Network fundamentals

1. What is network?

Network connects two or more computer to **communicate with each** other or for **exchange of information.**

Why we need networking?

- Better connectivity.
- Better communication.
- Helps in sharing resources.

Types of network:

1) Local Area Network (LAN)

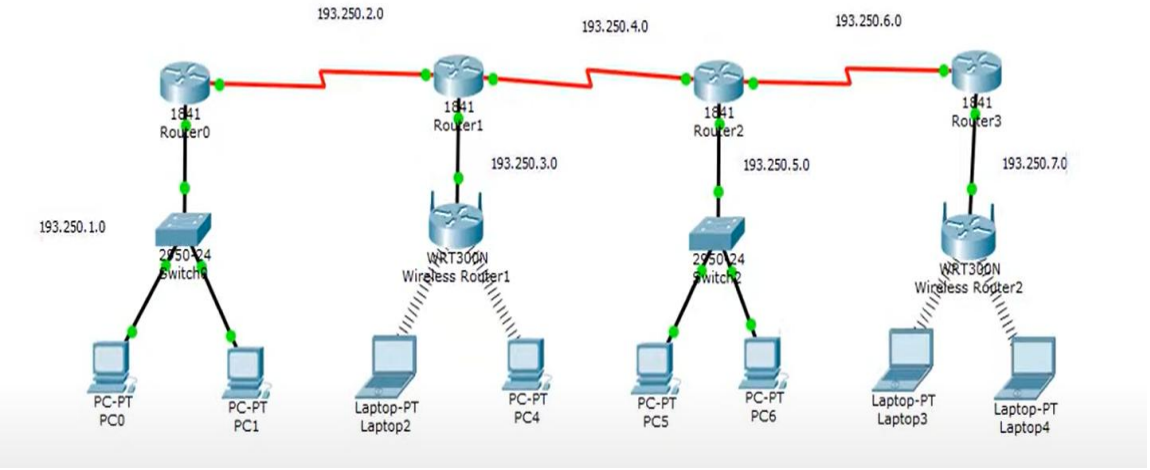
A LAN (Local Area Network) is a network that connects computers and devices within a **small geographical area**, such as a home, office, or school. It typically uses Ethernet or Wi-Fi for communication.

Example - same room, same building.

2) Wide Area Network (WAN)

A WAN (Wide Area Network) covers a **large geographical area**, often spanning cities, countries, or even continents. It connects multiple LANs and MANs through the internet, leased lines, or satellite links.

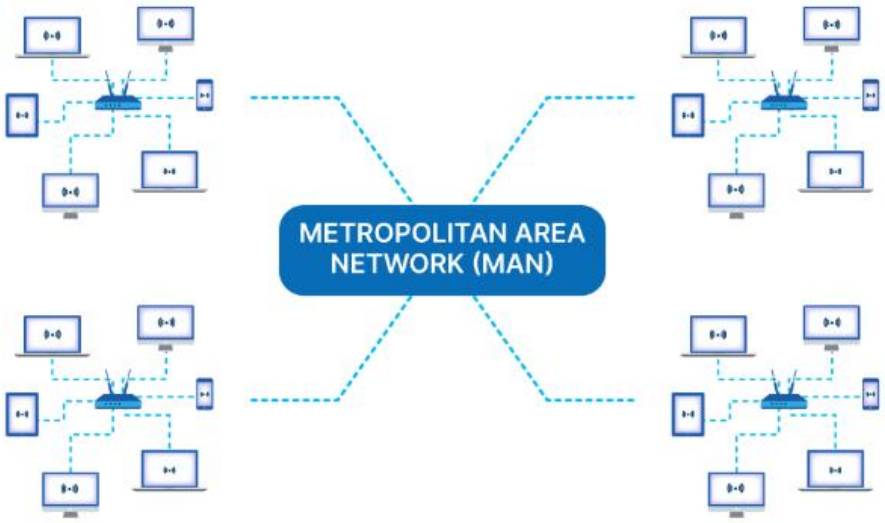
Example - across campuses/ cities.



3) Metropolitan Area Network (MAN)

A MAN (Metropolitan Area Network) covers a **city or large campus** and is larger than a LAN but smaller than a WAN. It connects multiple LANs within a metropolitan area using fiber optics or high-speed connections.

Example – cover campus, city's public Wi-Fi network.



4) Personal Area Network (PAN)

A PAN (Personal Area Network) is a network designed for personal devices within a short range (typically **a few meters**).

Example – USB, bluetooth headset, smartwatch syn with a phone.

5) Virtual Private Network (VPN)

It is a technology that creates a **secure, encrypted connection** over a public or private network (like the Internet). It allows users to securely access a private network and browse the internet anonymously by **masking their real IP address**.

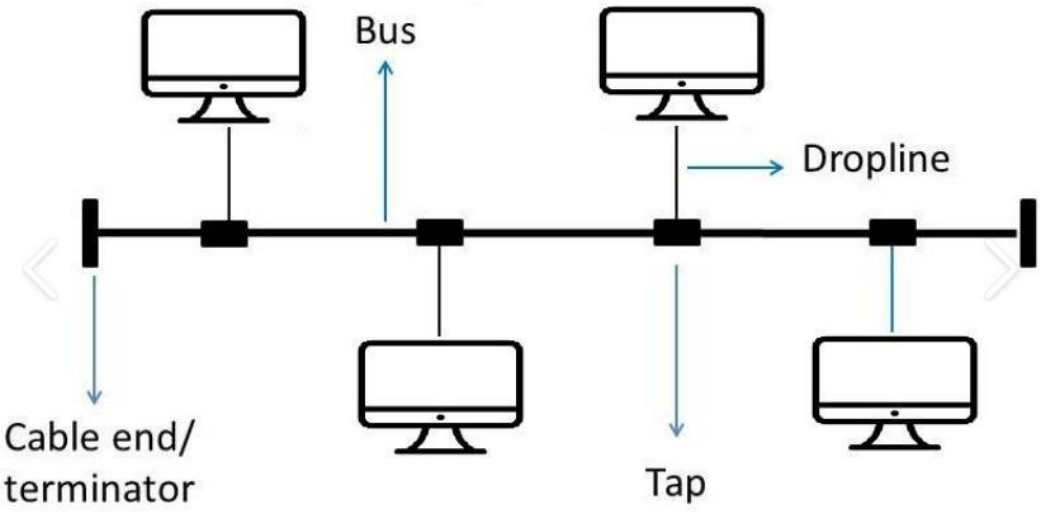
Example – use for remote work, individual use them to access blocked website.

2. Commonly used Physical Topologies

1. Bus Topologies

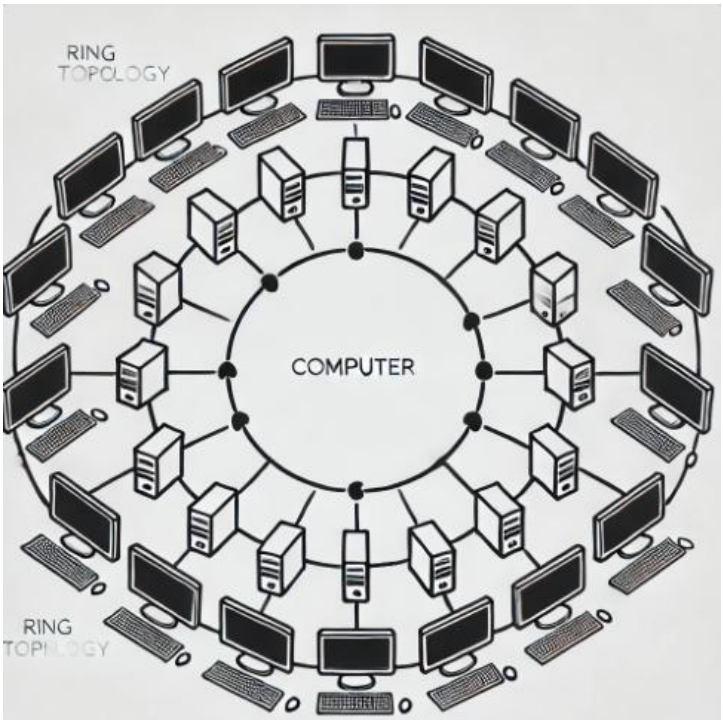
A bus topology is a network arrangement where all devices are connected to a single central communication cable (bus). Data is transmitted in both directions along the bus, and each device receives the data but only processes messages intended for it.

Example: A school computer lab where all computers are connected to a single main cable.



2. Ring Topologies

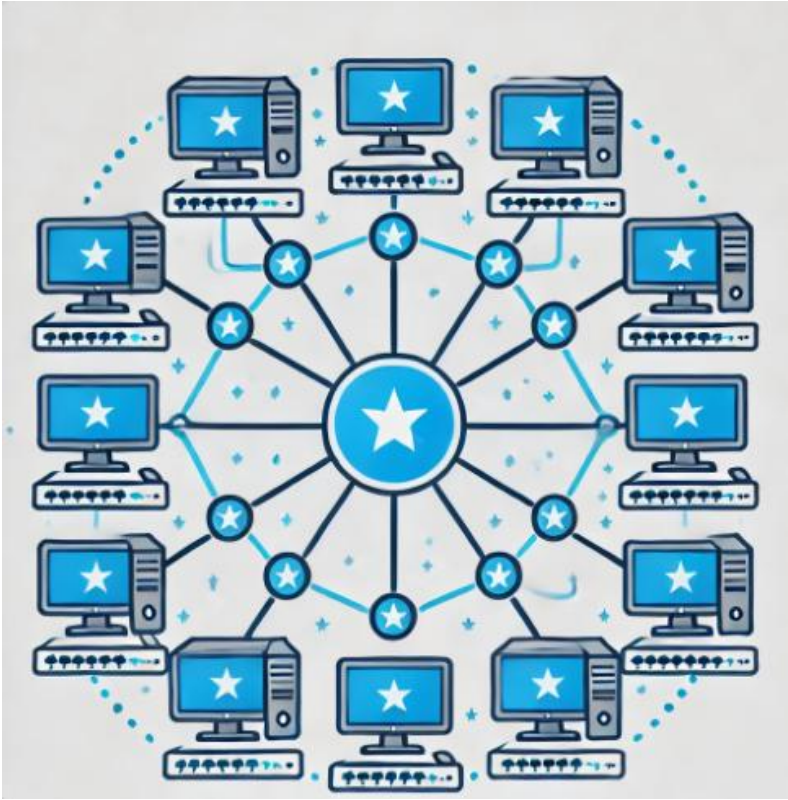
A ring topology is a network setup where each device is connected to exactly two other devices, forming a closed loop or ring. Data travels in one or both directions along the ring, passing through each device until it reaches its destination.
Example: A group of office computers connected in a circular manner, where data passes through each one before reaching its destination.



3. Star or Y Topologies

A **star topology** is a network structure where all devices are individually connected to a central hub, switch, or router. The central device manages and controls communication between nodes, ensuring efficient data transmission.

Example: A home Wi-Fi network where all devices (phones, laptops, TVs) connect to a central router.

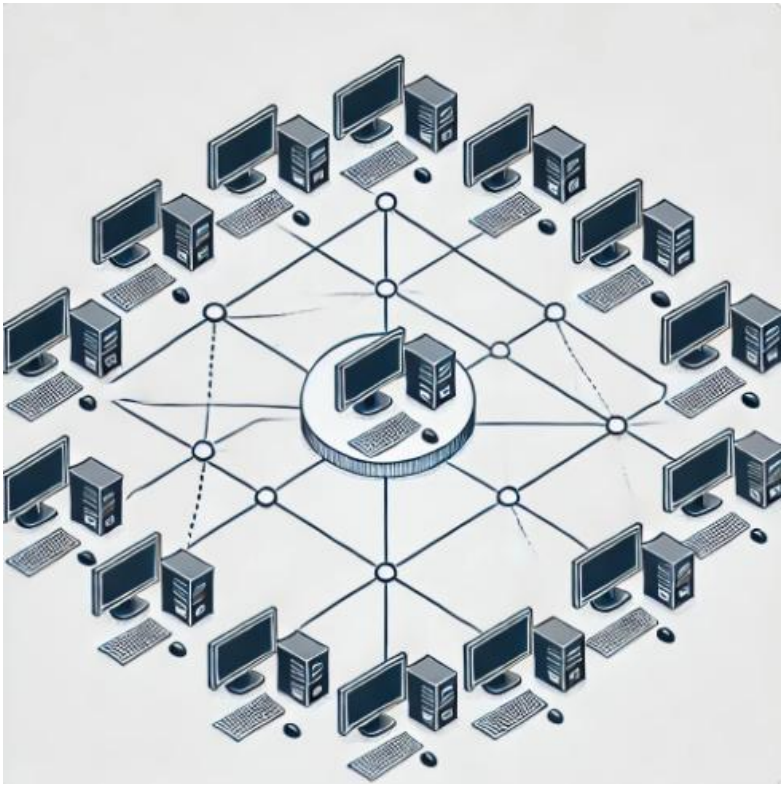


4. Mesh Topologies

A **mesh topology** is a network configuration in which devices are interconnected, either fully (every device connected to every other device) or partially (some devices connected to multiple others). This provides

redundancy and fault tolerance, ensuring continuous network operation even if some connections fail.

Example: The internet, where multiple servers are connected to ensure continuous access even if one server fails.



3. Network Architecture

Defines how computers and other devices **interact within a network.** It sets the rules and structure for data communication and determine how information flow.

Types of Network Architecture

1. Client – Server Architecture

Centralized network model where one or more servers provide services to multiple clients.

Example - Websites and web applications use client-server architecture.

2. Peer-to-Peer(P2P) Architecture

Decentralized network, all devices (or nodes) act as **both clients and servers.** Each device can communicate without a need of central server.

Example – Blockchain and file sharing software.

3. Hybrid Architecture

Combines elements of **both client-server** and peer-to-peer models. Offers flexibility for specific use cases.

Example - Microsoft Teams, where users can access centralized servers but also share files peer-to-peer.

4. Cloud-Based Architecture

Services and storage are provided over internet **by cloud** provider. User access resources remotely.

Example- Amazon Web Service (AWS), Google Cloud Platform (GCP).

5. Software-Defined Networking (SDN)

Separates the control plane (decision-making) from the data plane (packet forwarding). Centralized management allows

flexibility and rapid deployment of new service wherever they want.

Example - Cisco ACI or VMware NSX for flexible and scalable network management.

4. Networking Technologies

1. Wired Networking

Use physical cables to transmit data, offering higher speed, stability, and security.

- Ethernet

A wired networking technology that connects devices in a **LAN** (Local Area Network) using cables (like Cat5, Cat6). It provides **high-speed, stable, and secure** data transfer.

Example – Office network and broadband connection.

- Fiber Optic

A high-speed communication technology that uses **light pulses through glass or plastic fibers** to transmit data over long distances with minimal loss.

Example – Internet Service Provider (ISP) use fiber optic.

2. Wireless Networking

Use radio waves to transmit data, allow devices to connect without cable.

- Wi-Fi (Wireless Fidelity)

A wireless networking technology that allows devices to connect to the internet or a network using **radio waves**,

eliminating the need for physical cables. It follows IEEE 802.11 standard.

Example - Home Wi-Fi router connecting to devices.

- Near Field Communication (NFC)

  A **very short-range** wireless communication technology (typically **a few centimeters**) used for **contactless payments** and **data transfer**.

  Example – Tapping phone on a payment terminal.

- Bluetooth

  A short-range **wireless communication** technology that enables devices to exchange data over short distances (typically up to **10 meters**).

  Example – Wireless headphones connecting to a smartphone.

5. Network Communication Protocol

A protocol is a set of **rules and standards** that define how data is **transmitted** and received between devices in a network. It must be followed in order for the message to be successfully

delivered and understood.

Types of Network Protocols

1. Network Communication Protocols –

   How data is exchanged between devices over a network and **ensuring efficient communication**. They handle syntax,

semantics, synchronization, authentication, and error detection.

- HTTP (Hypertext Transfer Protocol) - Used for **web communication**, transferring webpages and resources between browsers and servers.
- TCP (Transmission Control Protocol) - Connection-oriented protocol and it **ensures reliable transmission** of data. Implement error-checking and retransmission of lost packets.
  Example - Web browsing, file transfers, email.
- UDP (User Datagram Protocol) – Connectionless protocol and allow fast transmission **without guaranteed delivery**. Sends packets without establishing a connection.
  Example – Streaming video/audio, online gaming.
- DHCP (Dynamic Host configuration Protocol) – A DHCP server automatically **assigns an IP address** and various other configurational changes to devices on a network so they can communicate with other IP networks.

2. Network Management Protocols -

These protocols are designed to monitor, control, and maintain network operations.

- SNMAP (Simple Network Management Protocol)- It's a 7 layer protocol that is used for **managing nodes** on an IP network. Used for monitoring and managing network devices like routers and switches.

- ICMP (Internet Control Message Protocol) – It is network layer supporting protocol used by network devices to **send error messages** and operational information. It is used to announce network errors, congestion, and timeouts, as well assist in troubleshooting.
- FTP (File Transfer Protocol) – It's a application layer protocol. Facilitates **file transfer** between computer over a network.
  Example – Website management, file sharing.
- POP3 (Post Office Protocol) – It is a protocol that a local mail client uses to **get email messages** from a remote email server over a TCP/IP connection. After the email client downloads the emails, they are **generally deleted** from the servers.

3. Network Security Protocols -

   These protocols **secure the data** in passage over a network. These protocols also determine how the network secures data from any unauthorized attempts to extract or review data.

   - SSL (Secure Socket Layer)- It mainly used for **protecting sensitive data** and securing internet connections. It **encrypts communication** between web browsers and servers. Establishes a secure connection by encrypting data transferred over HTTPS websites.
   - IPsec (Internet Protocol Security) – Secure IP communications by **encryption** and authenticating **data**

packet. Sets up encrypted, authenticated IP connections over a virtual private network (VPN).

- SSH (Secure Shell) – Provide **secure remote access** to devices over an untrusted network.
  It's act like a secure tunnel that form around the data transfer and manages server.
- SFTP (Secure File Transfer Protocol) – Facilitates **secure file transfer** between devices.
  Prevent unauthorized access during file uploads or downloads.

4. Application Layer Protocols -

These protocols **operate at the top layer** of the OSI model. These protocols enable direct **interaction between end-user** applications and the network.

- DNS (Domain Name System) - The DNS protocol helps in **translating** or mapping **host names to IP addresses**. Hosts are identified based on their IP addresses, but memorizing an IP address is difficult due to its complexity. IPs are also dynamic, making it all the more necessary to map domain names to IP addresses. DNS helps in resolving this issue
- IMAP (Internet Message Access Protocol) - ICMP protocol is used to **retrieve message** from the mail server. By using ICMP mail user can view and manage mails on his system. IMAP allows synchronizing **read, moved, and deleted messages**. IMAP is quite convenient when you check your email via multiple clients.

- SMTP (Simple Mail Transfer Protocol) - Sends **outgoing emails** from a client to a mail server or between servers, whereas POP and IMAP are used to retrieve emails on the end user's side. SMTP transfers emails between systems, and notifies on incoming emails.
- Telnet (Terminal emulation Protocol) – It enables a user to **communicate with a remote device**. Telnet lacks encryption capabilities and **sends** across critical information in **clear text**.

5. Network Layer Protocols –

These protocols facilitate **routing and forwarding** of data packets across networks.

- IP (Internet Protocol) – It is a fundamental set of rules that governs how **data is addressed**, routed, and transmitted across networks, including the Internet. It acts as the backbone of digital communication by ensuring that data packets are delivered from the source to the correct destination using **unique identifiers**.
- ARP (Address Resolution Protocol) **– Resolves IP** addresses into **MAC (Media Access Control) addresses** within a local network. A table called an ARP cache is used to maintain a correlation between each IP address and its corresponding MAC address.
- NAT (Network Address Translation) – is a process used in networking to **modify the IP address** of packets as they pass through a router. It allows multiple devices on a local network to share a single public IP address,

improving security and conserving IPv4 addresses. **Translates private IP** addresses into **public IP addresses** and vice versa.

- OSPF (Open Shortest Path First) – It is a **link-state routing protocol** used in **IP networks** to determine the best path for data transmission. It dynamically calculates the shortest and most efficient routes using the **Dijkstra algorithm** and adapts to network changes quickly.

6. Port Number of Protocols:

Port - A port is a **virtual point** where network connections **start and end**. It acts as a logical checkpoint to direct incoming and outgoing data traffic to the correct program or **service** on a device.

Ports are identified by **unique numbers** ranging from 0 to 65535, which help computers differentiate between types of traffic, such as emails or web pages.

Protocol	Port Number(s)	Description
HTTP	80	Hyper Text Transfer Protocol for web traffic
HTTPS	443	Secure HTTP for encrypted web traffic

Protocol	Port Number(s)	Description
FTP	20, 21	File Transfer Protocol for file transfers
SSH	22	Secure Shell for secure remote login
SFTP	22	Secure File Transfer Protocol (over SSH)
Telnet	23	Unencrypted remote access
SMTP	25	Simple Mail Transfer Protocol for email sending
DNS	53	Domain Name System for domain resolution
DHCP	67 (server), 68 (client)	Dynamic Host Configuration Protocol for IP allocation
POP3	110	Post Office Protocol v3 for email retrieval
IMAP	143	Internet Message Access Protocol for email retrieval
SNMP	161 (agents), 162 (traps)	Simple Network Management Protocol
RDP	3389	Remote Desktop Protocol for remote access to a computer

Protocol	Port Number(s)	Description
OSPF	89	Open Shortest Path First for routing
IPSec	500	Internet Protocol Security
NTP	123	Network Time Protocol
TCP	8080	Transmission Control Protocol is used as an alternative to port 80

7. OSI Model and TCP/IP Model

1. OSI Model

The OSI (Open Systems Interconnection) model is a **conceptual model** developed in 1982 by the **International Organization for Standardization (ISO)** that describes how communications should occur in a computer network. It defines a framework for computer network communications.

7 Application Layer

6 Presentation Layer

5 Session layer

4 Transport Layer

3 Network Layer

2 Data Link Layer

1 Physical Layer

- Application Layer

  The application layer has the responsibility of providing **application service** to the network applications.

  At this layer data still **resembles** something that people can **read**.

  Protocol – SMTP, FTP, HTTP, DNS

  Example – Web Surfing, Email, Virtual Terminal

  Function

  - User Interface
  - Network Services
  - Network Protocols

- Presentation Layer

  This layer transforms the data into a **required format** that can be accepted by the application in the application layer.

  First data is **converted** into a form that can be sent over a network.

  Protocol – SSL, SSH, IMAP, FTP, JPEG

  Example – ASCII, Unicode

  Function

  - Translation
  - Data Compression
  - Encryption

- Session layer

  This layer performs the function of **establishing sessions** between the devices, how long the session should be, which side will **transmit**, when to transmit and how long to transmit.

  Protocol – API, NetBIOS, RPC (Remote Procedure Call)

  Examples – A user logging into a remote server and maintaining an active session without re-authenticating repeatedly.

  Function

  - Session Establishment
  - Data Synchronization
  - Session termination

- Transport layer

  This layer ensures that the **delivery of data** from **one end point** to another indeed gets completed **without any errors**.

  Protocol – TCP (Transmission Control Protocol), UDP (User Datagram Protocol)

  Example - A video call ensuring that voice packets arrive in the correct order with minimal delay.

  Function

  - Segmentation & reassembly
  - Flow control
  - Error handling

- Network Layer

It is responsible for routing best path for data packet based on its **logical IP address**.

It responsible for **routing, addressing, and forwarding data** between different networks.

Protocol – IP (Internet Protocol), ICMP (Internet Control Message Protocol), BGP (Border Gateway Protocol).

Example - A router determining the best path for a data packet traveling from Mumbai to Sydney.

Function

- IP Addressing
- Routing
- Packet Forwarding

- Data Link Layer

  This layer is responsible for **node-to-node communication**, **framing**, **error detection & correction**, and **MAC addressing**. It perform error detection only at the frame level.

  Data packets are encoded and decoded into bits and It also ensures that data is transmitted correctly over the physical network.

  Protocol - Switches, Bridges, ARP (Address Resolution Protocol)

  Example - A switch forwarding data between computers in an office LAN based on MAC addresses.

  Function

  - Framing
  - MAC addressing

- Error detection & correction

- Physical Layer

  This layer is responsible for transmitting bits (0s and 1s) from one device to another device over a physical media. The media could be wire, wireless or optical fiber.

  Protocol – Repeater, Hub, Ethernet cables.

  Example – A fiber optic cable transmitting light signals between two data centers.

  Function

  - Bits Transmission
  - Hardware Connection
  - Signal Modulation

2. TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is a **network communication model** that defines how data is transmitted and received over the internet. It ensures **reliable data delivery, addressing, and routing** between devices across different networks. TCP/IP is the foundation of the modern internet.

4 Application Layer

3 Transport Layer

2 Internet Layer

1 Network Interface Layer

- Application Layer

  This layer combines the **application, presentation, and session layer** functionalities of the OSI reference model.

This layer is to hand over the data received from the bottom layer to the application and to make sure the application is able **to interpret the data** that it has received from the other network device.

- Transport Layer

  In this layer the data is to **deliver** from the **client to the server without error and loss.** Data can be lost during the transmission but TCP ensure that the data is not lost and triggers retransmission process until the data is correctly and completely received.

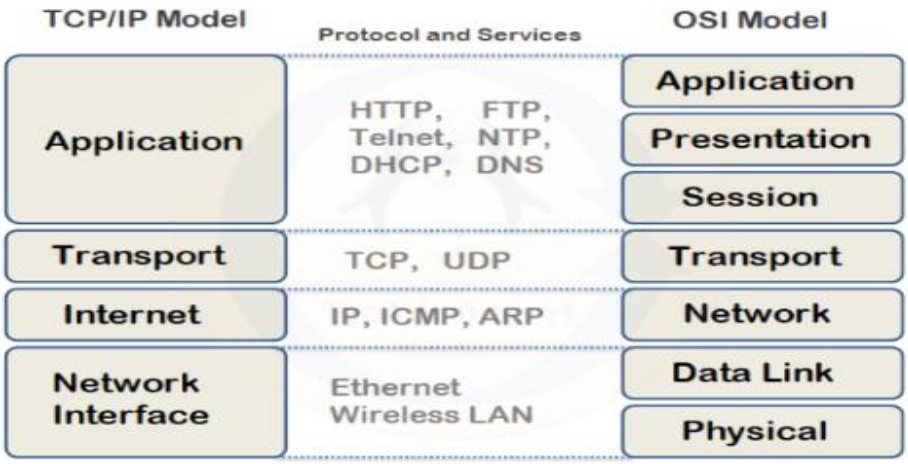
- Internet layer

  This layer is responsible for **moving the data** from one node to another node. This layer's function is very **similar to the network layer** function of OSI reference model.

- Network Access Layer/Physical Layer

  It combines the function of **Data Link and the Physical Layer** of OSI reference model. The Network Access Layer is responsible for **creating data 'frames'** for transmitting and receiving data from the Physical Layer.

  This function is implemented by Network Interface Card (NIC), an **adapter connected** to the computer through **physical wires** or optical fiber cable.



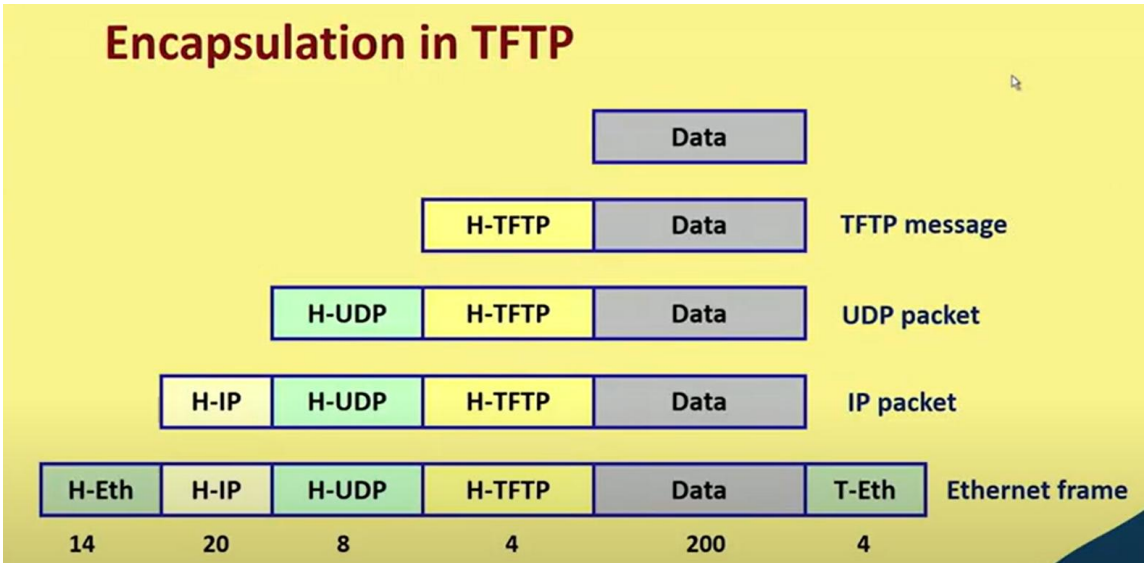
Difference between OSI Model and TCP/IP Model

Aspect	OSI Model	TCP/IP Model
Full Form	Open Systems Interconnection	Transmission Control Protocol/ Internet Protocol
Purpose	Conceptual framework for understanding network communication	Practical model for internet communication
Number of Layers	7 Layers: Application, Presentation, Session, Transport, Network, Data Link, Physical	4 Layers: Application, Transport, Internet, Network Interface
Development	Developed by ISO	Developed by ARPANET

Aspect	OSI Model	TCP/IP Model
	(International Standards Organization) in 1984	(Advanced Research Projects Agency Network) in the 1970s
Approach	Follows a vertical approach with clear distinctions between layers	Follows a horizontal approach with overlapping functionalities
Layer Functions	Each layer has specific roles and responsibilities	Combines some OSI layers into broader categories
Protocol Dependence	Protocol-independent; focuses on theoretical understanding	Protocol-specific; emphasizes practical implementation
Connection Types	Transport layer is connection-oriented	Supports both connection-oriented and connectionless communication
Flexibility	Rigid structure with distinct layers	Flexible and adaptable to real-world networking
Header Size	Smaller header size (5 bytes)	Larger header size (20 bytes)

Encapsulation

- As data flows **down the protocol hierarchy**, headers (and trailers**) get appended** to it.
- As data moves up the hierarchy, headers (and trailers) **get stripped off.**
- Example –
    - Trivial file transfer protocol (TFTP)
    - TFTP client transfer 200 bytes of data
    - 4 bytes of TFTP header gets added



8. IP Address

An IP address (Internet Protocol address) is a **unique numerical identifier** assigned to devices connected to a network that uses the Internet Protocol for communication. It functions like an

address, allowing **devices to locate** and communicate with each **other over the internet** or a local network.

Types of IP Addresses :–

1. Private IP Addresses –

A private IP address is an IP address **used within a local network** (LAN) and is **not routable on the internet**. These addresses are assigned to devices like computers, routers, and printers within a home, office, or enterprise network.

Classes of Private IP Addresses

Class A

- **Range** – 10.0.0.0 to 10.255.255.255
- **Subnet Mask** – 255.0.0.0 (/8)
- **Number of Address** – 16,777,216
- **Purpose** – Used for very large networks or multiple networks behind a single external.
- **Example** – 10.0.0.1

Class B

- **Range** – 172.16.0.0 to 172.31.255.255
- **Subnet Mask** – 255.224.0.0 (/12)
- **Number of Addresses** – 1,048,576
- **Purpose** – Suitable for medium – sized networks like enterprise-level LANs.
- **Example** – 172.25.22.168

Class C

- **Range** – 192.168.0.0 to 192.168.255.255
- **Subnet Mask** – 255.255.0.0 (/16)
- **Number of Addresses** – 65,536
- **Purpose** – Commonly used for small networks like home or office setups with fewer devices connected to the router.
- **Example** – 192.168.2.192

2. Public IP Address

A public IP address is **assigned by an Internet Service Provider** (ISP) and is used for communication over the internet. It is globally unique and can be accessed from anywhere in the world.

Class	Range	Default Subnet Mask	CIDR Notation	Example	Purpose
A	1.0.0.0 – 126.255.255.255	255.0.0.0	/8	10.2.108.249	Large networks (e.g., ISPs)
B	128.0.0.0 – 191.255.255.255	255.255.0.0	/16	142.160.56.47	Medium-sized networks
C	192.0.0.0 – 223.255.255.255	255.255.255.0	/24	251.16.16.106	Small networks
D	224.0.0.0 – 239.255.255.255				Multicasting
E	240.0.0.0 – 255.255.255.255				Reserved for research and

Class	Range	Default Subnet Mask	CIDR Notation	Example	Purpose
					future use

3. Static IP Address

A static IP address is a **fixed and unchanging** address assigned to a device. It remains constant unless manually changed by the user or the ISP.

Use Case

- Hosting websites or servers.
- Remote access (e.g., Remote Desktop Protocol).
- Businesses requiring consistent network configurations.

4. Dynamic IP Address

A dynamic IP address is **temporary and changes periodically.** It is automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server.

Use Cases

- Home internet users.
- Devices that do not require constant accessibility, such as smartphones or laptops.

5. IPv4

IPv4 is the fourth version of the Internet Protocol and is one of the core protocols of the Internet. It was developed in the early

1980s and is still widely used today for routing traffic on the internet. It uses broadcasting method.

Address Format

- **Length:** 32 bits
- **Representation:** Typically expressed in dot-decimal notation, which consists of four octets separated by periods (e.g., 192.168.1.1).
- **Example:** The address 192.168.1.1 consists of four octets: 192, 168, 1, and 1.

Address Space

IPv4 supports approximately **4 billion** unique addresses, which has led to address **exhaustion due to the rapid growth** of devices connected to the internet.

Security

IPv4 does **not have built-in security** features; instead, it relies on external protocols such as IPsec for securing data transmission.

6. IPv6

IPv6 is the sixth version of the Internet Protocol, designed to **replace IPv4 due to its limitations** in address space and features. It uses multicasting.

Address Format

- **Length:** 128 bits
- **Representation**: Expressed in hexadecimal notation, consisting of eight groups of four hexadecimal digits separated by colons

- **Example:** The address 2001:db8::ff00:42:8329 uses shorthand notation where consecutive zeros can be abbreviated using "::".

Address Space

IPv6 supports an enormous number of unique addresses—approximately **340 undecillion** .Solving the address exhaustion problem faced by IPv4.

Security

IPv6 has built-in security features through IPsec, which provides encryption and authentication

for secure data transmission.

Converting IP address into Binary

Example – 192.168.43.241

1. Converting each octet to binary
    - First Octet: 192
        - **Decimal:** 192
        - **Binary:** 11000000
        - **Explanation:** 128+64 =192
    - Second Octet: 168
        - **Decimal:** 168
        - **Binary:** 10101000
        - **Explanation:** 128+32+8 = 168
    - Third Octet: 43
        - **Decimal:** 43

- **Binary:** 00101011
- **Explanation:** 32+8+2+1= 43

- Fourth Octet: 241
  - **Decimal:** 241
  - **Binary:** 11110001
  - **Explanation:** 128+64+32+16+1= 241

2. Full Binary Representation

   11000000.10101000.00101011.11110001

9. Subnet Mask

A **subnet mask** is a 32-bit number used in IPv4 networking to divide an IP address into two parts: the **network portion** and the **host portion**. It determines which part of the IP address identifies the network and which part identifies individual devices (hosts) within that network. Subnet masks are essential for subnetting, which **allows large networks to be divided into smaller,** more manageable sub-networks (subnets).

Example-

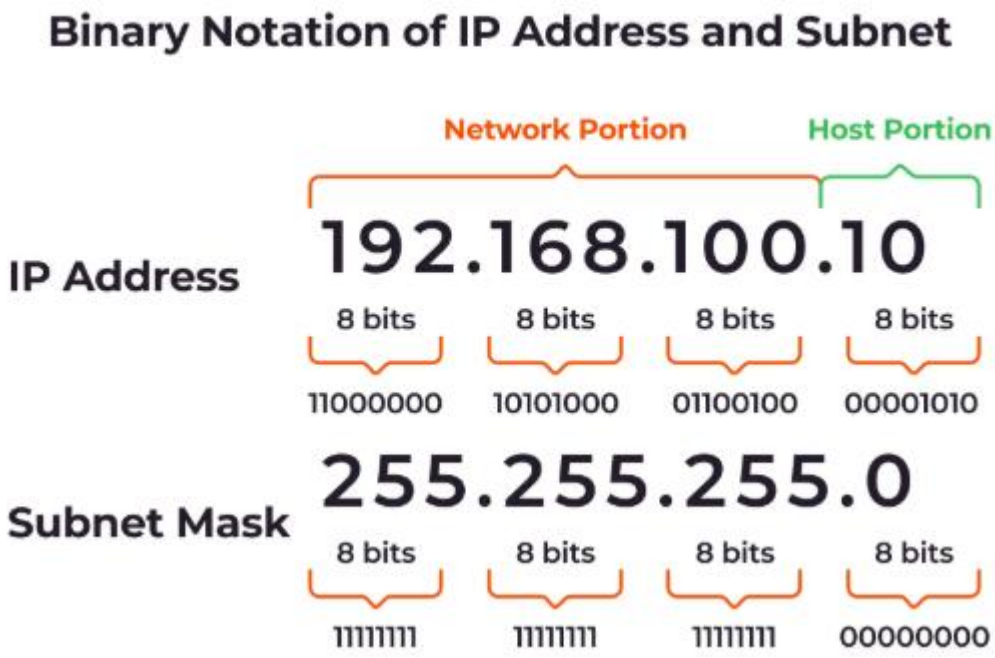
IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

The first three octets (192.168.2) represent the **network**, and the last octet (1) represents the **host.**

Router IP Address: 192.168.2.1

Broadcast Address: 192.168.2.255



10. CIDR (Classless Inter-Domain Routing)

It is a method for efficiently allocating and organizing IP addresses. Introduced in 1993 by the Internet Engineering Task Force (IETF), CIDR replaced the older classful addressing system (Class A, B, C) to address inefficiencies and prevent IPv4 address exhaustion. It uses **variable-length subnet masking (VLSM)** to create flexible and scalable subnetworks, improving routing efficiency and reducing wasted IP addresses.

Key components of CIDR

1. CIDR Notation

Represents an IP address followed by a forward slash (/) and a number indicating the number of bits used for

the network prefix.

Example :-

- 10.0.0.0/8 :- First **8 bits** are reserved for network**,** remaining **24 bits** are for host addresses.
- 172.16.0.0/16 :- First **16 bits** are reserved for network, remaining **16 bits** are for host address.
- 192.168.1.0/24 :- The first **24 bits** are reserved for network, leaving **8 bits** for host addresses.
- 192.168.1.100/32 :- All **32 bits** are used for the network, **0 bits** for host addresses

2. CIDR Block

A range of IP addresses sharing the same network prefix.

Example: 192.168.1.0/24 represents all IP from

192.168.1.0 to 192.168.1.255.

Example –

IP – 192.168.1.0/24

Subnet Mask – 255.255.255.0

Network Portion – first 24 bits

Host Portion: last 8 bits allow for 2^8 -2 = 254 usable addresses

Usable Range: 192.168.1.1 to 192.168.1.254

If we divide this smaller subnet:

Subnet 1: 192.168.1.0/25 (range: 192.168.1.1 to 192.168.1.126)

Subnet 2: 192.168.1.128/25 (range: 192.168.1.129 to 192.168.1.254)

Labs

1. Try Hack Me

Beginner:

- **Network Fundamentals**: Learn the basics of networking concepts. TryHackMe | Networking Concepts
- **Wireshark**: Get hands-on with packet analysis. TryHackMe | Wireshark Training
- **Nmap**: Learn how to leverage the Nmap network scanner to discover live hosts and open ports using basic and advanced scan options. TryHackMe | Nmap Training

Intermediate:

- **Network Exploitation Basics**: Understand, enumerate and attack various networking services in real-world environments. TryHackMe | Network Exploitation Basics Training
- **Network Security mad Traffic Analysis**: Understand the core concepts of Network Security and Traffic Analysis to spot and probe network anomalies using industry tools and techniques. TryHackMe | Network Security and Traffic Analysis Training
- **Network and System Security**: Explore principles of network & system security, including secure protocols, hardening OS, cloud, and network devices using latest

techniques. TryHackMe | Network and System Security Training

Advanced:

- **Network Security Evasion**: Learn how to bypass and evade different security solutions used in the industry, such as firewalls and IDS/IPS. TryHackMe | Network Security Evasion Training
- **Network Security Model:** Covers passive and active network attack TryHackMe | Network Security Training

2. Hack The BOX

Beginner:

- **Wifinetic:** Hack The Box :: Hack The Box
- **Networked**: Hack The Box :: Hack The Box

Intermediate:

- **Carrier**: Hack The Box :: Hack The Box
- **Sniper:** Hack The Box :: Hack The Box

Advanced:

- **Reddish:** Hack The Box :: Hack The Box
- **RastaLabs:** Hack The Box :: Hack The Box

Questions

1. Which of the following network is used to cover small area like a room/building?
   a) LAN
   b) WAN
   c) MAN
   d) PAN
2. Which of the following is/are transport layer protocol?
   a) UDP
   b) TCP
   c) IP
   d) Both a and b
3. Which of the following OSI layer is responsible for end-to-end reliable data transfer?
   a) Physical layer
   b) Network Layer
   c) Data Link Layer
   d) Transport Layer
4. Which of following statement is/are true for the IP address?
   a) It uniquely identifies a network interface of a computer system.
   b) When a packet is routed to the destination network, only the network number is used.
   c) It indicates how many hardware ports are there in the computer system.

d) None of these.

5. Which of the following is not a valid port number in TCP/IP?
   a) 21
   b) 80
   c) 8080
   d) 80800
6. Which address do the IP addresses 10.16.75.12 and 192.10.85.120 belong to?
   a) Class A and Class B
   b) Class C and Class B
   c) Class C and Class D
   d) Class A and Class C
7. Which of the following IP addresses does not represent broadcast address?
   a) 10.0.0.255
   b) 10.255.255.255
   c) 173.16.0.255
   d) 192.168.255.0
8. What is the subnet address if the destination IP address is 192.168.45.178 and the subnet mask is 255.255.248.0?
   a) 192.168.40.0
   b) 192.168.45.0
   c) 192.168.48.0
   d) 192.168.42.0
9. Which of the following is true for IPv6?

a) IPv6 address does not have any defined classes.

b) Base header size is 20 byte.

c) IPv6 is connection oriented.

d) All of these.

10. If a packet is to be delivered to all the host in a network, what kind of address should be specify the destination?

a) Unicast address.

b) Broadcast address.

c) Anycast address.

d) None of these.

11. How many layer are there in OSI model _____?

12. TCP is a _____ oriented protocol.

13. The IEEE standard for Wi-Fi is _____.

14. The protocol used to transfer files between computers is _____.

15. A _____ failure in a client – server model can lead to downtime for all connected client.

16. XYZ Corp is assigned the 144.16.192.24/29 network for internal use. The IT team needs to determine the valid IP address range. What is the correct address range for this block?

a) 144.16.192.0 to 144.16.192.8

b) 144.16.192.8 to 144.16.192.16

c) 144.16.192.16 to 144.16.192.24

d) 144.16.192.24 to 144.16.192.31

17. Sarah connects her smartphone to a smartwatch via Bluetooth to track her fitness activities. This type of

network operates within a very short range and is designed for personal device communication. What type of network is being used?

a) LAN

b) MAN

c) WAN

d) PAN

18. A company deploys a new network with addresses like 2001:0db8:85a3::8a2e:0370:7334. The IT team claims this system supports broadcasting to all devices. Is their claim correct?

a) Yes, because IPv6 allows broadcasting

b) No, because IPv6 does not support broadcasting

c) Yes, because IPv6 uses Class E addresses

d) No, because IPv6 only supports 32-bit addressing

19. A user is experiencing slow website loading times due to packet loss during transmission. The problem is identified in a layer responsible for error correction and flow control. Which layer is most likely affected?

a) Data Link

b) Transport

c) Network

d) Session

20. A company's network suddenly experiences massive packet loss. The IT team discovers that the problem is due to electromagnetic interference from nearby construction work, causing corrupted signals. Which

layer is affected?

a) Network

b) Data Link

c) Transport

d) Physical