NETWORKING SYSTEMS

Computer networking refers to **interconnected computing devices that can exchange data and share resources with each other**.

DATA COMMUNICATIONS

Data communications (DC) is the process of using computing and communication technologies to **transfer data from one place to another, or between participating parties**.

ELECTRONIC MAIL

- Electronic Mail (E-mail) is the **transmission of textual material** from one place to other by electronic means.
- Electronic mail systems work on the principle of providing each user with a **mail box located in a computer** in which messages are **stored and can be accessed**.

E-mail set-up

- Source/Destination (Computers)
- Data communication devices (modems)
- A communication channel (cable)
- Data communication software

Advantages of Email are

- Messages can be sent at whatever **time suits the user**
- Messages will be in the recipient's **mailbox within minutes**.
- **Delivery** of messages can be confirmed.

- **Copies can be sent automatically** to everyone on a **distribution list message**.

Dial-up lines

- In the data communication world, a dial-up line forms a link between two distant computers or local area networks.
- Dial-Up Line is any telecommunications link that is **serviced by a modem**. Dial-up lines are **ordinary phone lines used for voice communication.**

Leased Line

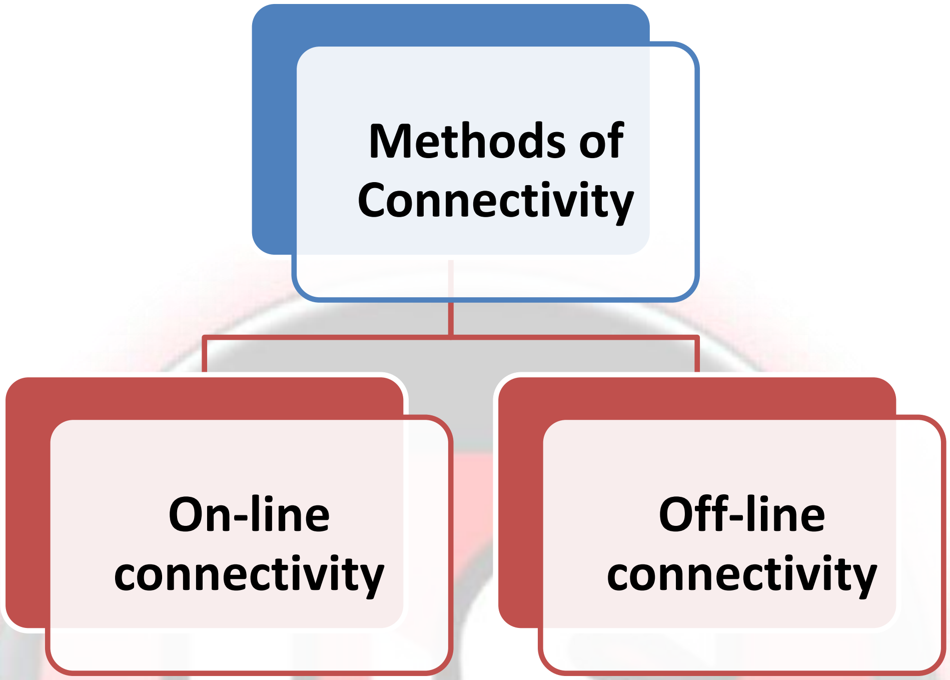
- A leased line is a bidirectional **telephone line** that has been rented for private voice, **data exchange or telecommunication use**.
- It is a dedicated link between the source and the destination. It is capable of meeting the **highest performance requir**ements.

INTERNET

The internet is a **globally connected network system** facilitating worldwide communication and access to data resources through a vast collection of **private, public, business, academic and government networks.**

INTERNET CONNECTIVITY

- The user gets connected to Internet through an Internet server.
- Internet servers are provided by many **organization**s. Those are called **Internet service providers**.



Methods of Connectivity

On-line connectivity

Off-line connectivity

On-Line Connectivity

- On line connection provides **dedicated Internet access** that requires **substantial initial investment in equipment**.
- The main continuing cost is a annual **fee for the use of the line**; the annual fee varies from the line capacity.

On-line connection through leased line

- In this, the user's system gets connected to an **Internet server by a dedicated telephone line.**
- In this leased line are connected **one end to the internet router** of the customer premises and the other end to the ISPs backbone router.

On-line connection through VSAT

This is a **wireless connection**. In this user's computer system is **connected to VSAT** (Very Small Aperture Terminal).

Requirements of VSAT connection are

- A device **with IP address**; VSAT with personal earth station (PES) and an **account on service provider system**.
- **A router (for local network connectivity**

OFF-LINE (DIAL-UP) CONNECTIVITY

Dial-up connection uses a **standard phone line and analog modem to access the Internet** at data transfer rates (DTR) of up to 56 Kbps

INTRANET

- An intranet is a **private network contained within an enterprise** that is used to **securely share company information and computing resources among employees.**
- Internet is a global network system and is available to all while **Intranet are available to the inside users**.

EXTRANET

- Extranet is an **external of computer network** that allows the trusted outside users to access the Intranet of organization.
- Extranets are connected to **Intranet through Routers** as well as **network security devices** such as Firewalls for securing Intranet from the users of Extranet.

LOCAL AREA NETWORKING

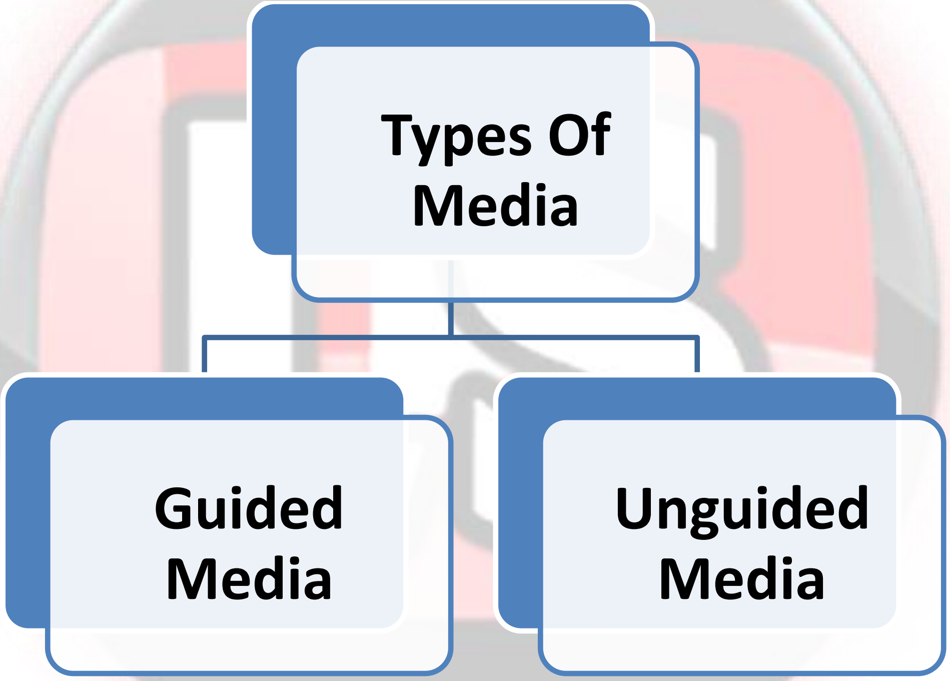
- The network is confined to a small area typically a single building or a cluster of buildings.
- The **data rate** on the network is high, anywhere from to **100Mbps to 10 Gbps.**
- In this any device can **initiate data exchange** with any other device.
- small businesses, **local governments and schools are** using the power of LANs to increase productivity and efficiency.

LAN HARDWARE AND SOFTWARE

LAN hardware and software is designed to connect all types of PCs.

Media

Media is a term that largely refers to the **cable or wires connecting together the various computing devices** that make up a LAN.


Types Of Media
Guided Media
Unguided Media

GUIDED MEDIA

It is defined as the **physical medium through** which the signals are transmitted. It is also known as **Bounded media**.

Twisted-pair wiring

Twisted pair is a physical media made up of a **pair of cables twisted with each other.**

Coaxial cable

- It contains **two conductors** parallel to each other.
- The inner conductor of the **coaxial cable** is **made up of copper**, and the outer conductor is made up of **copper mesh**.

Fibre optic cable

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the **optical fibres coated in plastic** that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide **faster data transmission than copper wires**.

Unguided Media

- An **unguided transmission transmits** the electromagnetic waves without using any physical medium. Therefore, it is also known as **wireless transmission**.
- In unguided media, **air is the media** through which the electromagnetic energy can flow easily.

Radio Transmission

- Radio waves are the **electromagnetic waves** that are transmitted in all the directions of free space.
- Radio wave is useful for **multicasting when there is one sender and many receivers.**
- An **FM radio, television, cordless phones** are examples of a radio wave

Hubs

- A Hub is a generic term that is used for a Networking device that acts as a central point for LAN cable.
- Hubs are devices that simply **connect cables together and regenerate data** thereby passing data from one device to another.

Bridge

- **Bridge** divides the **network up into separate smaller segment**, within each segment, devices will continue to **communicate with each other**.

Switches

Switches are used to connect multiple devices on the same network within a building or campus.

Routers

- **Routers** are used to **connect multiple networks together**.
- It manages traffic between these networks **by forwarding data**
- It **allows multiple devices** to use the same Internet connection.

NETWORK SECURITY EQUIPMENT - FIREWALLS, NIDS, HIDS, IPS

FIREWALLS

- A firewall is a part of a computer system or network that is **designed to block unauthorized access** while permitting authorized communications.
- Firewalls can be implemented in **either hardware or software**, or a combination of both.

INTRUSION DETECTION SYSTEM

- An intrusion detection system (IDS) is designed to **monitor all inbound and outbound network activity.**

- It identifies any **suspicious patterns** that may indicate a network or system attack from someone **attempting to break into or compromise a system.**
- IDS is considered to be a passive-monitoring system, since the main function of an IDS product is to **warn you of suspicious activity taking place - not prevent them.**

Network Intrusion Detection System (NIDS)

- Network-based IDS systems (NIDS) are often **standalone hardware appliances** that include network intrusion detection capabilities.
- It will usually consist of **hardware sensors installed in the system computers** which analyses data packets entering and leaving the network.

Host Intrusion Detection System (HIDS)

- Host-based IDS systems consist of **software agents installed on individual computers** within the system.
- HIDS **analyse the traffic to and from the specific computer** on which the intrusion detection software is installed on.
- Host-based IDS systems (HIDS) **do not offer true real-time detection,** but if configured correctly are close to true real-time.

INTRUSION PREVENTION SYSTEM (IPS)

- It is a device that controls access to IT networks in order to **protect systems from attack and abuse.**
- It is designed to inspect attack data and take the corresponding action, blocking it as it is developing and before it succeeds.

REMOTE ACCESS SERVICES

- A remote access service connects a client to a host computer, known as a **remote access server**.
- This connection allows remote access clients to **access resources from remote locations as if they were physically attached to the network**.

TYPES OF REMOTE ACCESS CONNECTIVITY

Dial-up remote access

- In this a remote access client uses the **public telephone network to create a physical connection** to a port on a remote access server.
- This is typically done by **using a modem or ISDN adapter** to dial into your remote access server.

Virtual private network (VPN)

- A VPN can provide **secure remote access through the Internet**, rather than through direct dial-up connections.
- It enables users who are working remotely to **securely access and use applications** and data that reside in the corporate data center.

WAN TECHNOLOGY

- It is a technology that connects your **offices, data centers, cloud applications, and cloud storage together**.
- It is called a wide-area network because it spans **beyond a single building or large campus** to include **multiple locations spread across a specific geographic area, or even the world**.

INTEGRATED SERVICES DIGITAL NETWORK(ISDN)

- ISDN is a **circuit-switched telephone network** system that transmits both data and voice over a digital line.

- ISDN device **can only communicate with another ISDN device**, or with a non-ISDN device **through an ISDN modem or ISDN Terminal Adapter (TA).**

TYPES OF ISDN CHANNELS

B-channel

- The Bearer channel is a **64-kbps channel**, which can be **used for voice, video, data, or multimedia calls**.
- B-channels can be **aggregated together** for even **higher bandwidth applications.**

D-channel

The **Delta channel** can be **either a 16 kbps or 64 kbps** channel used primarily for **communications between equipment in the ISDN network and the ISDN equipment at your site**.

These ISDN channels are delivered to the user in one of two pre-defined configurations.

Basic rate interface (BRI)

- BRI is the ISDN service **most people use to connect to the Internet**.
- An ISDN BRI connection s**upports two 64kbps B-channels and one 16 kbps D-channel** over a standard phone line therefore it is called **2B+D.**
- A single BRI line can support up **to three calls at the same time.**

Primary rate interface (PRI)

- ISDN PRI service is used primarily **by large organizations** with **intensive communications needs**.
- An ISDN PRI connection **supports 23 (64 Kbps) B3-channels ant one 64 kbps D-channel (or 23B+D)** over a high-speed line.

VSAT NETWORK SYSTEM

A very small aperture terminal (VSAT) is a small-sized earth station used in the transmit/receive of **data, voice and video signals over a satellite communication network**.

SATELLITE

- A communications satellite is an **artificial satellite that relays and amplifies radio telecommunication** signals via a transponder.
- It creates a communication channel between a **source transmitter and a receiver at different locations on Earth**

SATELLITE TRANSMISSION

First Stage

In the first stage, the **signal from earth is first beamed up to the satellite** from the ground station on the earth. This process is known **as uplink**.

Second stage

- The second stage **involves transponders such as radio receivers, amplifiers, and transmitters.**
- These transponders boost the **incoming signal and change its frequency** so that the outgoing signals are not altered.

Third stage

This stage involves a **downlink in which the data is sent to the other end of the receiver on the earth**.

Bands available for commercial telecommunication

- C band: 6/4 GHz
- Ku band: 14/11 GHz

• Ka band: 30/20 GHz

BENEFITS

Cost-efficient networking

VSAT networks provide the most **economical front-office to back-office communications** in a geographically dispersed banking network.

Improved customer service

- VSAT network ensures a pleasant **banking experience by processing transactions quickly and reliabl**y.
- VSAT network gives access to **valuable information about customer base** for more effective sales and marketing campaigns.

Interactive distance learning

The customer's **satisfaction depends upon the competence of the branch staff**. VSAT networks with **interactive distance learning plat or enable** bring products to market quickly and economically.

Low-cost network growth

VSAT is easy to install, so as changing demographics demand movement of branches, of new branches, **the network can quickly. and economically accommodate those changes**.

MULTIPROTOCOL LABEL SWITCHING (MPLS

Multiprotocol Label Switching (MPLS) **is a type of data-carrying technique** for high-performance **telecommunications networks** that directs data from one network node to the next **based on short path** labels rather than long network addresses,

COMPUTER NETWORKING PROTOCOL

Network protocols are **formal standards and policies** comprised of **rules, procedures and formats** that define **communication between two or more devices over a network.**

Types of Networking Protocols

Network communication protocols these are basic data communication protocols such **as TCP/IP and HTTP**

Network Security Protocols Implement security over network communications and include **HTTPS, SSL and SFTP**

Network Management Protocols provide **network governance and maintenance** and include SNMP and ICMP.

Software Defined Wide Area Network (SD-WAN) it allows **businesses to securely link users to applications** using any mix of **transport services, such as MPLS, LTE, and broadband internet services.**

VLAN (Virtual LAN)

- A VLAN (virtual LAN) as the name indicates**, allows several networks to work virtually as one LAN.**
- VLANs are created to **provide segmentation and assist in issues like security, network management and scalability**.

BENEFITS

- Allowing **network administrators to apply additional security** to network communication.
- Making expansion and relocation of a network or a network **device easier.**

- **Decreasing the latency and traffic load on the network** and the network devices, offering increased performance.

WIRELESS NETWORKS

A wireless local-area network (LAN) **uses radio waves to connect devices such as laptops to the Internet** and to the **business network and its applications.**

BENEFITS

CONVENIENCE Access your network resources **from any location within your wireless network's coverage area**.

MOBILITY The users are **no longer tied to desk**, as they were with a wired connection.

PRODUCTIVITY Wireless access to the Internet and to the organization's key applications and resources **helps the staff get the job done and encourages collaboration**.

EXPANDABLE One can easily expand **wireless networks with existing equipment.**

SECURITY advanced technologies are available for wireless networks to provide **robust security protections**.

COST Because wireless networks **eliminate or reduce wiring costs**, they can cost less to operate than wired networks.

WORLDWIDE INTEROPERABILITY FOR MICROWAVE ACCESS (WiMAX)

- WiMAX technology is a **broadband wireless data communications** technology **providing high speed data over a wide area**.
- WiMAX is **a long-range wireless system**, covering many **kilometres** that uses licensed or unlicensed spectrum to deliver connection to a network
- Single WiMAX antenna is **expected to have a range of up to 40 miles with the speed of 70 Mbps or more.**

TCP/IP & INTERNET

- TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols **used to interconnect network devices on the internet.**
- TCP/IP is also used as a communications protocol **in a private computer network.**

4 LAYERS OF THE TCP/IP MODEL

APPLICATION LAYER

- The application layer provides a**pplications with standardized data exchange**. It is responsible for **handling high-level protocols, issues of representation.**
- Its protocols include **HTTP, FTP, Post Office Protocol**.

TRANSPORT LAYER

- The transport layer is responsible for **maintaining end-to-end communications across the network.**
- TCP handles **communications between hosts** and provides flow control, multiplexing and reliability.

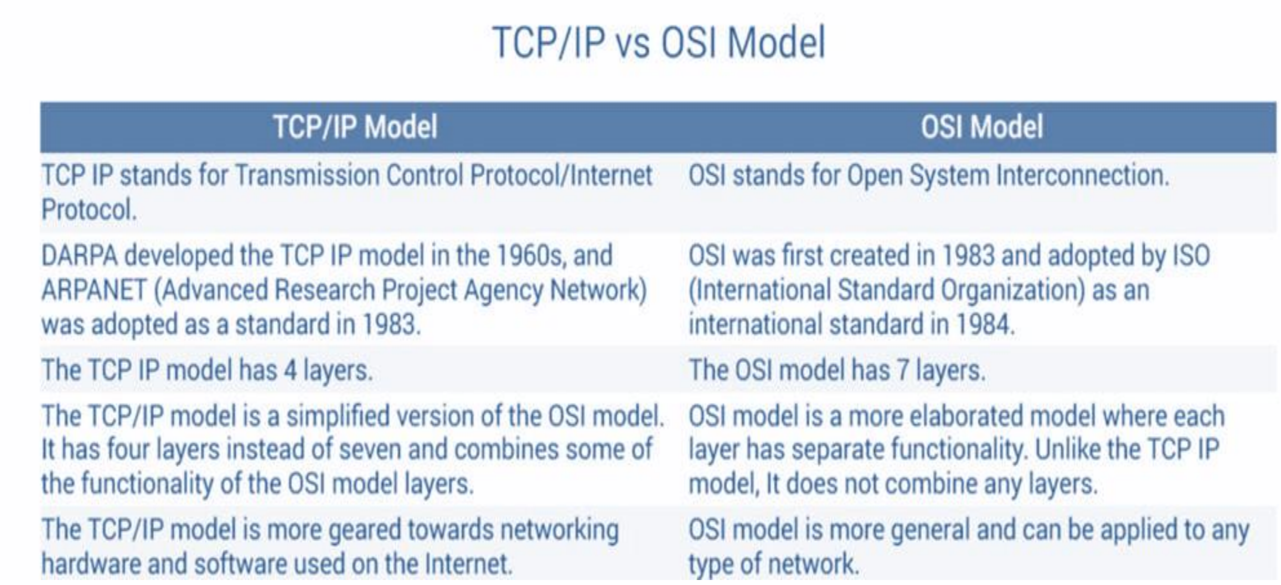
NETWORK LAYER

- The network layer, also called the **internet layer**, **deals with packets and connects independent networks** to transport the packets across network boundaries.
- The network layer protocols are IP and Internet Control Message Protocol, which is used for error reporting.

PHYSICAL LAYER

- The Physical Layer is **the lowest layer of the TCP/IP model**. It deals with **data in the form of bits**.
- This layer mainly handles **the host to host communication** in the network local area networks and Address Resolution Protocol.

COMPARISON OF TCP/IP MODEL WITH OSI MODEL



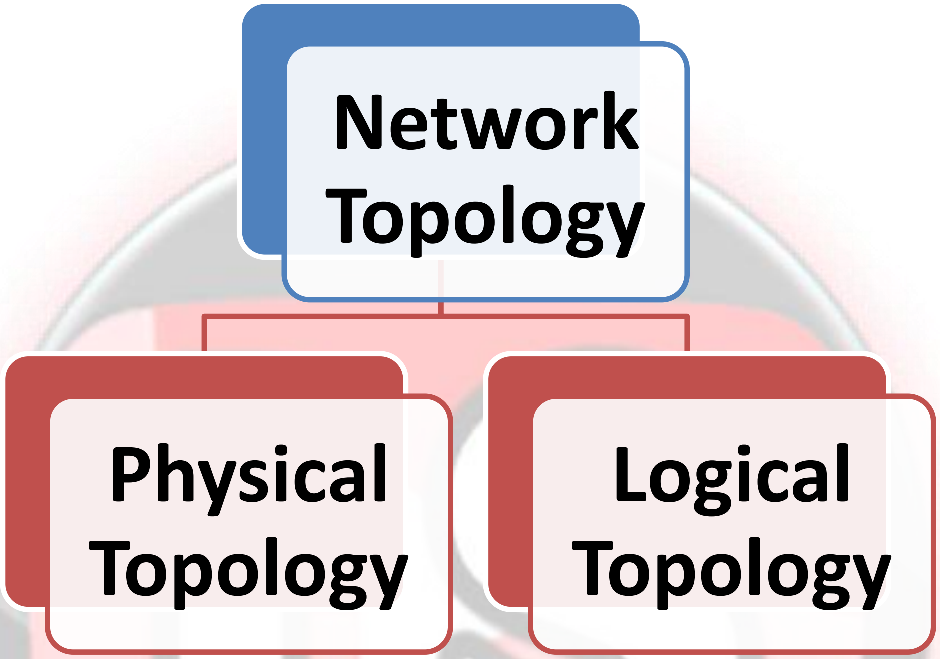
TCP/IP vs OSI Model

TCP/IP Model	OSI Model
TCP IP stands for Transmission Control Protocol/Internet Protocol.	OSI stands for Open System Interconnection.
DARPA developed the TCP IP model in the 1960s, and ARPANET (Advanced Research Project Agency Network) was adopted as a standard in 1983.	OSI was first created in 1983 and adopted by ISO (International Standard Organization) as an international standard in 1984.
The TCP IP model has 4 layers.	The OSI model has 7 layers.
The TCP/IP model is a simplified version of the OSI model. It has four layers instead of seven and combines some of the functionality of the OSI model layers.	OSI model is a more elaborated model where each layer has separate functionality. Unlike the TCP IP model, It does not combine any layers.
The TCP/IP model is more geared towards networking hardware and software used on the Internet.	OSI model is more general and can be applied to any type of network.

NETWORK TOPOLOGY

- A network topology is the **physical and logical arrangement** of **nodes and connections in a network**.

- Nodes usually include devices such as **switches, routers and software with switch and router features.**

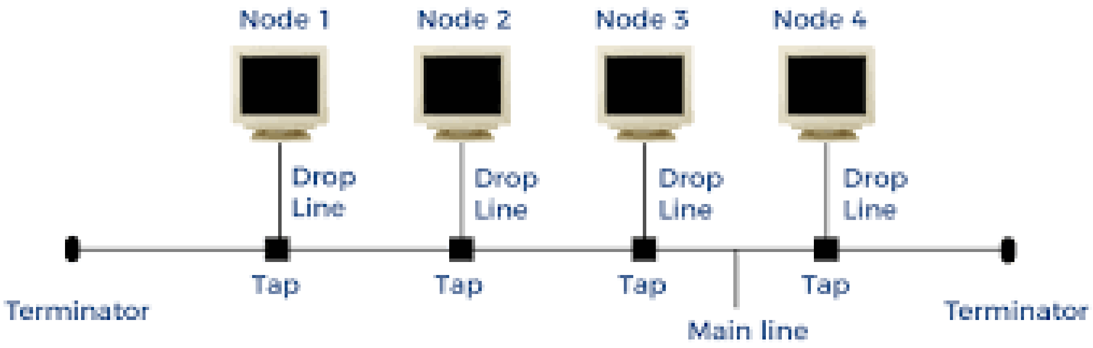


PHYSICAL TOPOLOGY

The physical topology of a network is the **actual geometric layout of workstations.**

Types of Physical Topology

Bus Network Topology
In this topology **every workstation is connected to a main cable called the bus** and each workstation is directly connected to every other workstation in the network.



Bus Topology

Advantages

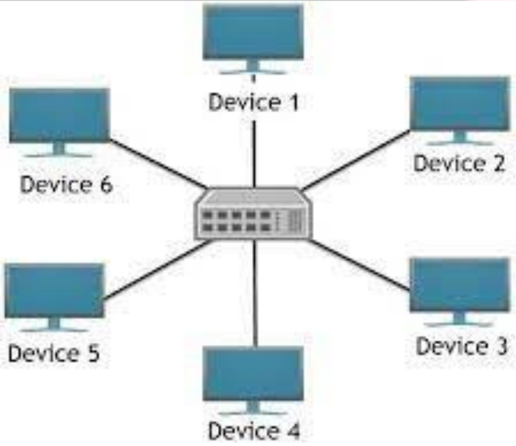
- **Easy to connect a** computer or peripheral to a linear bus.
- Requires **less cable length** than a star topology.

Disadvantages

- Entire **network shuts down** if there is a **break in the main cable**.
- **Terminators** are required at **both ends of the backbone cable**.
- Difficult to **identify the problem** if the entire network shuts down.

Star Network Topology

- In the star network topology, there is a **central computer or server to which all the workstations are directly connecte**d.
- Every workstation is **indirectly connected** to every other through the central computer.



Advantages

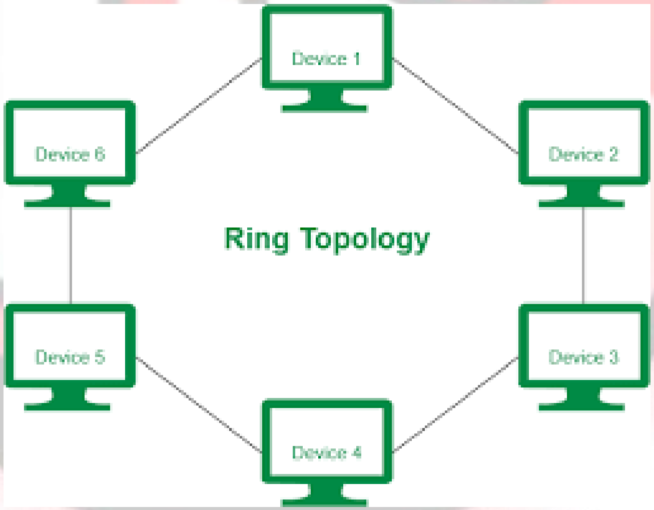
- Easy to install and wire.
- **No disruptions** to the network when **connecting or removing devices.**
- Easy to **detect faults and to remove parts**.

Disadvantages

- Requires **more cable length than a bus topology**.
- More **expensiv**e than linear bus

Ring Network Topology

- In this the workstations are **connected in a closed loop configuration.** Adjacent pairs of workstations are directly connected.
- Other pairs of **workstations are indirectly connected**, the data passing through **one or more intermediate nodes**.



Advantages

- This type of network **topology is very organized**. This helps to reduces chances of collision.
- There is no need for **network server** to control the connectivity between workstations.
- Each computer has **equal access to resources**.

Disadvantages of Ring Topology

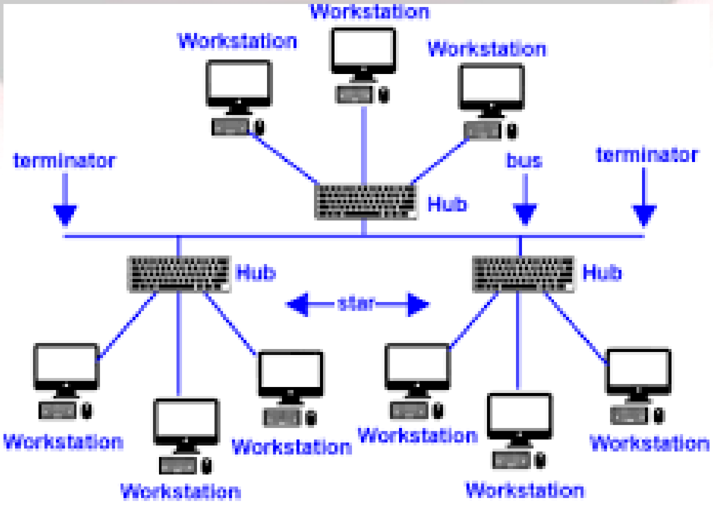
- Each packet of data must **pass through all the computers** between **source and destination**.
- If **one workstation or port goes down**, the entire network gets affected.
- Network is **highly dependent on the wire** which connects different components.

Mesh Network Topology

- This topology employs **either of two schemes**, called **full mesh and partial mesh**.
- In the full mesh topology, each workstation is **connected directly to each of the others.**
- In the **partial mesh topology, some workstations are connected to all the others**, and some are **connected only to those other nodes with which they exchange the most data.**

Tree Network Topology

It uses **two or more-star networks connected together**. The central computers of the star networks are connected to a main bus. Thus, a tree network is a bus network of star networks.

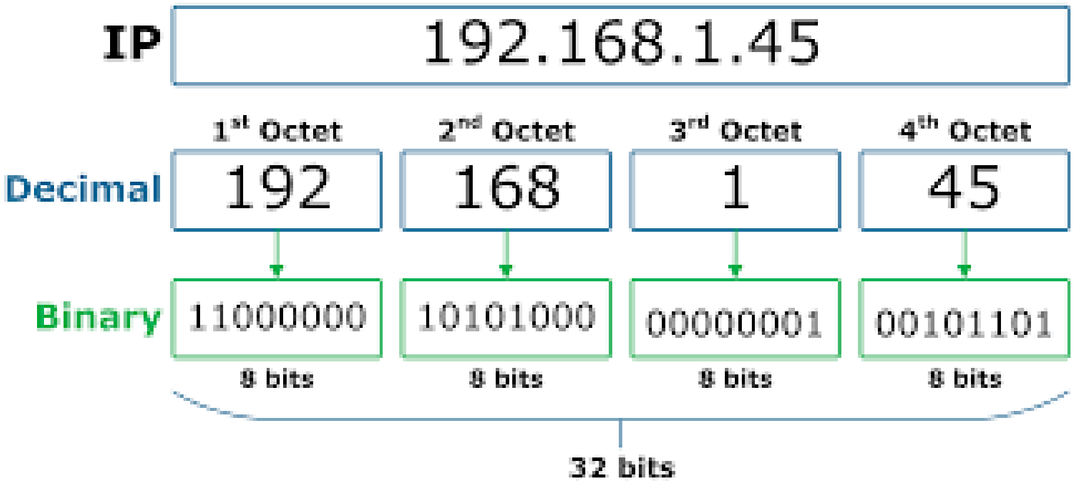


LOGICAL TOPOLOGY

A logical topology is a concept in networking that defines the architecture of the **communication mechanism for all nodes in a network.**

IP ADDRESSING

- An IP (Internet Protocol) address is a **unique identifier for a node or host connection on an IP network.**
- Every IP address consists of **two parts**, one **identifying the network and one identifying the node**.



IPv4 addresses

- IP stands for **Internet Protocol and v4 stands** for Version Four (IPv4). IPv4 was the primary version brought into action for **production in 1983**.
- IP version four addresses are **32-bit integers** which will be expressed in decimal notation.

Address Classes of IPv4

Class	Address Range	Supports
Class A-	1.0.0.1 to 126.255.255.254	Large networks with many devices

Class B-	128.1.0.1 to 191.255.255.254	Medium-sized networks.
Class C-	192.0.1.1 to 223.255.254.254	Small networks (fewer than 256 devices)
Class D-	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E-	240.0.0.0 to 255.255.255.254	Reserved for R&D

Private Subnets

- There are three IP network **addresses reserved for private networks.** The addresses are 10.0.0.0/8, **172.16.0.0/12,** and **192.168.0.0/16.**
- They can be used by anyone setting up internal IP networks, such as a lab or home LAN behind a NAT (Network Address Translator) or proxy server or a router.

IPv6 addresses

- This new generation of the Internet Protocol was eventually named **Internet Protocol Version 6 (IPv6) in 1995**.
- The address size was increased **from 32 to 128 bits (16 octets**

DIFFERENCE BETWEEN IPv 4 AND IPv6

IPv4	IPv6
The size of an address in IPv4 is 32 bits	The size of an address in IPv6 is 128 bits
IPv4 header has 20 bytes	IPv6 header is the double, it has 40 bytes
IPv4 header has many fields (13 fields)	IPv6 header has fewer fields, it has 8 fields.

IPv4 is subdivided into classes <A-E>.	IPv6 is classless. IPv6 uses a prefix and an Identifier ID known as IPv4 network
IPv4 address uses a subnet mask.	IPv6 uses a prefix length.
IPv4 has no built-in security. Encryption and authentication are optional	IPv6 has a built-in strong security - Encryption - Authentication