Networking Basics

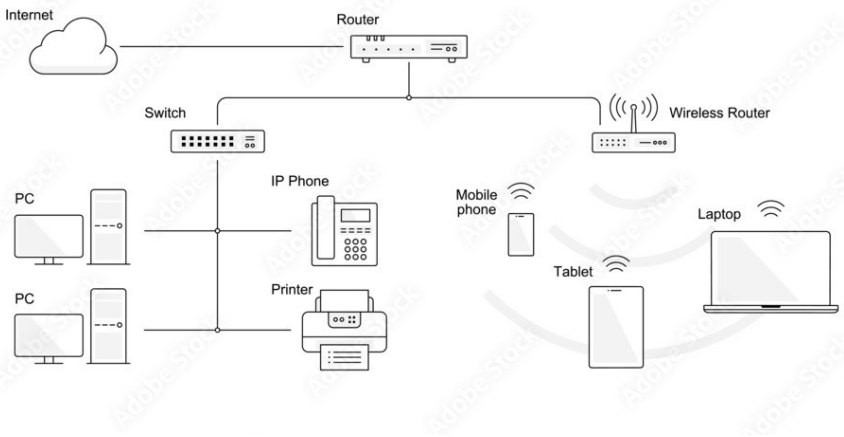
1.Introduction to networking

- What is a network? - network is a collection of interconnected devices that share resources and information.

1.1 Network components

- Consists of Nodes & Links
    - Node: Any device that can send, receive, or forward data in a network. This includes laptops, mobiles, printers, earbuds, servers, etc.
    - Links: wires or cables or free space of wireless networks
    - Transmission Media: The physical or wireless medium through which data travels between devices.(Wired media: Ethernet cables, optical fiber.), (Wireless media: Wi-Fi, Bluetooth, infrared)
    - Networking Devices - Devices that manage and support networking functions. This includes routers, switches, hubs, and access points.
        - Access points - connects wireless devices to wired network
        - Switch - multiport bridge with a buffer designed that can boost its efficiency (a large number of ports imply less traffic) and performance. Performs error checking before forwarding.
        - Router - a device like a switch that routes data packets based on their IP addresses.connects LAN to WAN. Desicions based on routing table.
        - Controller
        - Gateway - a passage to connect two networks/ entry point of networks
        - NIC- used to connect the computer to the network.
        - Repeater - to amplify (i.e., regenerate) the signal over the same network before the signal becomes too weak or corrupted
        - Hub- a multiport repeater. Broadcast data to all ports.

        - Bridge - a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination.
        - Modem,Proxy server,Firewall
    - Service Provider Networks: Networks offered by external providers that allow users or organizations to lease network access and capabilities. This includes internet providers, mobile carriers, etc.



2 .Types of networks

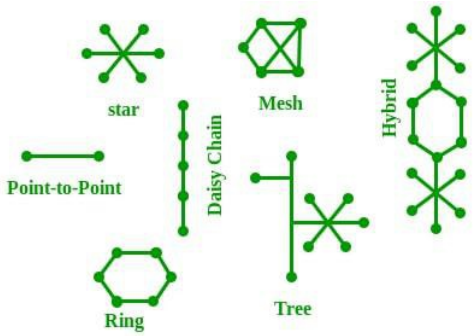
- **LAN**
- **WAN**

3. Types of network architecture

- client – server, P2P (peer - peer)
- **Client-Server Network**:
    - In a client-server network, devices are divided into **clients** and **servers**. The **server** is a central system that provides resources or services (like files, printers, or websites) to the clients, which request these resources.

    - **Advantages**: Centralized control and management, Scalability, Better security and data consistency
    - **Disadvantages**: Requires specialized server hardware and software, If the server goes down, all clients are impacted.
- **Peer-to-Peer (P2P) Network**:
    - In a P2P network, each device (or "peer") is both a client and a server. Peers can share resources (files, printers) directly with each other without relying on a central server.
    - **Advantages**: Lower cost and simpler setup, more resilient
    - **Disadvantages**: Less control over data security and consistency,Harder to manage as the number of peers grows.

4. Network Topologies



Network topology refers to the physical or logical layout of how devices and components are connected in a network. The topology defines the structure and flow of data within the network. It influences the network's performance, scalability, reliability, and cost.

Common Types of Network Topologies:

1. **Bus Topology**: All devices are connected to a single central cable (the bus). It's simple but prone to network failure if the bus cable is damaged.
2. **Ring Topology**: Devices are connected in a circular fashion. Data travels in one direction around the ring, passing through each device. It's efficient but can be vulnerable if one device or connection fails.
3. **Star Topology**: Devices are connected to a central hub or switch. This is the most common and reliable topology, as a failure in one device does not affect the others.
4. **Mesh Topology**: Every device is connected to every other device. This offers high redundancy and reliability but is complex and expensive to implement.

5. **Tree Topology**: A hybrid topology combining characteristics of bus and star topologies, often used in large networks.

5. Network Models

- **OSI Model – Open System Interconnection**
- It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.
- 7-layer architecture

Layer	Name	Function	Protocols	Devices
1	Physical	• Encoding/decoding • Modulation/demodulation • Transmission mode •	Ethernet Wi-fi Bluetooth Usb	
2	Data Link	• Framing • Error detection • Error Correction • Flow control • Addressing		
3	Network	• Assigning Logical address • Packetizing • Host to host delivery • Forwarding • Fragmentation & reassembly • NAT • Routing	IP ICMP ARP NAT	
4	Transport	• End to End communication • Flow control • Multiplex/demultiplex • Conncetion establishment & termination • Reliable data delivery • QoS •	TCP UDP	
5	Session	• Session establishment • Communication synchronization • Activity management • Dialog Management	SSL TLS JPEG UTF-8	

		• Data transfer • Resynchronisation		
6	Presentation	• Data Translation • Data Compression • Data encryption/decryption • Syntax & semantics • Interoperability		
7	Application	• Data representation • Network service Access • Application protocols • Session Management	HTTP DNS TELNET DHCP FTP SMTP NFS SNMP	

- **TCP/IP Stack**

- practical, real-world implementation used to facilitate communication between networked devices.

- IP (for addressing), TCP/UDP (for transport), HTTP/FTP/DNS/DHCP (for application)

TCP/IP Model	OSI Model	Explanation	
Network Access/Link	Data Link + Physical	Handles hardware addressing, framing, and transmission over physical media	
Internet	Network	Responsible for logical addressing and routing	
Transport	Transport	Same purpose; uses TCP and UDP for reliable/unreliable transport	
Application	Session + Presentation + Application	Combines OSI's top three layers; includes protocols like HTTP, DNS, FTP	

6. **6.IP Addressing**

- IP address - Unique identifier address of devices in a computer network
- Notation – binary/decimal/hexadecimal
- 2 parts – network id & host id

6.1 versions of IP addresses:

- IPv4 and IPv6
- pros/cons

IPv4	IPv6
32 bits ip addr	128 bits ip addr
4 sections of 8 bits each	8 sections of 16 bits each
Dotted decimal notation	Dotted hexadecimal notation
Uses subnet mask component (32 bits) to identify n/w & host addr	Fixed bits for n/w & host addr --> 64 bits each.
IP addr: 192.168.1.10 Subnet mask: 255.255.255.0	`2001:0000:0db8:85a3:0000:8a2c:3233:3312`

IPv6 (Internet Protocol version 6) and **IPv4 (Internet Protocol version 4)** are two different versions of the Internet Protocol used for addressing devices in a network.

IPv4 Addressing:

- **Format**: IPv4 addresses are 32-bit numbers, typically represented in **dotted-decimal format** (e.g., 192.168.1.1).
- **Address Space**: IPv4 provides approximately **4.3 billion unique addresses**, which is no longer sufficient due to the growing number of internet-connected devices.
- **Address Classes**: IPv4 addresses are divided into classes (A, B, C, D, and E), and the addressing scheme supports both private and public addresses.

IPv6 Addressing:

- **Format**: IPv6 addresses are 128-bit numbers, typically represented in **hexadecimal format** (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- **Address Space**: IPv6 provides a vastly larger address space, offering about **340 undecillion (3.4 × 10^38)** unique addresses, ensuring that every device on the planet (and beyond) can have a unique address.
- **No Need for NAT**: Because of the vast address space, IPv6 does not require **NAT (Network Address Translation)**, unlike IPv4.
- **Simpler Header**: IPv6 has a simplified header structure that improves processing efficiency.

Key Difference:

IPv4 uses 32-bit addresses, while **IPv6** uses 128-bit addresses, providing a significantly larger address space and additional features like built-in security and simplified routing.

6.2 Subnet mask

- Distinguish n/w addr from host addr
- 32 bit
- Dotted decimal, binary or /n notation
- Sets bit at each network bit position, resets host bits

IP addr: 192.168.1.10

Subnet mask: 255.255.255.0

192.168.1.0/24 -->

n/w addr – 192.168.1.0

Bc addr – 192.168.1.255

Available host address – 254

192.168.1.1 to 192.168.1.254

6.3 Subnetting

- Large IP n/w to smaller independent networks with a range of IP addrs
- IP addrs clacsses – class A,B,C,D (Multicast),E (Reserved) based on no:of bits for network id.

	8 bits	8 bits	8 bits	8 bits
Class A	n/w	host	host	host
Class B	n/w	n/w	host	host
Class C	n/w	n/w	n/w	host

- 1st addr – n/w addr, last addr – broadcast addr
    - 192.168.0.0/24 network to 3 subnets with 50,30,20 hosts

hosts	Add + 2	Nearest ^2	Subnet mask	Subnet allocation	VLAN alloc
50	52	64 (2^6)	/26 (255.255.255. 192)	sn1– 192.168.0.0/26 Host – 192.168.0.1 to 192.168.0.62 Bc – 192.168.0.63	VLAN 1 IP 192.168.0.0/26
30	32	32 (2^5)	/27 (255.255.255. 224)	sn1– 192.168.0.64/27 Host – 192.168.0.65 to 192.168.0.94 Bc – 192.168.0.95	VLAN 2 IP 192.168.0.64/27
20	22	32 (2^5)	/27 (255.255.255. 224)	sn1– 192.168.0.96/27 Host – 192.168.0.97 to 192.168.0.126 Bc – 192.168.0.127	VLAN 3 IP 192.168.0.96/27

6.4 Static/ Dynamic IP addressing

6.5 Public/private ip address

- Public IP addresses are globally unique IP addresses assigned to devices that need to be directly accessible over the internet. They are routable on the global internet and are issued by Internet Service Providers (ISPs) or assigned by the Internet Assigned Numbers Authority (IANA). Public IPs are typically used by servers, websites, and other services that need to be accessed by users anywhere on the internet.

- Private IP addresses, on the other hand, are used within private local area networks (LANs). These IP addresses are not routable over the internet, meaning that devices using private IPs cannot be accessed directly from the internet. Instead, private IP addresses are designed for use within an organization's internal network. The specific ranges for private IP addresses are defined by RFC 1918:
- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255
- Private IP addresses are used by devices like computers, printers, and smartphones in local networks. These devices can access the internet through Network Address Translation (NAT), which allows them to share a single public IP address to connect to the internet. This helps conserve global IP address space and improves security by preventing direct access to private devices from outside the local network.

- Nb: Mac address, Logical/physical address

7.Protocols

7.1 DNS

- The **Domain Name System (DNS)** is essentially the **phonebook** of the internet, translating human-readable domain names (like **www.example.com**) into machine-readable IP addresses (like **192.168.1.1**). Since humans find it easier to remember names than numeric IP addresses, DNS helps in this translation to ensure that when you type a website URL into your browser, the correct IP address is located to establish the connection.
- How DNS Works:
- When you type a URL into your browser, a **DNS query** is initiated to find the corresponding IP address.
- The query is first sent to a **DNS resolver** (usually provided by your ISP or a public DNS service like Google DNS or Cloudflare).
- If the resolver doesn't have the IP address cached, it queries other DNS servers, starting with the **root DNS servers**, which then point to the **TLD (Top-Level**

Domain) servers (e.g., .com, .org), and finally to the **Authoritative DNS servers**, which return the actual IP address.
- Once the IP address is found, your device connects to the web server at that IP address.

7.2 DHCP

- **DHCP** is a **network management protocol** used on **IP networks** to automatically assign **IP addresses**, **subnet masks**, **default gateways**, and other network configuration settings to devices on a network. This process significantly reduces the need for manual IP address assignment, making network management more efficient and error-free.

- How DHCP Works:

- **Discovery**: When a device (e.g., a computer or smartphone) joins a network, it sends a **DHCP Discover** message to find available DHCP servers.
- **Offer**: The DHCP server responds with a **DHCP Offer**, which includes an available IP address and configuration settings.
- **Request**: The device then sends a **DHCP Request** message to the server to confirm the offer.
- **Acknowledgment**: Finally, the DHCP server sends a **DHCP Acknowledgment**, and the device is assigned the IP address and network settings.
    - Key Benefits:

- **Automatic IP Assignment**: Devices don't need to be manually configured with an IP address, reducing errors.
- **Efficient Management**: DHCP servers can manage IP address pools, ensuring addresses are not duplicated.
- **Lease Time**: IP addresses are leased for a specific duration and are returned to the pool when no longer in use.
    - In summary, DHCP simplifies network configuration by automatically assigning IP addresses and other parameters to devices as they connect to the network.

7.3 TCP / UDP

- TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two core transport layer protocols in the TCP/IP stack, but they have distinct characteristics and use cases.
- TCP is a connection-oriented protocol, meaning that a reliable connection must be established between the sender and receiver before any data is transmitted. It ensures that data is transmitted correctly and in the right order, and it retransmits any lost packets. It also provides flow control to prevent network congestion and error-checking to ensure data integrity. Because of these features, TCP is typically used in applications where reliability is paramount, such as:

- Web browsing (HTTP/HTTPS)
- Email (SMTP, IMAP)
- File transfer (FTP)
- Key features of TCP:

- Reliability: Ensures all data is delivered.
- Error Checking: Detects and retransmits lost or corrupted packets.
- Flow Control: Manages the rate of data transfer.
- Ordered Delivery: Ensures data arrives in the correct sequence.
- UDP is a connectionless protocol, meaning it doesn’t establish a connection before data is sent, and it doesn't ensure data reliability or ordering. It simply sends data packets to the receiver without waiting for acknowledgment, making it faster but less reliable. UDP is typically used in applications where speed is more important than reliability, such as:

- Streaming media (video/audio)
- Online gaming
- Voice over IP (VoIP)
- DNS queries

- Key features of UDP:

- Faster transmission: No overhead for establishing a connection or error checking.
- No reliability: Packets may be lost or delivered out of order.
- Low latency: Ideal for real-time applications where delays need to be minimized.
- In summary, TCP is used when data integrity and reliability are essential, while UDP is used for applications that prioritize speed and can tolerate some data loss.

The **handshake process** differs significantly between **TCP (Transmission Control Protocol)** and **UDP (User Datagram Protocol)** due to the inherent characteristics of these two protocols.

TCP Handshake (Three-Way Handshake):

- **Purpose**: Establishes a reliable, connection-oriented communication channel.
- **Process**: TCP uses a **three-way handshake** to synchronize sequence numbers and establish a reliable connection before data transfer.
- **Reliability**: Guarantees the delivery of data, checks for lost packets, and ensures the data arrives in order. If any packet is lost, it will be retransmitted.
- **Flow Control**: TCP uses mechanisms like **flow control** and **congestion control** to manage data transfer.

UDP Handshake:

- **Purpose**: UDP is a **connectionless** protocol, meaning it does not require a handshake or connection establishment before sending data.
- **Process**: With UDP, the sender simply sends packets (datagrams) to the destination without first establishing a connection.
- **Reliability**: UDP does not provide any guarantee of delivery, order, or error correction. It is faster but less reliable than TCP.
- **Flow Control**: UDP does not have flow control or congestion control mechanisms.

Key Difference:

- **TCP** requires a handshake to establish a reliable connection, while **UDP** is connectionless and does not use a handshake process.

7.4 ARP

ARP (Address Resolution Protocol) is used to map an IP address to a corresponding MAC address in a local area network (LAN). This allows devices on the same network to communicate directly using MAC addresses, which are necessary for the data link layer (Layer 2) communication.

ARP Process:

1. **ARP Request**: When a device wants to communicate with another device on the same network and knows the IP address but not the MAC address, it sends an **ARP request** to the network. This is a broadcast message sent to all devices on the local network asking, "Who has this IP address?"
2. **ARP Reply**: The device with the matching IP address responds with an **ARP reply** containing its MAC address. The reply is sent directly to the requesting device.
3. **Caching**: The requesting device stores the IP-MAC mapping in its **ARP cache** for future use, so it doesn't need to repeat the ARP process every time it communicates with that device.
4. **Communication**: Once the MAC address is known, the device can send data frames directly to the destination device using the MAC address.

ARP Cache: A table that stores IP-to-MAC address mappings for a specified period. It helps avoid sending ARP requests repeatedly.

7.5 NAT

- **Network Address Translation (NAT)** is a technique used to translate private IP addresses into public IP addresses and vice versa. It is commonly used in home and corporate networks to allow multiple devices to share a single public IP address.

- How NAT Works:

- **Outbound NAT**: When a device on the internal network sends a packet to the internet, the NAT device (usually a router) changes the source IP address of the packet from a private IP address to the router's public IP address.
- **Inbound NAT**: When a response is received from the internet, the NAT device checks its translation table and forwards the packet to the appropriate internal device by changing the destination IP address to the correct private IP address.
- **Port Address Translation (PAT)**: Often, NAT uses **PAT**, where multiple internal devices share a single public IP address. Each outgoing connection is tracked by its unique port number to differentiate between different sessions.
    - NAT helps to conserve public IP addresses, as many internal devices can share a single public IP address.

8.Network params

- Bandwidth/frequency/channel/ spectrum/ range

Bandwidth in networking refers to the maximum rate at which data can be transmitted over a communication channel, typically measured in **bits per second (bps)**, kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps). Bandwidth determines the capacity of the network link — the higher the bandwidth, the more data can be transmitted within a given time.

While **bandwidth** represents the potential data transfer rate, it is not the same as **speed**. Network speed can be affected by factors like network congestion, latency, and packet loss, even if the available bandwidth is high. Bandwidth is often likened to the width of a highway: a wider highway (more bandwidth) can accommodate more cars (data), but factors like traffic (congestion) or road conditions (latency) can still slow things down.

- Jitter/latency

Latency in networking refers to the time it takes for a data packet to travel from its source to its destination. It is usually measured in **milliseconds (ms)**

- Data rate/ throughput

6.Network Tools

- Ping/ traceroute

A **ping test** is a network diagnostic tool used to test the reachability of a host on an IP network. It works by sending an **ICMP (Internet Control Message Protocol)** Echo Request message to the target IP address and waiting for an **Echo Reply**. The time taken for the reply to return is measured and reported in milliseconds (ms).

How the Ping Test Works:

1. A user sends a "ping" request to a specific IP address or domain.
2. The target device responds with an Echo Reply, indicating that the device is reachable.
3. The round-trip time (RTT) is calculated and reported, showing how long it took for the ping to travel from the source to the target and back.

Uses of Ping in Troubleshooting:

- **Network Connectivity**: A ping test can verify if a device (e.g., a server or router) is reachable across the network or the internet.
- **Latency Measurement**: It measures the round-trip time for packets to travel, indicating network latency.
- **Packet Loss**: If packets are lost (i.e., no reply is received), it could indicate network congestion, faulty hardware, or routing issues.
- **Diagnosing Network Failures**: Ping is often the first step in troubleshooting a network failure, helping to identify whether the issue is with a specific device or a broader network problem.

□ □Packet Structure: Data Flow (Example)

A client device connects to a website:

```
App Layer → HTTP GET request
↓
Transport → TCP segment (Port 443)
↓
```

Network → IP packet (Src IP, Dst IP)
↓
Data Link → Wi-Fi/Ethernet frame (Src MAC, Dst MAC)
↓
Physical → Modulated signal (802.11 PHY)