Computer Science By SAMPAT LILER

These complete notes have been made for class 12th board computer science exam.

10.Computer Network

Introduction to Computer Networks

In today's world, everything is interconnected through digital communication. A **network** is a system where two or more entities (computers, devices, or people) are linked together for the purpose of sharing resources and information. Examples of networks in daily life include:

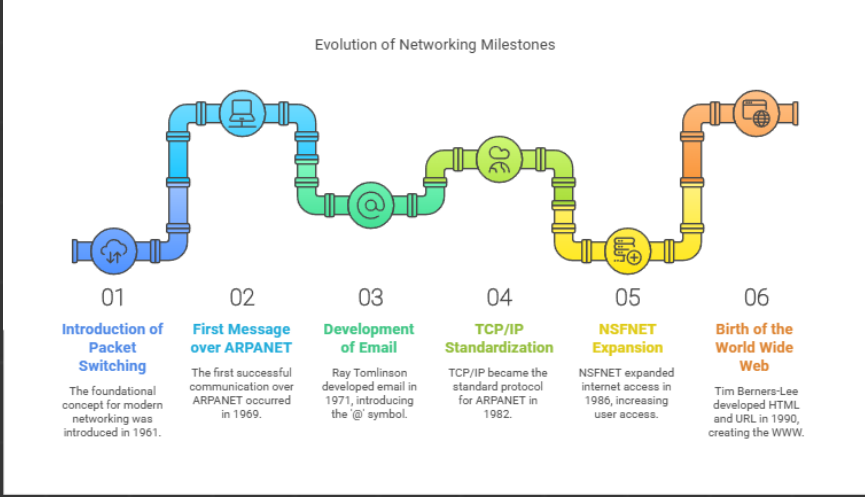
- **Social Networks**: Platforms like Facebook, Twitter, and Instagram where people interact.
- **Mobile Networks**: Telecommunication systems that enable calling and internet access.
- **Computer Networks**: A system where multiple computing devices share data and resources.
- **Airline, Railway, and Banking Networks**: Large-scale systems used for ticketing, reservations, and transactions.

A **computer network** consists of two or more computing devices that are interconnected. These connections enable sharing of resources such as files, printers, and internet access. Networks can vary in size from small (two computers connected in a room) to large (millions of connected devices across the globe). Common devices used in networks include **servers, desktops, laptops, smartphones,** and **networking devices** like switches and routers.

Evolution of Networking

The concept of networking started in the **1960s** with a project by the **Advanced Research Projects Agency Network (ARPANET)** under the **U.S. Department of Defense**. The goal was to connect different research institutions for collaboration. The first successful communication occurred between the **University of California, Los Angeles (UCLA)**, and **Stanford Research Institute (SRI)**. Over the years, advancements in networking led to the development of the modern Internet. Important milestones include:

- **1961**: The concept of packet switching (foundation of modern networking) was introduced.
- **1969**: The first message was sent over ARPANET.
- **1971**: **Email** was developed by Ray Tomlinson; the '@' symbol was introduced to separate user names and domain names.
- **1982**: **TCP/IP (Transmission Control Protocol/Internet Protocol)** became the standard protocol for ARPANET.
- **1986**: The **National Science Foundation (NSFNET)** expanded internet access to more users.
- **1990**: **Tim Berners-Lee** developed **HTML (HyperText Markup Language)** and **URL (Uniform Resource Locator)**, leading to the birth of the **World Wide Web (WWW)**.
- **1997**: The first version of **Wi-Fi (802.11 standard)** was introduced, allowing wireless communication.



Types of Networks

Networks are categorized based on their **geographical coverage** and **data transfer speed**:

Personal Area Network (PAN)

- Definition: A PAN is the smallest type of network, designed to connect personal devices within a short range (typically within 10 meters).
- Example: A Bluetooth connection between a smartphone and a laptop, or a USB connection between a printer and a PC.
- Technologies Used:
  - Bluetooth – Short-range wireless communication technology.
  - Infrared (IR) – Used in older remote controls and some wireless connections.
  - USB (Universal Serial Bus) – Wired connection for transferring data.
- Usage:
  - Connecting wireless headsets, smartwatches, or fitness trackers.
  - Transferring files between devices via Bluetooth.

Local Area Network (LAN)

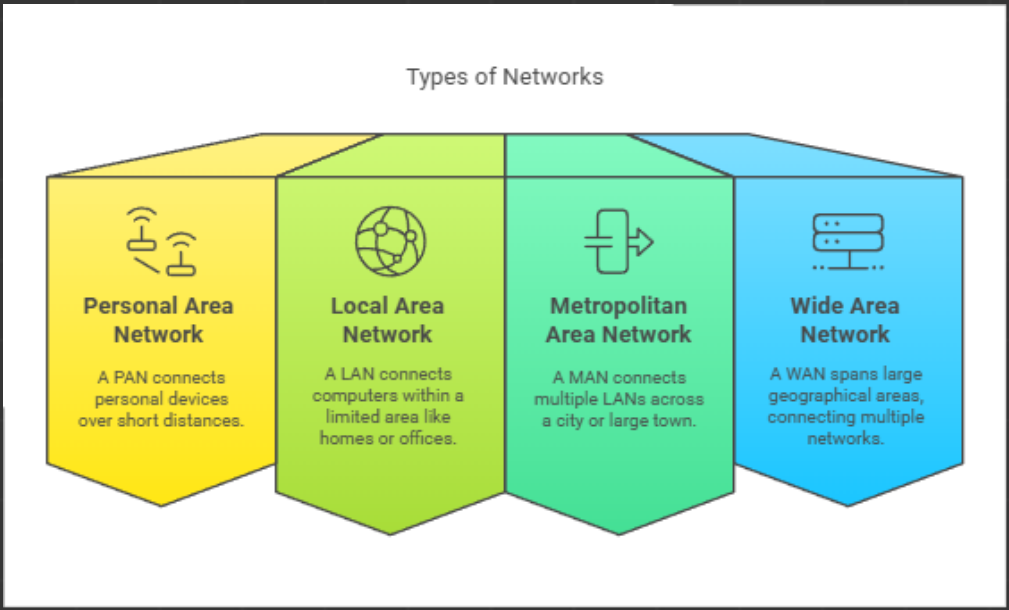
- Definition: A LAN covers a small area, such as an office, school, or home. It enables fast communication between computers and devices.
- Example: A network inside a school connecting all computers in a lab.
- Technologies Used:
  - Ethernet (IEEE 802.3) – A wired communication standard for high-speed networking.
  - Wi-Fi (IEEE 802.11) – Wireless LAN technology allowing mobile device connectivity.
  - Switches & Routers – Used for managing and directing data in a LAN.
- Characteristics:
  - High-speed data transfer (up to 1 Gbps or more).
  - Limited geographical coverage (a few hundred meters).
  - Can be wired or wireless (WLAN).
- Usage:
  - Office networking for sharing printers, files, and internet access.
  - Connecting multiple computers in a cyber café or home network.

Metropolitan Area Network (MAN)

- Definition: A MAN connects multiple LANs within a city or large town, usually maintained by telecom providers or ISPs. It extends up to 30–40 km.
- Example: A city-wide Wi-Fi network or cable TV network.
- Technologies Used:
  - Fiber Optic Cables – Used for high-speed data transmission over long distances.
  - Microwave Links – Wireless transmission of data over city areas.
  - Coaxial Cables – Used in cable television networks.
- Characteristics:
  - Covers an entire city or district.
  - Higher bandwidth than LAN but lower than WAN.
  - Typically managed by ISPs or large organizations.
- Usage:
  - Broadband internet service providers (ISP) offering city-wide coverage.
  - Campus-wide networking in universities or government organizations.

Wide Area Network (WAN)

- Definition: A WAN spans large geographical areas, often across countries or continents, and connects multiple LANs and MANs. The Internet is the largest WAN.
- Example: The banking network connecting ATMs nationwide or multinational company networks.
- Technologies Used:
    - Satellite Communication – Used for long-distance communication.
    - Optical Fiber – High-speed data transfer over thousands of kilometers.
    - Leased Lines & MPLS (Multiprotocol Label Switching) – Used for secure business communications.
- Characteristics:
    - Covers thousands of kilometers or even globally.
    - Slower speeds compared to LAN/MAN due to long distances.
    - Managed by telecom providers and ISPs.
- Usage:
    - Global corporate networks connecting offices worldwide.
    - Internet services connecting billions of devices.
    - Online banking, cloud computing, and remote working.



Network Devices

Networking devices help in data transmission and network management. Some common devices include:

Repeater

A digital signal can only travel so far down a cable until it degrades. This gradual weakening is referred to as attenuation rate. A repeater operating at the OSI model's physical layer (Layer 1) is a powered device that reenergizes the signal to keep traveling further. Dedicated repeaters are rarely used today, as powered hubs, switches, and routers do the job of a repeater. However, repeaters are occasionally employed to extend the range of remote wireless access points.[Two Ports Device]

Hub

A network hub is an essential multiport device that connects multiple Ethernet devices into a single broadcast network segment, which makes them prone to traffic congestion. There are three types of Hub:

Passive hub: No power source is needed to connect devices without amplification.

Active hub: This hub amplifies incoming signals before broadcasting and requires external power. Thus, it acts as a repeater.

Intelligent hub: Includes network management, monitoring, and diagnostic features.

Once widespread, hubs are now rarely used as switches have replaced them. Like repeaters, hubs operate at the OSI model's physical layer (Layer 1).

Bridge

While a hub connects multiple devices, a network bridge connects two or more network segments and filters the traffic between them. Their role is to isolate local segment traffic and reduce traffic congestion for better network performance. A local bridge connects two or more network segments within the exact physical location or LAN. In contrast, a remote bridge connects network segments that are geographically separated, often over a WAN link.

There are two types of bridges: -

- Transparent bridges
- Source bridges

Transparent bridges build and maintain a MAC address table by examining incoming frames' source addresses and making forwarding decisions by checking the destination MAC address against this table.

Source bridges used a different approach and were commonly used with token ring networks, which are virtually obsolete. Bridges operate at the OSI model's data link layer (Layer 2). You will most likely never work with either type of bridge today.

Routers

The main job of a router is to direct traffic. Routers transfer packets to their destinations by charting a path through interconnected networking devices using different network topologies. They are intelligent devices that store information about their connected networks. Routers commonly use access control lists (ACLs) to filter traffic; some can even serve as packet-filtering firewalls.

Routers also divide internal networks into two or more subnetworks and can be connected internally to other routers, creating zones that operate independently. Routers establish communication by maintaining tables about destinations and local connections. A router also contains information about the routers they are connected to and uses this information to forward packets to any destination it doesn't know about. Routers operate at the OSI model's network layer (Layer 3). There are two types of router:

- Static Router
- Dynamic Router

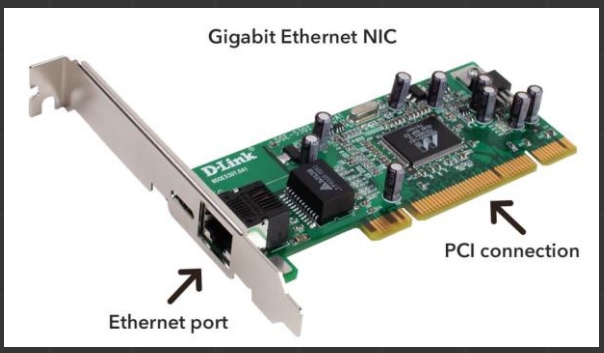
Static Router -
A static router uses manually configured routes to direct network traffic to ensure consistent, predefined data-pack paths without automatically adjusting to network changes. They are ideal for smaller networks.

Dynamic Router -
A dynamic router automatically communicates with other dynamic routers to modify its routing table based on real-time network conditions. It uses dynamic routing protocols like OSPF, RIP, or BGP to exchange information about network topology and link states with other routers. These protocols enable routers to discover optimal paths, adapt to network changes, and reroute traffic efficiently. Dynamic routers continuously update their routing tables, allowing automatic failover and load balancing. They can quickly respond to network failures or congestion by finding alternative routes. This flexibility makes them ideal for large, complex networks where manual configuration would be impractical.

Gateway -
A gateway is a network device that establishes an intelligent connection between a local network and external networks with completely different structures i.e. it connects two dissimilar networks. In simple terms, it is a node on a network that serves as an entrance to another network.
The computers that control traffic within your company's network or at your local Internet Service Provider (ISP) are gateway nodes. A network gateway can be implemented completely in software, completely in hardware, or as a combination of both. In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. Here a proxy server is a node that is not actually a server but just appears to be so and a firewall is a system designed to prevent unauthorized access to or from a private network. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet. It expands the functionality of the router by performing data translation and protocol conversion. You will sometimes see the term default gateway on network configuration screens in Microsoft Windows. In computer networking, a default gateway is the device that passes traffic from the local subnet to devices on other subnets. The default gateway often connects a local network to the Internet, although internal gateways for local networks also exist.

Network Interface Card
Any network-connected device includes a Network Interface Card (NIC). This card provides a dedicated connection between a computer and a network and manages the data transmission and reception. It is referred to as a card, originally designed as an expansion card inserted into a slot in the motherboard. Most NICs today are integrated directly into the motherboard. They come in various types, including:
- Wired (e.g., Ethernet)
- Wireless (e.g., Wi-Fi)
- Fiber optic

NICs typically consist of several key components:
A controller for processing data
A port for cable or transceiver connection
A bus interface for connecting to the computer
A unique MAC address for identification on the network



Modems

A modem (short for modulator-demodulator) is a device that converts digital signals into analog signals of different frequencies and transmits them to a modem at the receiving location. These signals From the modem can be transmitted over telephone lines, cable systems, or other communication mediums. A modem also works to convert incoming analog signals back into digital data. They are commonly used to facilitate internet access by customers of an Internet Service Provider (ISP).

Types of Modems

There are four main types of modems:

DSL modem: Uses telephone cables and is considered the slowest connection.

Cable modem: Transmits information over TV lines faster than DSL.

Wireless modem: Connects devices using Wi-Fi networks and relies on nearby Wi-Fi signals.

Cellular modem: Allows a device to connect to the internet using a cellular network instead of Wi-Fi or fixed-line connections.

Switch

A switch is a device that is used to break a network into different subnetworks called subnet or LAN segments. This prevents traffic overloading on the network. They allow different nodes of a network to communicate directly with one another in a smooth and efficient manner. Network switches appear nearly identical to network hubs, but a switch generally contains more intelligence than a hub. We can say that a switch is an intelligent hub and is obviously more expensive than a hub. Unlike hubs, network switches are capable of inspecting data packets as they are received, determining the source and destination device of each packet, and forwarding them appropriately. By delivering messages only to the connected device intended, a network switch conserves network bandwidth and offers generally better performance than a hub.

RJ45 connector

RJ45 stands for Registered Jack 45 and is the most commonly used connector in wired networks. The jacks are mainly used to connect to the Local Area Network (LAN). It was earlier devised for telephones but is now widely used in Ethernet Networking. The 45 in RJ45 basically stands for the listing number. The width of RJ45 is usually greater than that of the telephone cables or other Registered Jacks. Compared to additional jacks the bandwidth provided by these is high and the range is usually 10 Gbps. Because of speed and enhanced security, they are used to connect personal computers to servers, routers etc. These jacks are mostly used in Star Topology.

Structure of RJ45

RJ45 has a transparent plastic structure and is an 8-pin connector. It is an 8P8C connector and the number of wires that can be connected is 8. The jacks are mostly used with Shielded Twisted Pair cables or Unshielded Twisted Pair cables. If we take a close look at the end of the Ethernet cable connected to the RJ45 we can see the 8 wires out of which 4 wires are solid coloured and 4 are strip coloured. The classification of RJ45 is done based on the wiring

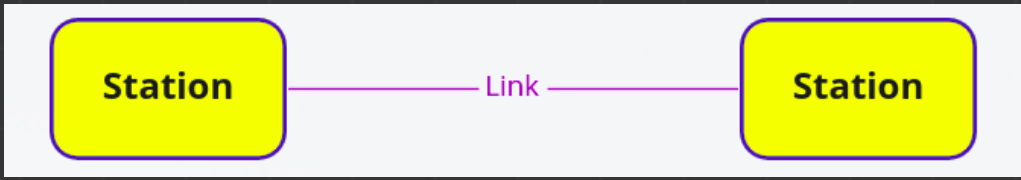
Networking Topologies

- A **network** is a set of devices(often referred to as nodes) connected by communication links.
- A **node** can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- A **link** can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.

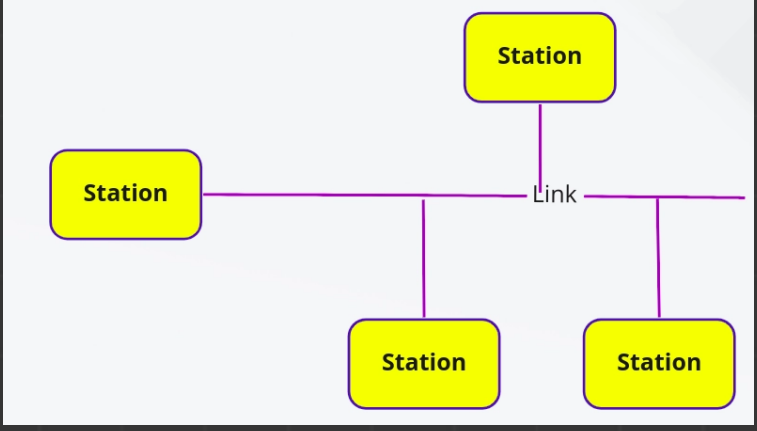
Physical Structure of a Network

Types Of Connection:

- **Point to Point Connection**:- It is a **dedicated link between two devices**. These two devices share the capacity of this link. Generally, Point to point connections uses an actual length of wire/cable to connect the two devices. There are other options also, like, microwave links, satellite links, Infrared rays from television remote to television, etc.



- **Multipoint**:- It is a connection in which more than two devices share a single link.



Topology refers to the arrangement of devices in a network. Common types include:

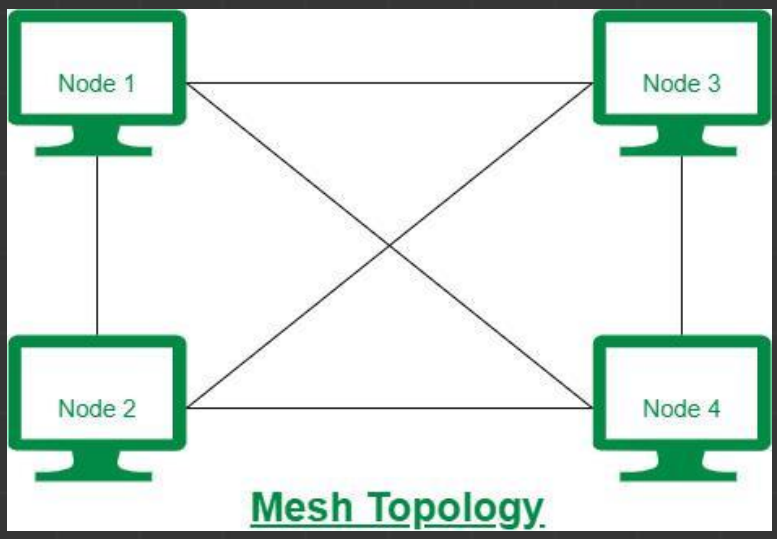
Types of Network Topology

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology. Below are various network topologies that include:

1. Mesh Topology

In Mesh Topology, every node has a dedicated point-to-point link in every other node. Such a network is called complete because, for any two devices, there is a special link and non-redundant links cannot be added to the main network.

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. There are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = **N * (N-1).**
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.



Mesh Topology

There are two types of Mesh topologies:

- **Full Mesh Topology :** All the nodes within the network are connected with every other If there are n number of nodes during a network, each node will have an n-1 number of connections.
- **Partial Mesh Topology :** The partial mesh is more practical as compared to the full mesh. In a partially connected mesh, all the nodes aren't necessary to be connected with one another during a network.

Advantages of Mesh Topology

- Easy fault identification and isolation.
- Failure during a single device won't break the network.
- There is no traffic problem as there is a dedicated point to point links for every computer.
- It provides high privacy and security.
- Data transmission is more consistent because failure doesn't disrupt its processes.
- Adding new devices won't disrupt data transmissions.
- This topology has robust features to beat any situation.
- A mesh doesn't have a centralized authority.

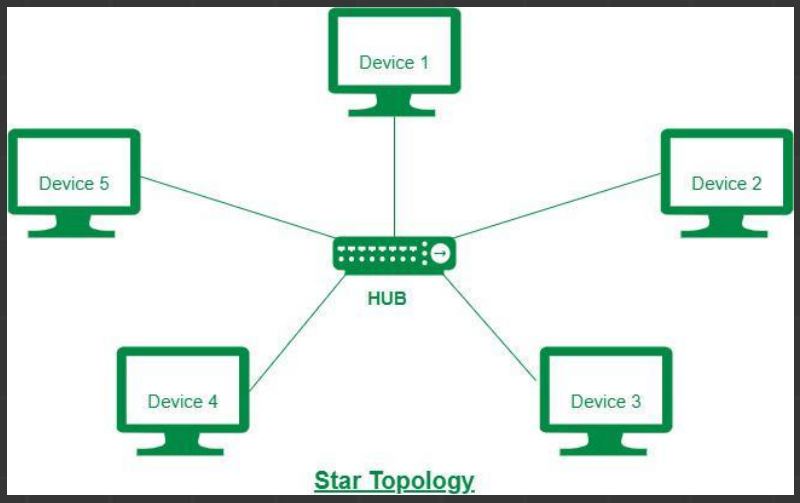
Disadvantages of Mesh Topology

- Each node must have an interface for every other node.
- There is only a limited number of I/O ports in a computer.
- The cost to implement mesh topology is high
- There is a high risk of redundant connections.
- Maintenance needs are challenging with a mesh topology.

2. Star Topology

In a Star Topology, all the nodes (PCs, printers and peripherals) are connected to the central server. It has a central connection point, like a hub or switch. In star topology .each device is connected with central hub.

Advantages of Star Topology



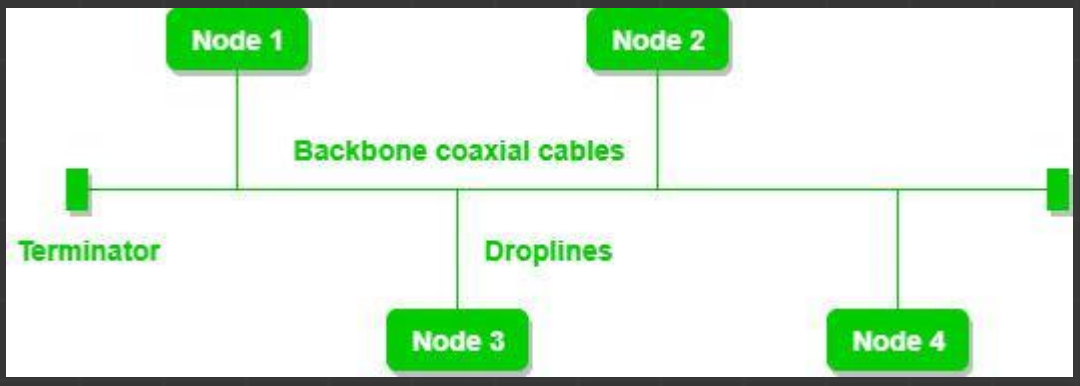
- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Disadvantages of Star Topology

- Star networks can require more cable length than a linear topology.
- More expensive cabling.
- Performance is based on the single concentrator i.e. hub.

3. Bus Topology

In bus topology, all stations are attached to the same cable. In the bus network, messages are sent to both directions from a single point. In the bus topology, signals are broadcast to all stations. Each computer checks the address on the signal (data frame) as it passes along the bus. If the signal's address matches that of the computer, the computer processes the signal. If the address doesn't match, the computer takes no action and travels down the bus.



Advantages of Bus Topology

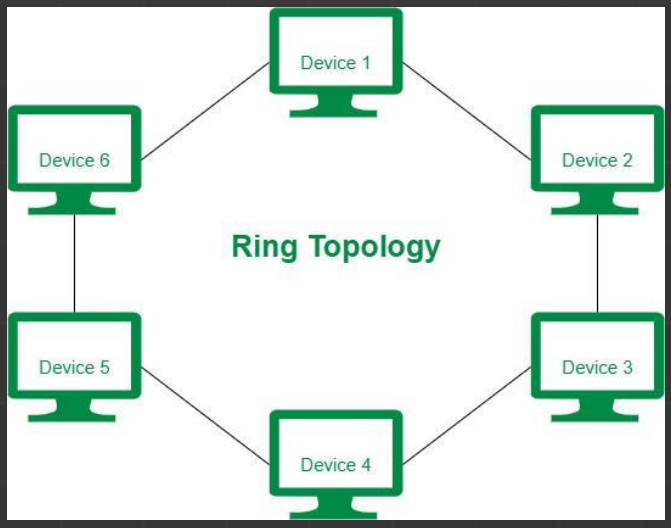
- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.

Disadvantages of Bus Topology

- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

4. Ring Topology

All the nodes in a Ring Topology are connected in a closed circle of cable. Messages that are transmitted travel around the ring unit they are addressed to, the signal being refreshed by each node. In a ring network, every device has exactly two neighbors for communication purposes.



The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Advantages of Ring Topology

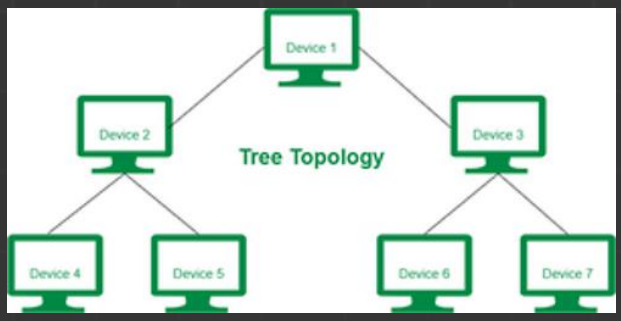
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology
- Less secure.

5. Tree Topology

In tree topology nodes are connected in a hierarchical structure to form a tree. There is a root node in tree topology and the remaining nodes are considered as child nodes, basically it is a combination of star and bus topology. The central bus works as a communication pathway, and each star-configured network represents a level in the tree. In tree topology, a hierarchy is formed by the branching cable having no loops that connect the root with all other nodes for communication.



Advantages of Tree Topology

- Security is high in Tree Topology
- Tree Topology is more reliable
- Tree topology is more scalable
- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.

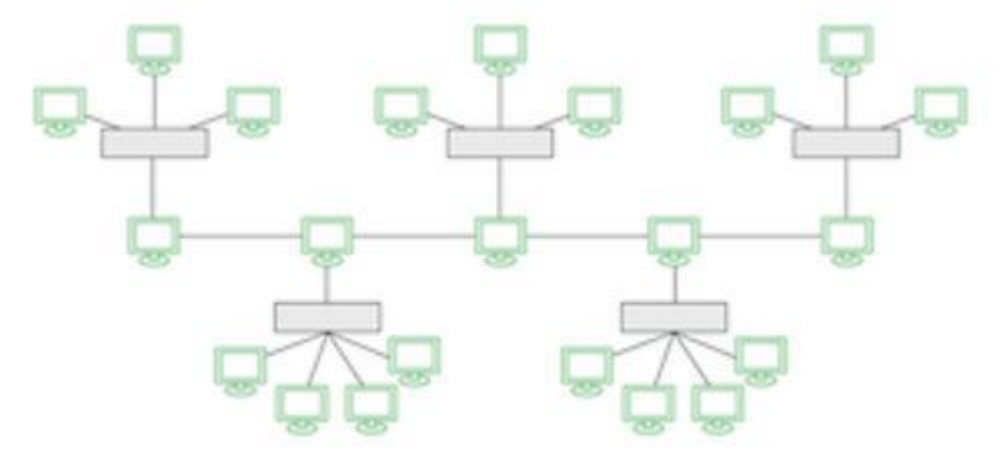
- We can add new devices to the existing network.
- **Error detection** and **error correction** are very easy in a tree topology.

Disadvantages of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

6. Hybrid Topology

Hybrid topology is the combination of two or more types of topology, they arise from the integration of multiple network topologies that is why called Hybrid Network Topology.



Advantages of Hybrid Topology

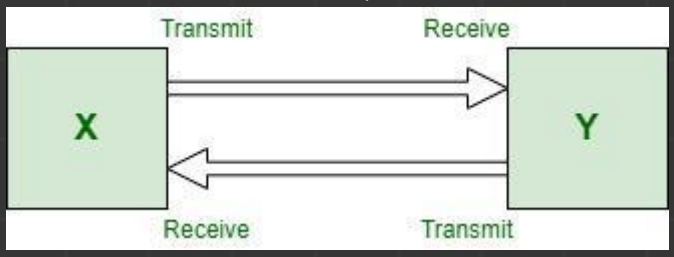
- Hybrid Topology provides more flexibility than others topologies.
- Hybrid topology is more robust than the other.
- Hybrid Topology provides optimized performance

Disadvantage of Hybrid Topology

- It is challenging to design the architecture of the Hybrid Network.
- **Hubs** used in this topology are very expensive.
- The infrastructure cost is very high as a hybrid network requires a lot of cabling and network devices.

7. Point to Point Topology

Point-to-Point Topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Advantages of Point to Point Topology

- P2P networks are highly efficient as they allow for direct communication between two devices without any intermediate devices or network components.
- P2P networks are relatively more secure than other topologies as they do not rely on intermediate devices that can be compromised or attacked.

- P2P networks are easy to configure and require minimal management or administration.

Disadvantages of Point to Point Topology

- P2P networks are not scalable as adding new devices requires establishing a separate link between each new device and the existing network, which can be time-consuming and expensive.
- P2P networks can be difficult to maintain as each device has to be managed separately.
- P2P networks do not provide redundancy, which can be a problem if a link fails or a device goes offline. with a dedicated communication connection between two systems.

Network Addressing -

1. MAC Address (Media Access Control Address)

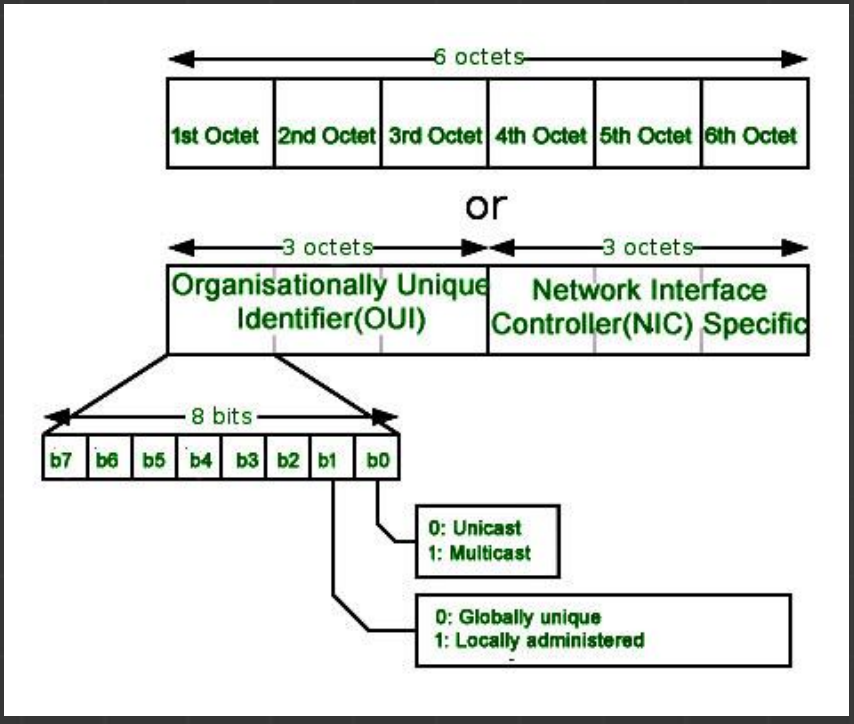
A **MAC address** is a unique, permanent hardware address assigned to a device's Network Interface Card (NIC). It operates at the **Data Link Layer (Layer 2) of the OSI model** and is essential for local network communication within a LAN.

Architecture and Structure

- A MAC address is a **48-bit (6-byte) hexadecimal address** written in the format:
  - 00:1A:2B:3C:4D:5E (colon-separated)
  - 00-1A-2B-3C-4D-5E (hyphen-separated)
- The **first 24 bits (OUI - Organizationally Unique Identifier)** are assigned by the IEEE to the manufacturer.
- The **last 24 bits** are assigned uniquely by the manufacturer to the device.

Size and Address Range

- **Size:** 48 bits (6 bytes)
- **Address Range:**
  - Since it is **48 bits long**, the total number of possible MAC addresses = **248=281,474,976,710,6562^{48} = 281,474,976,710,656 (approx. 281 trillion devices)**.



Types of MAC Addresses

1. **Unicast MAC Address:** Identifies a single device. The least significant bit of the first byte is **0**.
2. **Multicast MAC Address:** Used to send data to multiple devices in a group. The least significant bit of the first byte is **1**.
3. **Broadcast MAC Address:** FF:FF:FF:FF:FF:FF, used to send data to all devices in a network.

Explanation

- MAC addresses ensure that data packets within a LAN reach the correct device.
- Switches use MAC addresses to forward frames efficiently.
- MAC addresses do **not** change unless the NIC is replaced.

2. IP Address (Internet Protocol Address)

An **IP address** is a **logical address** assigned to a device to enable communication across networks. It operates at the **Network Layer (Layer 3) of the OSI model** and can change when a device moves to a different network.

Types of IP Addresses

There are two versions of IP addresses: **IPv4 and IPv6**.

IPv4 (Internet Protocol Version 4)

Architecture and Structure

- IPv4 is a **32-bit (4-byte) address**, written in **decimal format**, separated by dots (e.g., 192.168.1.1).
- It consists of **four octets**, where each octet is 8 bits.
- Example: 11000000.10101000.00000001.00000001 (Binary form of 192.168.1.1).

Size and Address Range

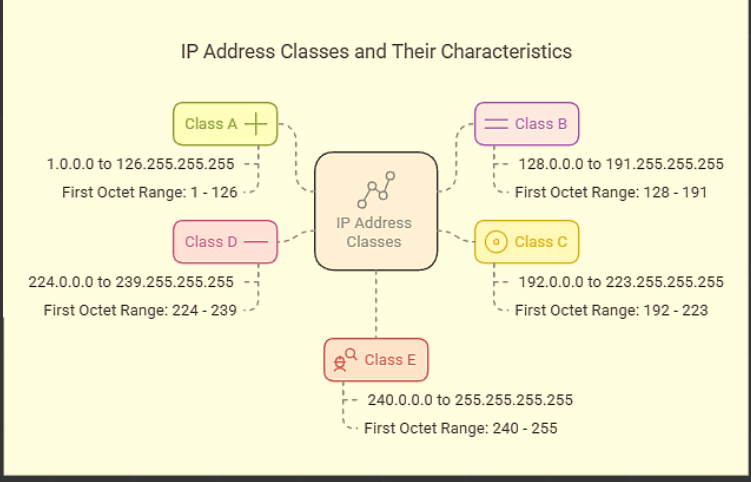
- **Size:** 32 bits (4 bytes).
- **Total Possible Addresses:**
  - 232=4,294,967,296$2^{32}$ = 4,294,967,296 (around 4.3 billion unique addresses).

Types of IPv4 Addresses

1. **Public IP Address:** Used on the internet, assigned by ISPs (e.g., 8.8.8.8).
2. **Private IP Address:** Used within local networks (e.g., 192.168.1.1).
3. **Loopback Address:** 127.0.0.1, used for testing a device's network stack.
4. **Broadcast Address:** 255.255.255.255, used for network-wide communication.
5. **Multicast Address:** 224.0.0.0 – 239.255.255.255, used for group communication.

IPv4 Address Classes and Their Ranges

Class	Starting Address	Ending Address	First Octet Range	Purpose
A	1.0.0.0	126.255.255.255	1 – 126	Large networks (Public)
B	128.0.0.0	191.255.255.255	128 – 191	Medium networks (Public)
C	192.0.0.0	223.255.255.255	192 – 223	Small networks (Public)
D	224.0.0.0	239.255.255.255	224 – 239	Multicast (Special use)
E	240.0.0.0	255.255.255.255	240 – 255	Reserved for research



IPv6 (Internet Protocol Version 6)

Architecture and Structure

- IPv6 is a **128-bit (16-byte) address**, written in **hexadecimal format**, separated by colons (e.g., 2001:db8::ff00:42:8329).
- It consists of **8 groups of 16-bit hexadecimal numbers**.
- Leading zeros can be omitted for simplification.

Size and Address Range

- **Size:** 128 bits (16 bytes).
- **Total Possible Addresses:**
  - 21282^{128} = **340 undecillion (340 x 103610^{36})**, making it virtually unlimited.

Types of IPv6 Addresses

1. **Unicast Address:** Identifies a single device.
2. **Multicast Address:** Data is sent to multiple devices.
3. **Anycast Address:** Data is sent to the nearest node in a group.

IPv6 vs IPv4 Comparison

Feature	IPv4	IPv6
Address Length	32 bits	128 bits
Address Format	Decimal (e.g., 192.168.1.1)	Hexadecimal (e.g., 2001:db8::1)
Total Addresses	4.3 billion	Virtually unlimited
NAT Required?	Yes	No (supports direct communication)
Security Features	Optional (IPSec)	Built-in IPSec

Key Differences Between MAC and IP Addresses

Feature	MAC Address	IP Address
Nature	Permanent (hardware)	Temporary (logical)
Layer	Data Link Layer (Layer 2)	Network Layer (Layer 3)
Address Type	48-bit or 64-bit	32-bit (IPv4) / 128-bit (IPv6)
Example	00:1A:2B:3C:4D:5E	192.168.1.1 (IPv4) / 2001:db8::1 (IPv6)
Function	Identifies devices within a LAN	Identifies devices across networks
Changeability	Fixed (unless NIC changes)	Changes with network movement

---

Internet, Web, and IoT

Internet

The **Internet** is a **global network** that connects **millions of computers, servers, smartphones, and other devices** worldwide. It enables communication, information sharing, and various online services.

Key Features of the Internet

- **Global Connectivity**: Anyone can access information and communicate globally.

- **Decentralized Structure**: No single entity owns the Internet; it is managed by multiple organizations like ICANN, IETF, and ISPs.
- **Data Transmission**: Uses **TCP/IP (Transmission Control Protocol/Internet Protocol)** to send and receive data.
- **Services**: Supports **email, websites, social media, cloud computing, streaming services**, etc.
- **Accessibility**: Can be accessed using **wired (fiber, DSL, Ethernet)** or **wireless (Wi-Fi, mobile networks)** connections.

How the Internet Works?

1. **Users connect** to the Internet using an ISP (Internet Service Provider).
2. Data is broken into **packets** and sent across various **network routers**.
3. The packets travel across different networks to reach the **destination device**.
4. The receiving device **reassembles** the packets to display the complete data.

Uses of the Internet

- **Communication**: Email, video calls, social media.
- **Information Access**: Search engines, online news, digital libraries.
- **Entertainment**: Streaming videos, online gaming, music.
- **E-commerce**: Online shopping, banking, digital transactions.
- **Education**: Online courses, research, digital classrooms.

World Wide Web (WWW)

The **World Wide Web (WWW)** is a **collection of interlinked web pages** that can be accessed through the **Internet** using a web browser. It was developed by **Tim Berners-Lee** in **1990**.

Components of the WWW –

- **Web Pages**: Documents written in **HTML (HyperText Markup Language)** that can display text, images, videos, and links.
- **Websites**: A collection of related web pages with a common domain (e.g., www.google.com).
- **Web Browsers**: Software used to access web pages (e.g., Chrome, Firefox, Edge).
- **URLs (Uniform Resource Locators)**: The address of a webpage (e.g., https://anviraeducation.com/).
- **HTTP/HTTPS (HyperText Transfer Protocol)**: The protocol used to transfer web pages over the Internet.

How the WWW Works?

1. A user enters a **URL** in a web browser.
2. The browser sends a request to the **web server** hosting the webpage.
3. The server processes the request and sends back the web page.
4. The browser renders the webpage for the user.

Difference Between Internet and WWW

Internet	WWW
A global network of connected devices.	A system of web pages and websites accessed via the Internet.
Provides various services like email, VoIP, cloud storage.	Mainly used for accessing information through web pages.
Uses protocols like TCP/IP, FTP, SMTP, etc.	Uses protocols like HTTP, HTTPS.

Uses of the WWW

- **Information Sharing**: Websites provide news, research, blogs, and educational content.
- **Online Services**: Banking, shopping, reservations.
- **Social Networking**: Facebook, Twitter, Instagram.
- **Cloud Computing**: Google Drive, OneDrive, Dropbox.

HTML stands for Hypertext Markup Language. It is the most basic language, and simple to learn and modify. It is a combination of both hypertext and markup language. It contains the elements that can change/develop a web page's look and the displayed contents. Or we

can say that HTML creates or defines the structure of web pages. We can create websites using HTML which can be viewed on internet-connected devices like laptops, android mobile phones, etc. It was created by Tim Berners-Lee in 1991. The first version of HTML is HTML 2.0 which was published in 1999, and the latest version is HTML 5. We can save HTML files with an extension .html.

What is Hypertext?

Text that is not restricted to a sequential format and that includes links to other text is called Hypertext. The links can connect online pages inside a single or different website.

What is Markup Language?

Markup Language is a language that is interpreted by the browser and it defines the elements within a document using "tags". It is human-readable, which means that markup files use common words rather than the complicated syntax of programming languages.

What is URL (Uniform Resource Locator) ?

A URL or Uniform Resource Locator is a Unique identifier that is contained by all the resources available on the internet. It can help to locate a particular resource due to its uniqueness. It is also known as the web address. A URL consists of different parts like protocol, domain name, etc. The users can access the URLs by simply typing them inside the address bar or by clicking any button or link web page.

Example URL:
https://www.anviraeducation.com/

Structure of a URL

A URL starts with a protocol followed by the name of the resource that has to be accessed. URL uses the protocols as the primary access medium to access the domain or subdomain specified after that wherever the resource is located. It uses multiple protocols like HTTP (Hypertext Transfer Protocol), HTTPS Protocol (Secured HTTP), mailto for emails, FTP (File Transfer Protocol) for files, and TELNET to access remote computers. Mostly the protocol names are specified using the colons and the double forward slashes, but the mailto protocol is specified using the colons only.

What is HTTP?

HTTP (HyperText Transfer Protocol) is a protocol used for communication between web browsers and web servers. It defines how messages are formatted and transmitted, as well as how web servers and browsers should respond to various commands.

Key Features of HTTP:

Stateless: Each request is independent, meaning the server does not remember previous interactions.
Uses TCP (Transmission Control Protocol): Typically runs on port 80.
Text-Based Protocol: Requests and responses are human-readable.
Insecure Communication: Data is transmitted in plain text, making it vulnerable to hackers

What is HTTPS?

HTTPS (HyperText Transfer Protocol Secure) is an extension of HTTP that includes SSL/TLS (Secure Socket Layer / Transport Layer Security) encryption. This ensures secure data transmission between the client and the server.

Key Features of HTTPS:

Secure Communication: Encrypts data, preventing eavesdropping and data tampering.
Uses SSL/TLS Encryption: Provides authentication and data integrity.
Runs on Port 443: Instead of port 80 used by HTTP.
Required for Secure Transactions: Used for banking, login forms, and sensitive data transfers.

---

3. Internet of Things (IoT)

The **Internet of Things (IoT)** refers to **connecting everyday objects** (like smartphones, home appliances, cars, industrial machines) to the **Internet**, allowing them to collect and exchange data.

Key Features of IoT

- **Interconnectivity**: Devices communicate with each other via the Internet.
- **Automation**: Reduces human intervention by enabling smart functionalities.
- **Real-time Data Processing**: Devices collect and analyze data instantly.
- **Remote Control**: Devices can be controlled from anywhere using mobile apps.

How IoT Works?

1. **Sensors and devices** collect data from the environment.
2. The data is sent to **cloud servers** via the Internet.
3. The data is processed and analyzed using **AI (Artificial Intelligence) and ML (Machine Learning)**.
4. The processed information is sent back to the **IoT device**, which performs an action (e.g., turning on a smart bulb).

Examples of IoT Devices

- **Smart Homes**:
  - Smart TVs, Alexa, Google Home.
  - Smart thermostats (e.g., Nest) adjust temperature automatically.
  - Smart locks and security cameras for home safety.
- **Healthcare**:
  - Wearable devices (smartwatches) monitor heart rate, sleep, and fitness.
- **Smart Cities**:
  - Smart traffic lights, pollution monitoring, waste management systems.
- **Industrial IoT (IIoT)**:
  - Automated factories use sensors for machine monitoring.

Advantages of IoT

- **Convenience**: Automates routine tasks.
- **Energy Efficiency**: Smart devices reduce power consumption.
- **Improved Safety**: IoT-based security systems enhance protection.
- **Better Healthcare**: Remote patient monitoring improves medical treatment.

Challenges of IoT

- **Security Risks**: Hackers can exploit vulnerabilities in smart devices.
- **Data Privacy Issues**: IoT devices collect large amounts of personal data.
- **High Initial Cost**: Implementing IoT in industries and homes can be expensive.

Domain Name System (DNS)

- **Domain Name System (DNS)**: The **Domain Name System (DNS)** is a system used to translate human-friendly domain names (like www.google.com) into IP addresses (like 142.250.183.4). Since computers use IP addresses to communicate, DNS acts like a **phonebook of the internet**, allowing users to access websites using easy-to-remember names instead of numeric addresses.
- **DNS Server**: DNS Server Instead of remembering IP addresses, we assign a domain name to each IP. But, to access a web resource, a browser needs to find out the IP address corresponding to the domain name entered. Conversion of the domain name of each web server to its corresponding IP address is called domain name resolution. It is done through a server called DNS server. Thus, when we enter a URL on a web browser, the HTTP protocol approaches a computer server called DNS server

to obtain the IP address corresponding to that domain name. After getting the IP address, the HTTP protocol retrieves the information and loads it in our browser.

A DNS server maintains a database of domain names and their corresponding IP addresses. To understand how the domain name resolution works, we have to understand how and where the DNS servers are kept. The DNS servers are placed in hierarchical order. At the top level, there are 13 servers called root servers. Then below the root servers there are other DNS servers at different levels. A DNS server may contain the IP address corresponding to a domain or it will contain the IP address of other DNS servers, where this domain entry can be searched.