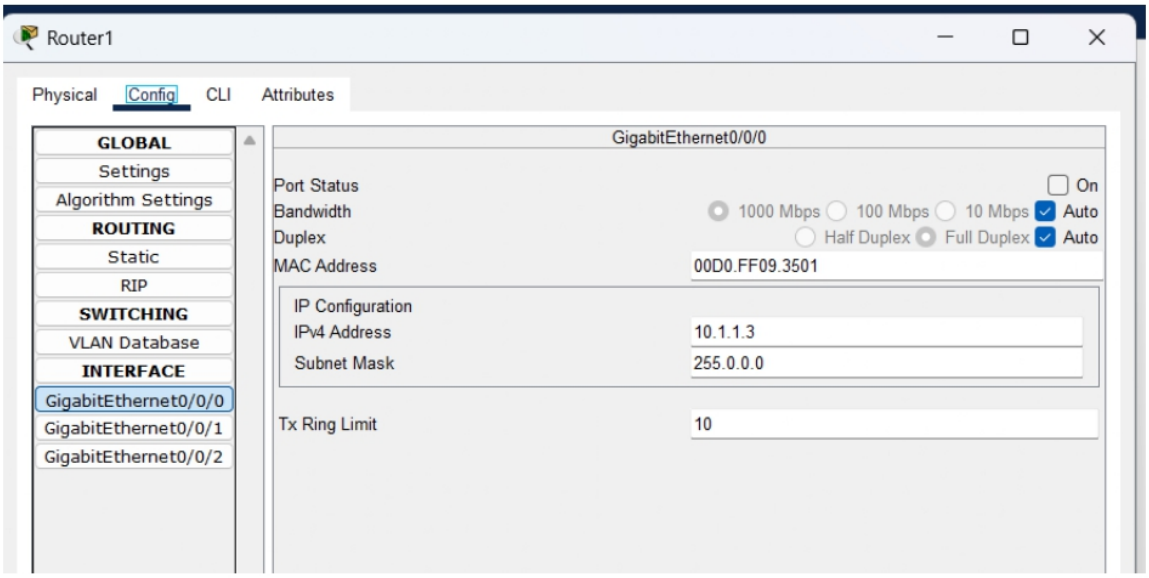
- **Network address:** `10.1.1.0`
- **Broadcast address:** `10.1.1.255`
- **Usable range:**

```
10.1.1.1 - 10.1.1.254
```

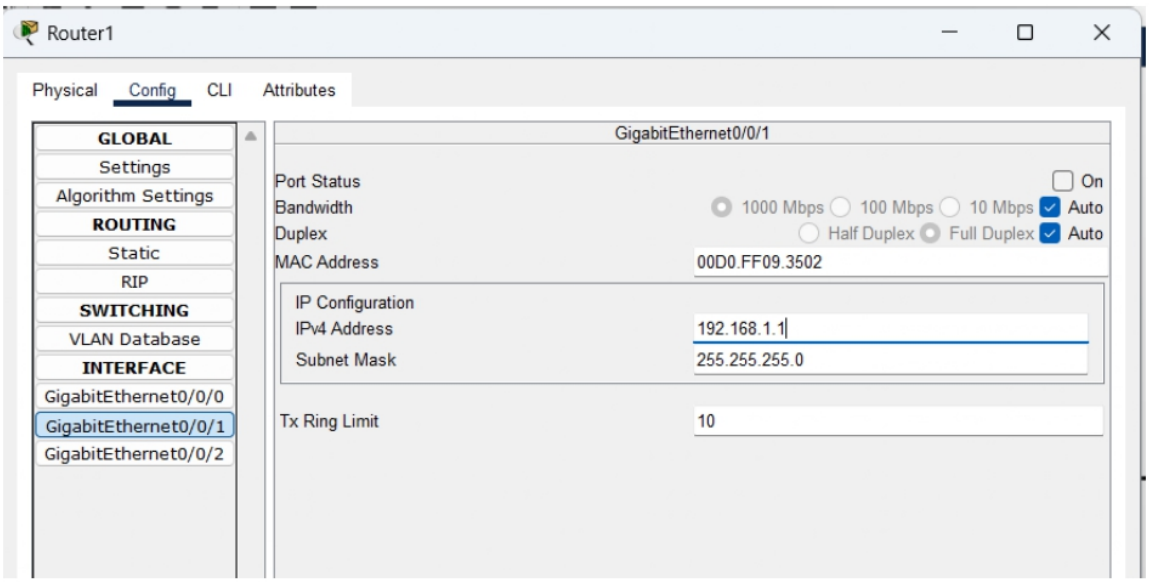
- Here, `10.1.1.1` is the **first usable host**. ✅

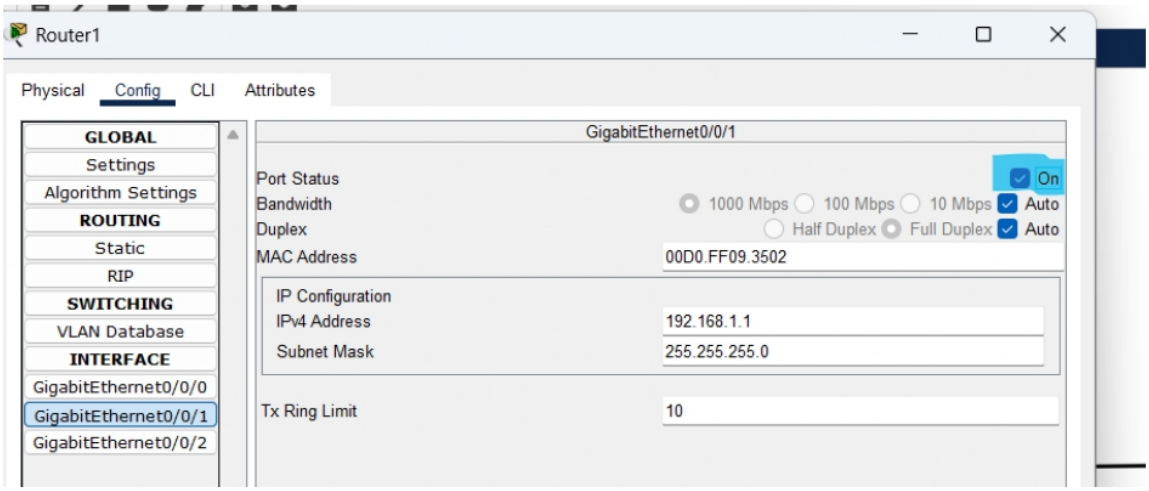


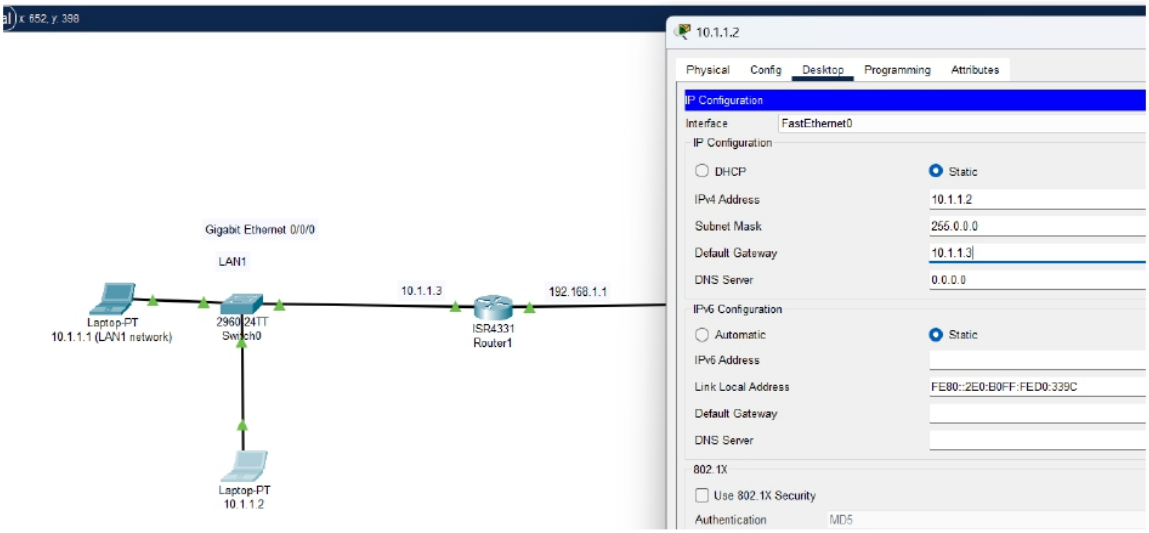
Configuring ip for LAN1 connection

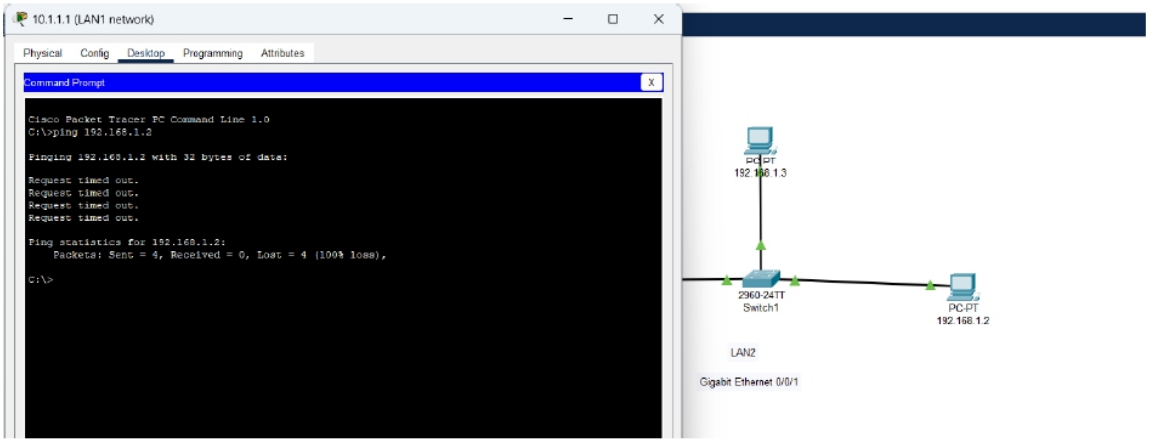


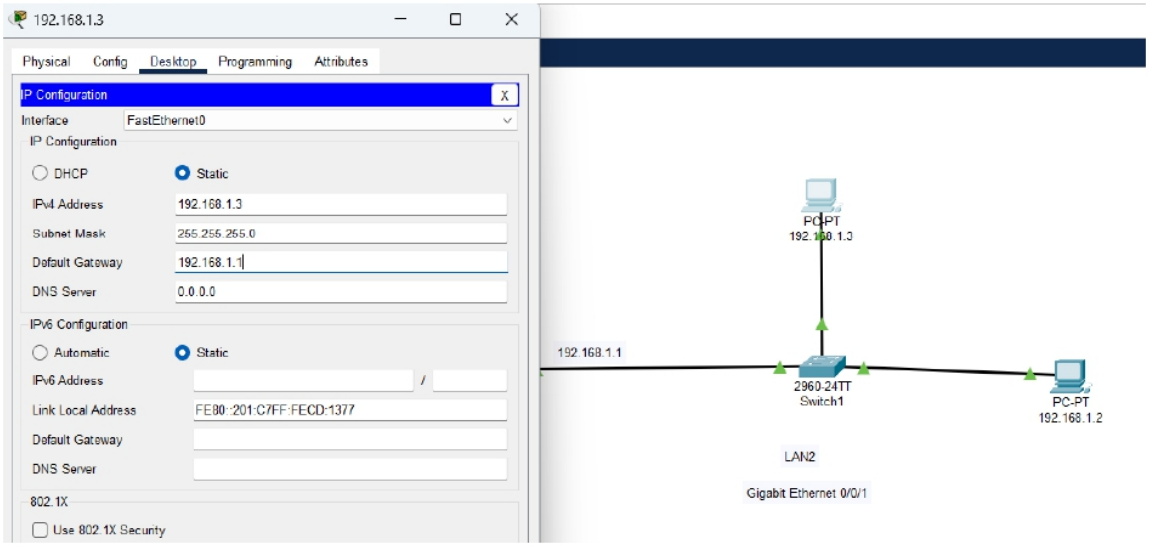
Configuring ip for LAN2 connection

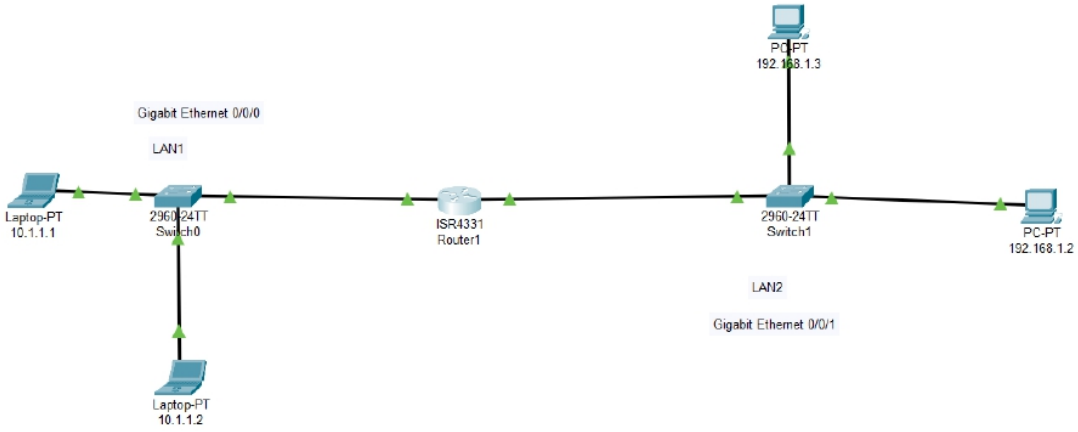


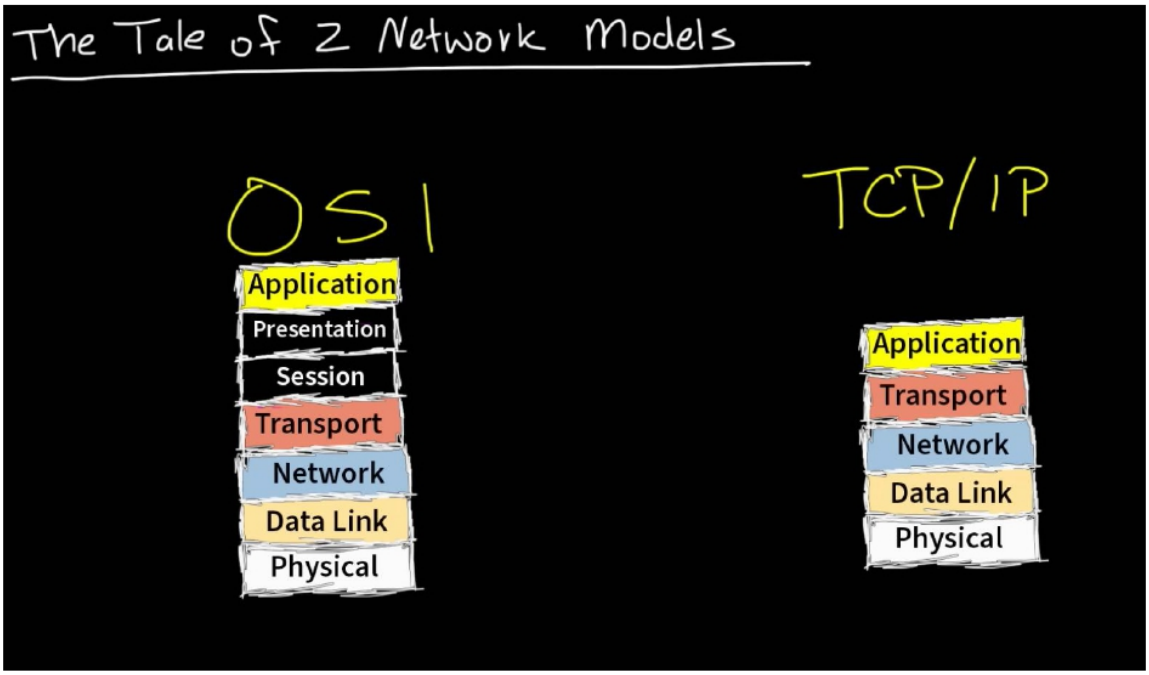

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.FF09.3502
IP Configuration
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Gigabit Ethernet 0/0/0
LAN1
10.1.1.3
192.168.1.1
Laptop-PT
10.1.1.1 (LAN1 network)
2960-24TT
Switch0
ISR4331
Router1
Laptop-PT
10.1.1.2
10.1.1.2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
10.1.1.2
Subnet Mask
255.0.0.0
Default Gateway
10.1.1.3
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2E0:B0FF:FED0:339C
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5


10.1.1.1 (LAN1 network)
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
192.168.1.3
2960-24TT
Switch1
PC-PT
192.168.1.2
LAN2
Gigabit Ethernet 0/0/1


192.168.1.3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::201:C7FF:FECD:1377
Default Gateway
DNS Server
802.1X
Use 802.1X Security
PC-PT
192.168.1.3
192.168.1.1
2960-24TT
Switch1
PC-PT
192.168.1.2
LAN2
Gigabit Ethernet 0/0/1


PC-PT
192.168.1.3
Gigabit Ethernet 0/0/0
LAN1
Laptop-PT
10.1.1.1
2960-24TT
Switch0
ISR4331
Router1
2960-24TT
Switch1
PC-PT
192.168.1.2
LAN2
Gigabit Ethernet 0/0/1
Laptop-PT
10.1.1.2


The Tale of 2 Network Models
OSI
Application
Presentation
Session
Transport
Network
Data Link
Physical
TCP/IP
Application
Transport
Network
Data Link
Physical

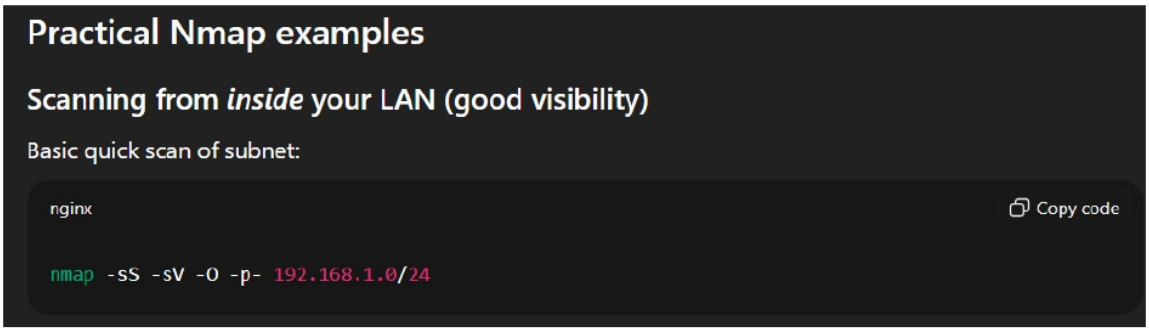
The **OSI model** is a seven-layer theoretical framework that describes how data moves across a network. Its layers are Physical, Data Link, Network, Transport, Session, Presentation, and Application. It is mainly used as a reference model to understand, design, and troubleshoot networks. It is a **theoretical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

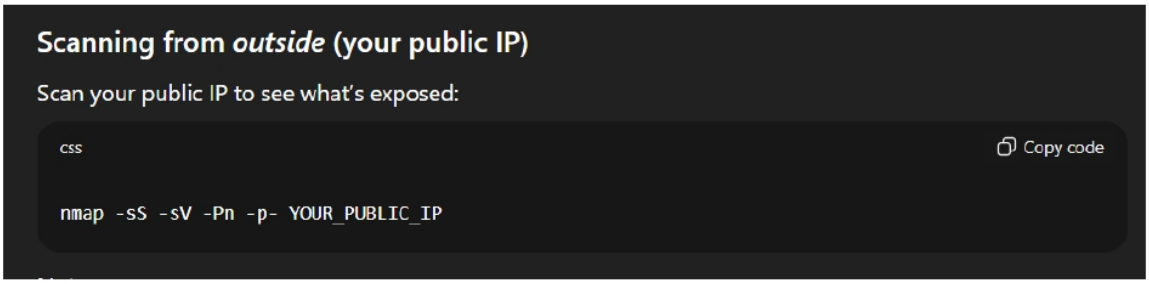
Nmap network scanning from outside of network :

nmap –script vuln <publicipof network>

nmap -sT <publicipofnetwork>

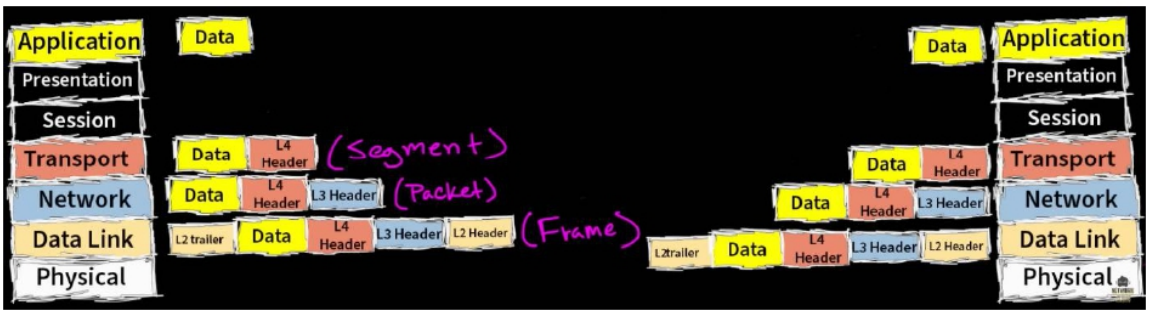


192.168.1.0 should be your private ip in home network !



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

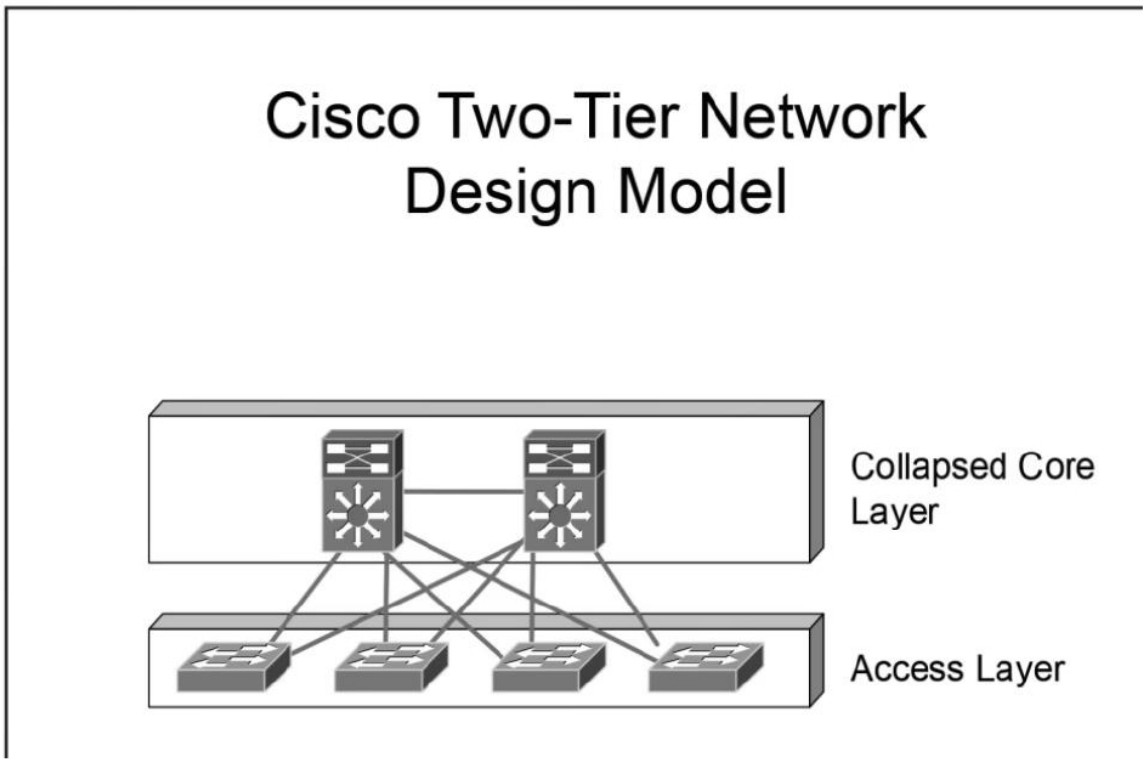
UDP = fast but not reliable

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.

Tier 2

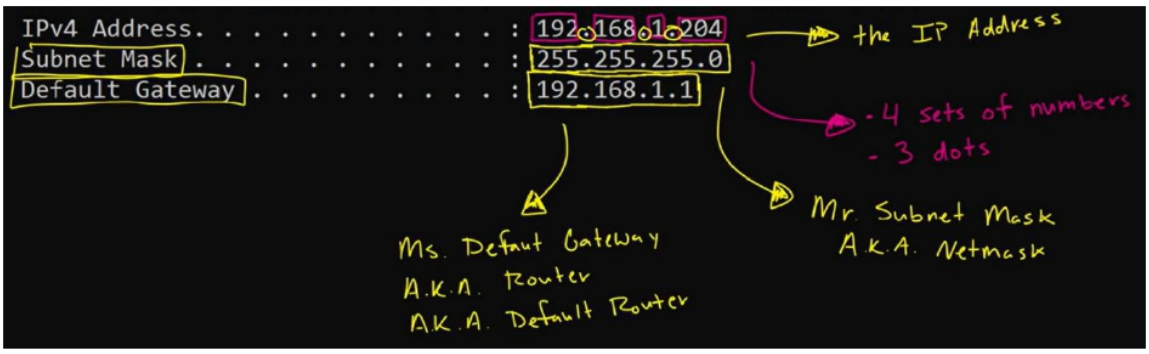


A **VLAN (Virtual Local Area Network)** is a **logical separation of a single physical network** into multiple virtual networks. Each VLAN behaves as if it were a separate LAN — its own broadcast domain — even though the same cables and switch hardware are used.

Note : Fiber optics cable uses light to transmit data.

What is an ip address ?

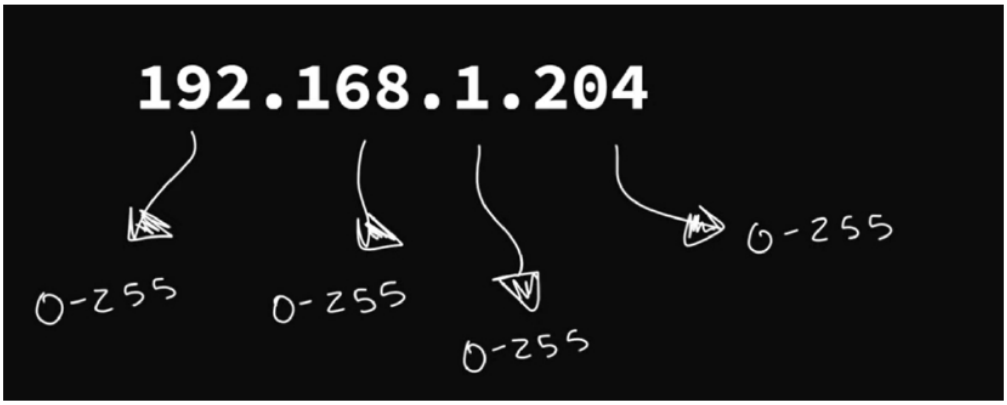
IP (Internet Protocol) is like name of the person or typical address of house. It allows a way to communicate between devices across the internet, basically why we need to know other's name or address just to call, or locate them , it's a basic presequite of communication right. It also opens up the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

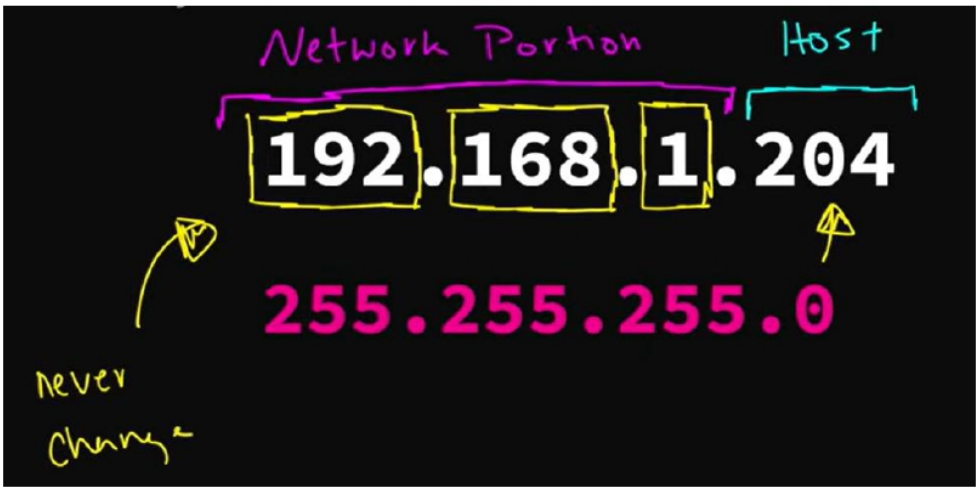


Just press win key + R and type cmd, and type command : ipconfig

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.

✅ **In short:**

> Router gives each device a private IP (via DHCP).
> When devices access the internet, the router uses **NAT** to share **one public IP** (from ISP) for all devices.

💡 **Inside your home (Private network)**

- Your **router** gives each device (phone, laptop, TV, etc.) a **private IP** like `192.168.1.2`, `192.168.1.3`, etc.
- These private IPs are **only used inside your home network** — they don't work on the internet.

This assigning process is called **DHCP (Dynamic Host Configuration Protocol)**.

🌍 **When a device goes online**

When your device (say your phone) opens a website:

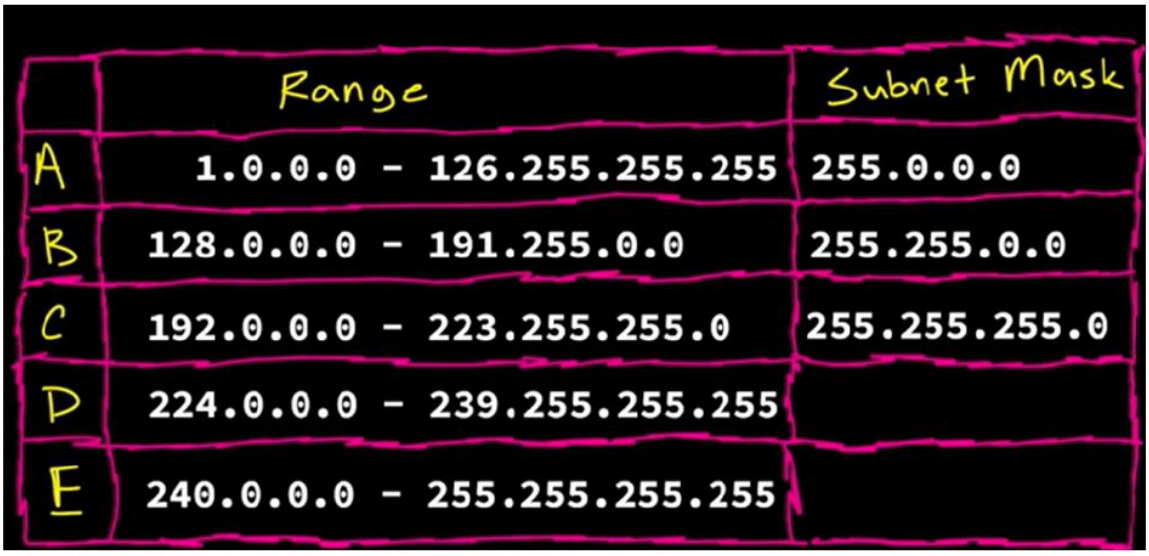
1. The request goes **first to the router**.
2. The router replaces your phone's **private IP** with its own **public IP** (the one given by your ISP).
3. The router keeps a small record of who asked for what — using a method called **NAT** (**Network Address Translation**).

🔁 **When the website replies**

- The reply comes back to the **router's public IP**.
- The router checks its NAT table and sends the reply to the **right private device** (e.g., your phone).

🌐 **Result:**

- Inside the home → devices have **different private IPs**
- Outside on the internet → they all appear to have the **same public IP** (the router's IP)



	Range	Subnet Mask
A	1.0.0.0 - 126.255.255.255	255.0.0.0
B	128.0.0.0 - 191.255.0.0	255.255.0.0
C	192.0.0.0 - 223.255.255.0	255.255.255.0
D	224.0.0.0 - 239.255.255.255	
E	240.0.0.0 - 255.255.255.255	

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

	Private	
A	10.0.0.0 - 10.255.255.255	255.0.0.0
B	172.16.0.0 - 172.31.255.255	255.255.0.0
C	192.168.0.0 - 192.168.255.255	255.255.255.0

🌐 1. Private IP — your local identity

When you connect your phone or laptop to Wi-Fi, your **router gives you a private IP**.
Examples:

- `192.168.x.x`
- `10.x.x.x`
- `172.16.x.x – 172.31.x.x`

These ranges are **reserved** for private use — they **don't exist on the internet**.

So if two people in different homes both have `192.168.1.5`, it's fine —
because these private IPs live only **inside their local networks** and never mix.

📶 2. Router — your local "traffic manager"

The **router** sits between your **local network** (LAN) and the **outside world** (WAN/Internet).

It does two big jobs:

1. **Assigns private IPs** to all your devices using **DHCP**.
2. **Translates** between private and public IPs using **NAT**.

🌍 3. Public IP — your home's address on the internet

Your **ISP (Internet Service Provider)** gives your **router one public IP address** — something like `103.92.45.12`.

This is how the entire internet sees your home network.
So even though your phone, laptop, and TV all browse different sites,
to the internet they all look like **one device** — your router.

- **Private IPs** aren't unique globally; every home can reuse them.
  So there's **no danger** if someone sees `192.168.1.5`.
  It means nothing outside your home.
- But your **public IP** is **unique** on the internet —
  it can reveal your **approximate location**, **ISP name**, and can be used for tracking or attacks.
  That's why **VPNs** and **proxies** exist — they **hide your public IP** and show another one instead.

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

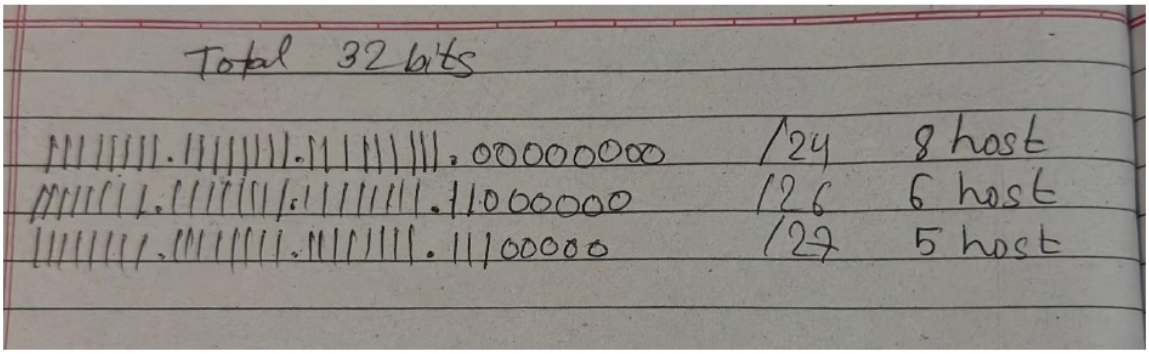
1 : network bits

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

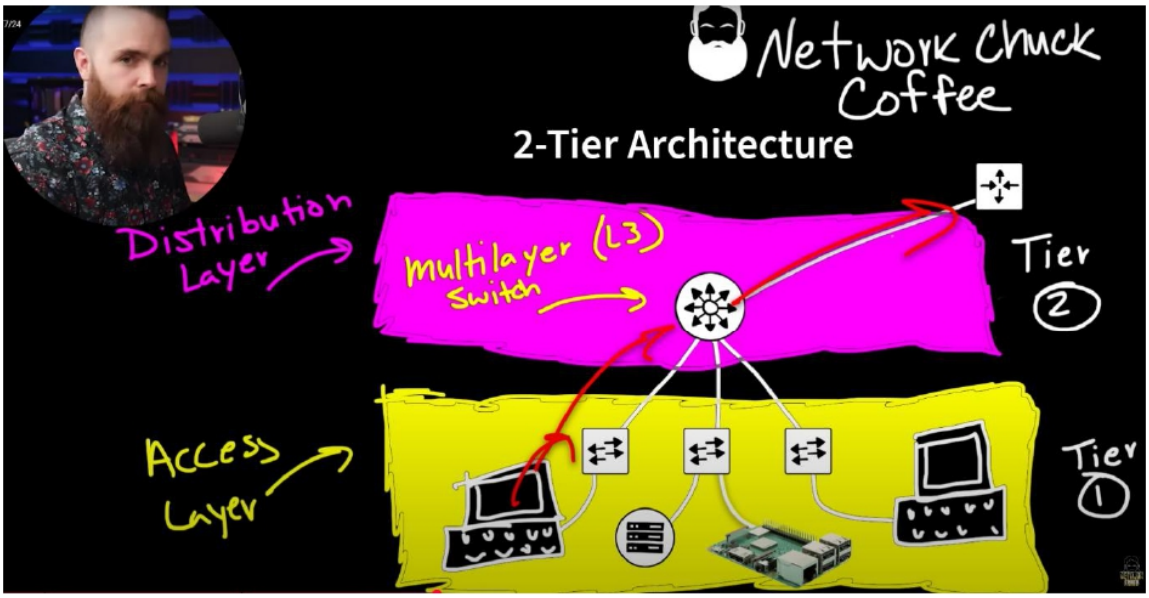


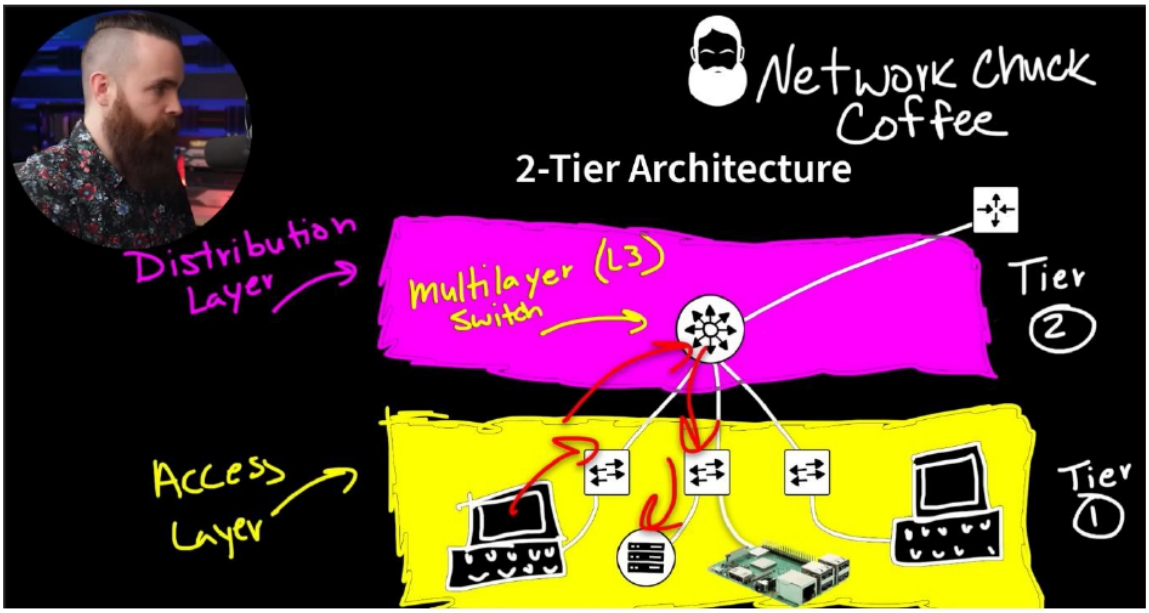
- Ports are numbered from **0 to 65535** (16-bit number).

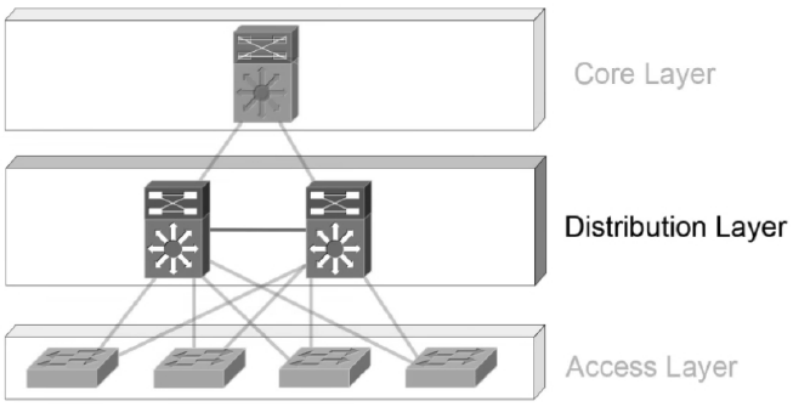
Port Range	Type	Description
0–1023	*Well-known ports*	Used by common protocols (HTTP, FTP, SSH, etc.)
1024–49151	*Registered ports*	Assigned to specific services by companies or developers
49152–65535	*Dynamic / Private ports*	Used temporarily by client devices for connections

Service	Protocol	Port
HTTP (Web)	TCP	80
HTTPS (Secure Web)	TCP	443
FTP (File Transfer)	TCP	21
SSH (Secure Shell)	TCP	22
DNS (Domain Name System)	UDP	53
SMTP (Email sending)	TCP	25

DHCP	UDP	**67 (server), 68 (client)**	Dynamic Host Configuration Protocol — automatically assigns IP addresses to devices.
TFTP	UDP	**69**	Trivial File Transfer Protocol — lightweight version of FTP, used for booting network devices or transferring small config files.


Network Chuck Coffee
2-Tier Architecture
Distribution Layer
multilayer (L3) Switch
Tier 2
Access Layer
Tier 1


Network Chuck Coffee
2-Tier Architecture
Distribution Layer
multilayer (L3) Switch
Tier 2
Access Layer
Tier 1


Core Layer
Distribution Layer
Access Layer

Tier 3