Networking Protocols and IP Addressing: A Comprehensive Guide

1. Protocol in Networking

1.1. Network Protocol

Total ports : 65,535
Protocols are the set of rules that define how data is transmitted over a network. Protocols ensure successful communication between devices.

1.1.1. TCP/IP model

- **Application Layer**
  - **Protocols:** Telnet, SMTP, POP3, FTP, NTP, HTTP, SNMP, DNS, SSH and many more
  - **Function**: Provides protocols for applications to interact with the network.

- **Transport Layer**
  - TCP, UDP (Both are considered core communication protocols)
  - **Function**: Handles end-to-end communication, reliability, and flow control.

- **Internet Layer**
  - IP,ICMP, ARP, DHCP
  - **Function:** Handles addressing, routing, and packet forwarding.

- **Network Access Laye**r
  - Ethernet, PPP, ADSL
  - **Function**: Manages physical addressing and access to the media.

1.2. Type of protocol

- **TCP (Transmission Control Protocol):**
  - Reliable, connection-oriented protocol that ensures data is delivered in order and without errors.
- **UDP (User Datagram Protocol):**
  - Unreliable, connectionless protocol used for applications where speed is critical, and loss of data is acceptable.

1.3. How Tcp works

6 FLAGS

- **URG (urgent):** Data contained in the packet should be processed immediately.
- **FIN (finish):** when data is transmitted then to disconnect connection fin is used
- **RST (REST)** : Resets the connection.
- **PSH (PUSH)** : send all buffered data immediately
- **ACK (Acknowledgement)** : Acknowledges the receipt of a packet
- **SYN (Synchronize)** : Initiates a connection between hosts. First flag

Tcp - Follow 3 way handshake SYN(send), SYN+ACK(received), ACK(send)

- SYN: Initiates the connection.
- SYN+ACK: Acknowledges the SYN and signals readiness to establish a connection.
- ACK: Confirms the connection is established.

1.4. Tcp vs UDP

1.4.1 TCP

- Stands for Transmission Control Protocol ,
- Follow 3 way handshake SYN(send), SYN+ACK(received), ACK(send),
- Slow than UDP during data transmission,
- Most reliable in term of data safety and security due its way handshake feature,
- Used in applications where data integrity is critical (e.g., HTTP, FTP).

1.4.2. UDP

- Stands for User Datagram Protocol,
- It request data and male response on it it does not perform any handshake to establish connection,
- Fast than TCP,
- Not reliable in term of data safety and security,
- Used in real-time applications where speed is essential (e.g., VoIP, streaming).

2. IP address

2.1 Introduction

IP stands for Internet Protocol Address which define each device with unique identifier that are connected
Range: 0-255

Eg: 192.168.10.11
Total 32 bits ie. equal to 4 bytes (32 bits=4 bytes) each pair of 8 bits
1st pair define country,
2nd pair define state,
3rd pair defines city and ISP name,
4th pair defines all details of the device.

2.2 IPv4 vs IPv6

2.2.1. IPv4

- **Address size**: 32 bit number
- **Address Format**: Dotted Decimal Notation eg:192.168.10.10
- **Number of address**: 2^32 addresses

2.2.2. IPv6

Updated version of IPv6

- **Address size**: 128 bit number
- **Address Format:** HexaDecimal Notation (0-9 and a-f)
- **Number of address**: 2^128 addresses

2.3. Type of Ip address

Public IP (Like real name of person)

- Used in WAN,

Private IP (Like nick-name of person)

- Used in Local area Network (LAN),

- To interact to each other both ip should have same type like Public to Public IP and Private to Private IP,

- But the private ip range should also need to be the same because it is used in LAN only but public IP can.

Static IP

- Manually assigned, remains constant.

Dynamic IP

- Automatically assigned by DHCP, may change over time.

2.4. IP and subnet masking

IP Address: 192.168.10.10/24

- **CIDR Notation (/24):**
  - The **/24** indicates that the first 24 bits of the IP address are the network portion ie. 1 , and the remaining bits (8 bits in this case) are used for host addresses within that network.
- **Subnet Mask:**
  - The **/24 refers to 24*1**'s which defines the network portion of the IP address in binary value i.e: **11111111.11111.1111111.00000000** and its decimal conversion is **255.255.255.0** which is a subnet masking of that IP.

2.5. Subnetting and host calculation

2.5.1. Network Portion:

- The first CIDR(/24) bits refers to the network.

2.5.2.Host Portion:

- The last 0 bits are used to identify individual hosts within a network.

2.5.3. Calculation

- **2^(total nbr of zero) - 2** (**'-2'** for the 2 reserved IP i.e network address and broadcast addresses)
- **Network Address** (all zeros): Used to identify the network itself i.e 192.168.10.0
- **Broadcast Address** (all ones): Used to send data to all hosts in the network i.e 192.168.10.255.
- So, **Total usable host IPs = 2^(nbr of zeros in subnet mask) - 2**

= 2^8 - 2
= 254 usable IP addresses for host

Therefore, **IP Address: 192.168.10.10/24**
Subnet Mask: 255.255.255.0
Number of Usable Hosts: 254
Host Range: 192.168.10.1 to 192.168.10.254

3. DNS

3.1. Function:

Translates domain names (e.g., www.google.com) into IP addresses (e.g., 8.8.8.8).

1. Domain Name system
2. Address Book of Internet
3. Translate Domain to IP
4. Store all data in form of record in zone file

4. Working of Router

4.1. How Routers Function in IP Networks?

An ISP reserves a range of public IP addresses for communication within the WAN. It then allocates one of these reserved public IP addresses to a customer's router. The router, in turn, manages a range of reserved private IP addresses, which it assigns to devices connected to the local network. The router itself has a unique MAC address, which is used for network communication at the hardware level.

IP address allocation can be done either manually or automatically.

- In the manual method, a private IP address is assigned to a device by configuring it directly on the device.
- For automatic IP address allocation, the router typically uses the Dynamic Host Configuration Protocol (DHCP) server feature. The DHCP server automatically assigns IP addresses to devices on the network, ensuring that each device receives a unique IP address without manual intervention, and it also manages IP address leasing, which can help prevent conflicts.

Public IP Allocation:

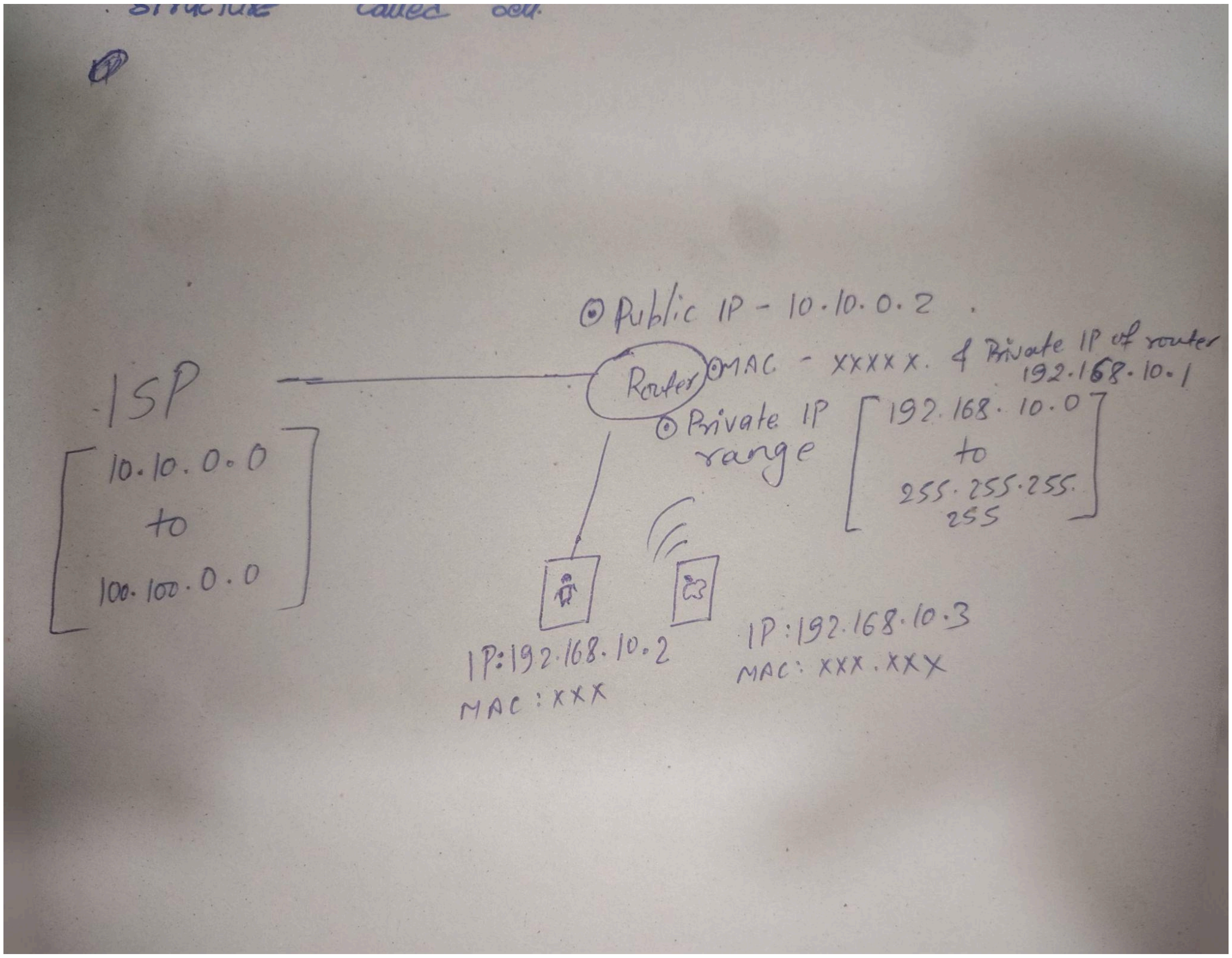
- ISPs allocate public IP addresses to customers' routers.

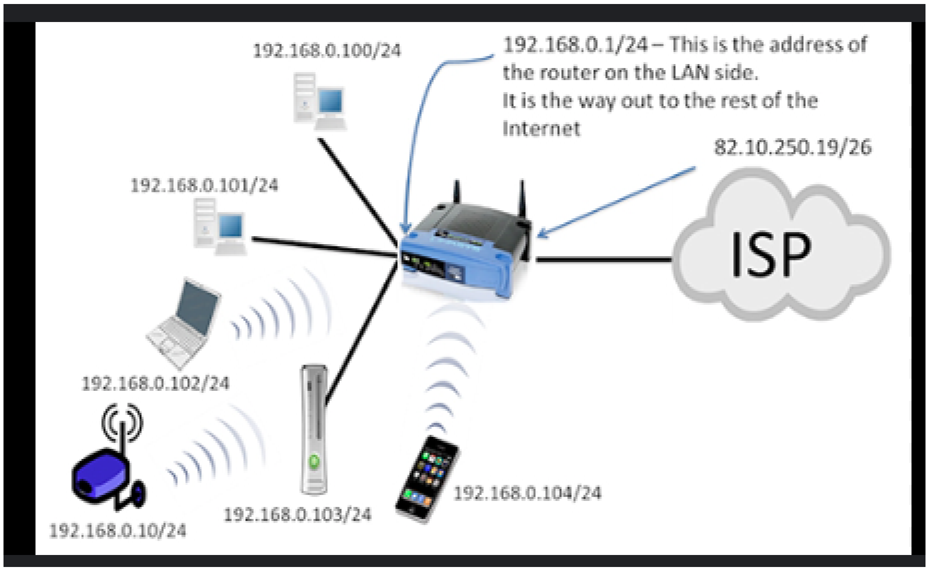
Private IP Allocation:

- Routers assign private IPs to devices within the LAN, typically using DHCP.

Routing:

- Routers manage the flow of data between networks, using IP addresses and MAC addresses for communication.




192.168.0.1/24 – This is the address of the router on the LAN side.
It is the way out to the rest of the Internet

5. OSI & TCP/IP models

5.1. OSI model (Open Systems Interconnection)

- Conceptual model with seven layers,
- 7 layer
  - Application layer
  - Presentation layer
  - Session layer
  - Transport layer
  - Network layer
  - Data link layer
  - Physical layer

5.2. TCP/IP layer model (Transmission Control Protocol/Internet Protocol)

- Improved form of OSI model,
- Practical model with four layers,
- 4 layer model
  - Application layer
  - Transport layer
  - Internet layer
  - Network Access layer

5.3. OSI vs TCP/IP

Layer	OSI Model	Tcp/IP model	Protocol
Application	Application (Layer 7)	Application	HTTP, FTP, SMTP, and DNS
	Presentation (Layer 6)		
	Session (Layer 5)		
Transport	Transport (Layer 4)	Transport	TCP, UDP
Network	Network (Layer 3)	Internet	IP, ICMP, ARP
Datalink	Data link (Layer 2)	Network Access	

Physical	Physical (Layer 1)		

Kali

Make sure to upgrade and update apt

- Command: **sudo apt update && sudo apt upgrade**

Installing file

- Download with apt
    - Command: **sudo su**
        - **apt install <file _name>**

- Download with official website
    - Command: **sudo su**
        - Download with it from it's official website the downloaded file is in .deb prefix and open it's file path on terminal and use command;
        - **ls**
        - **dpkg -i <file_name.deb>**
        - **dpkg**

- Download wit github or any third party site
    - Copy the github link of file and use command:
        - **Git clone <github-link>**