UNIT – 1

PART - 1: INTRODUCTION

Introduction to Computer Network:

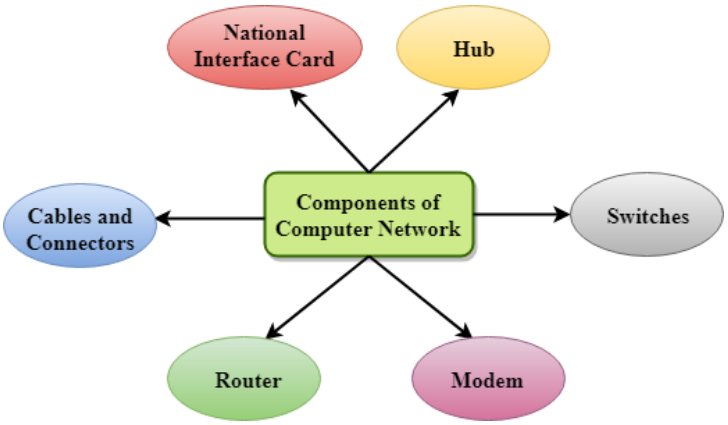
What is Computer Networking?

A computer network is a collection of computers capable of transmitting, receiving, and exchanging voice, data, and video traffic. Because of the capability of computer networking, everything is becoming more automated and capable of communicating and managing itself.

Definition – A group of computers which are connected to each other and follow similar usage protocols for the purpose of sharing information and having communications provided by the networking nodes is called a **Computer Network**.

If there is no computer network, you will not be able to read this article by simply conducting a search on the topic and getting results in a matter of milliseconds. Because of the internet's powerful network, you can use Google and YouTube and watch other information with just a few clicks. It is possible due to computer networks.

Components Of Computer Network:



Major components of a computer network are:

NIC (National interface card):

- NIC is a hardware component used to connect a computer with another computer onto a network
- It can support a transfer rate of 10,100 to 1000 Mb/s.
- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

There are two types of NIC: wireless NIC and wired NIC.

- **Wireless NIC:** All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the **radio wave technology**.
- **Wired NIC:** Cables use the **wired NIC** to transfer the data over the medium.

Hub: A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Switches: A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

Cables and connectors: Cable is a transmission media that transmits the communication signals. **There are three types of cables:**

- **Twisted pair cable:** It is a high-speed cable that transmits the data over **1Gbps** or more.
- **Coaxial cable:** Coaxial cable resembles like a TV installation cable. Coaxial cable is more expensive than twisted pair cable, but it provides the high data transmission speed.
- **Fibre optic cable:** Fibre optic cable is a high-speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables. It is more expensive as compared to other cables, so it is installed at the government level.

Router:

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Modem:

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified in the following categories:

- Standard PC modem or Dial-up modem
- Cellular Modem
- Cable modem

Unique Identifiers of Network:

Below given are some unique network identifiers:

Hostname: Every device of the network is associated with a unique device, which is called hostname.

IP Address: IP (Internet Protocol) address is as a unique identifier for each device on the Internet. Length of the IP address is 32-bits. IPv6 address is 128 bits.

DNS Server: DNS stands for Domain Name System. It is a server which translates URL or web addresses into their corresponding IP addresses.

MAC Address: MAC (Media Access Control Address) is known as a physical address is a unique identifier of each host and is associated with the NIC (Network Interface Card). General length of MAC address is : 12-digit/ 6 bytes/ 48 bits

Port: Port is a logical channel which allows network users to send or receive data to an application. Every host can have multiple applications running. Each of these applications are identified using the port number on which they are running.

Other Important Network Components:

ARP: ARP stands for Address Resolution Protocol which helps network users to convert the IP address into its corresponding Physical Address.

RARP: Reverse Address Resolution Protocol gives an IP address of the device with given a physical address as input.

Uses Of Computer Network:

- **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- **Server-Client model:** Computer networking is used in the **server-client model**. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
- **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
- **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

Features Of Computer network:

- **Communication speed:** Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.
- **File sharing:** File sharing is one of the major advantage of the computer network. Computer network provides us to share the files with each other.
- **Back up and Roll back is easy:** Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

- **Software and Hardware sharing:** We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.
- **Security:** Network allows the security by ensuring that the user has the right to access the certain files and applications.
- **Scalability:** Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices. But it decreases the speed of the connection and data of the transmission speed also decreases, this increases the chances of error occurring. This problem can be overcome by using the routing or switching devices.
- **Reliability:** Computer network can use the alternative source for the data communication in case of any hardware failure.

Computer Network Architecture:

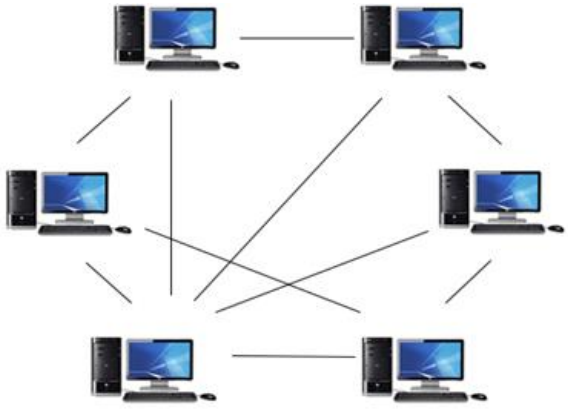
Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

The two types of network architectures are used:

1. Peer-To-Peer network
2. Client/Server network

1. Peer-To-Peer network:

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages Of Peer-To-Peer Network:

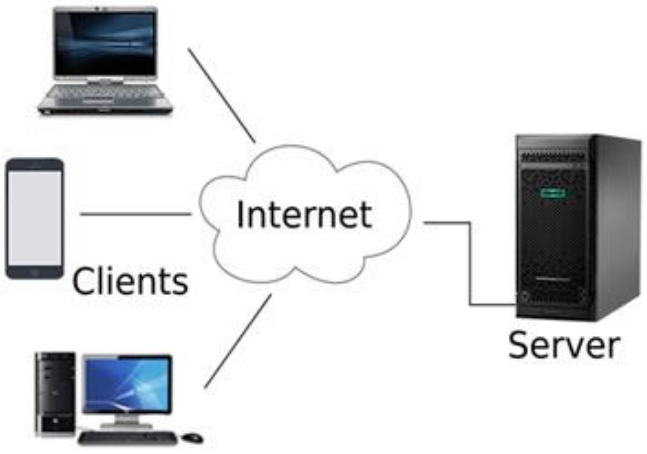
- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

2. Client/Server Network:

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages Of Client/Server network:

- A Client/Server network contains the centralized system. Therefore, we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

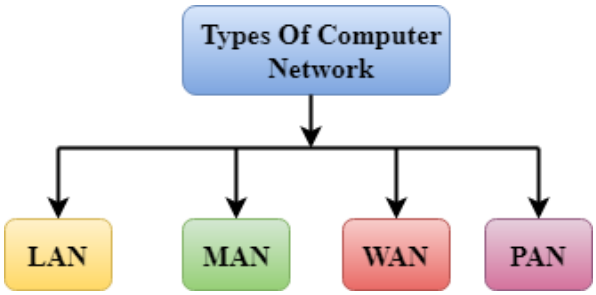
Disadvantages Of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Computer Network Types:

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



1. LAN (Local Area Network):

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.

- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

2. PAN (Personal Area Network):

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of Personal Area Network:

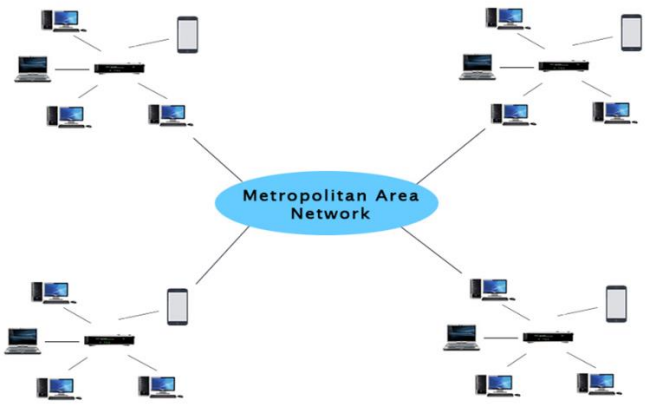
1. **Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.
2. **Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
- **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
- **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

3. MAN (Metropolitan Area Network):

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network (LAN).

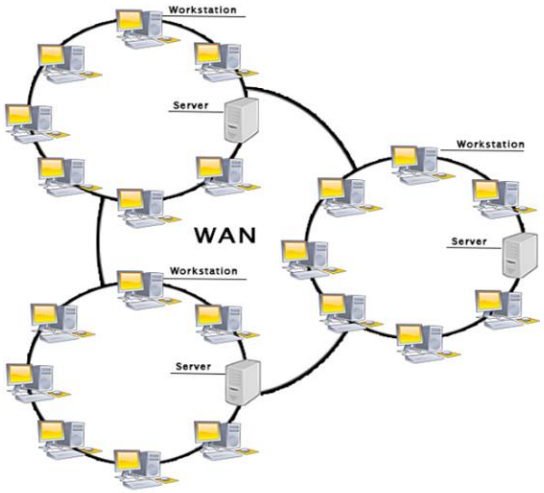


Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

4. WAN (Wide Area Network):

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.

- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, WhatsApp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

5. Internetwork:

- An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
- An internetworking uses the **internet protocol**.
- The reference model used for internetworking is **Open System Interconnection (OSI)**.

Types Of Internetwork:

1. Extranet: An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, at least it must have one connection to the external network.

2. Intranet: An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

- **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
- **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
- **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
- **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.
- **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

History and Development of Computer Networks:

The history and development of computer networks can be traced back to the mid-20th century. The evolution of computer networks has been marked by significant milestones, technological advancements, and the proliferation of communication protocols.

Here is a brief overview of the key stages in the history and development of computer networks:

1. **Early Concepts (1950s-1960s):** The concept of computer networking emerged in the late 1950s and early 1960s. One of the earliest examples was the SAGE (Semi-Automatic Ground Environment) system developed by the United States for air defense, which involved interconnected computers for radar data processing.
2. **ARPANET (1969):** The Advanced Research Projects Agency Network (ARPANET) is often considered the precursor to the modern Internet. Developed by the U.S. Department of Defense's ARPA (Advanced Research Projects Agency), ARPANET was launched in 1969 and connected four major research institutions. It used the packet-switching technique, dividing data into packets for more efficient transmission.
3. **TCP/IP Protocol (1970s-1980s):** In the 1970s, the Transmission Control Protocol (TCP) and Internet Protocol (IP) were developed by Vinton Cerf and Robert Kahn. TCP/IP became the standard communication protocol for ARPANET and laid the foundation for the Internet. Its open architecture allowed for the integration of diverse networks.
4. **Ethernet and Local Area Networks (LANs) (1970s-1980s):** Ethernet, developed by Robert Metcalfe and his team at Xerox PARC in the 1970s, became a widely adopted LAN technology. LANs allowed computers to communicate within a limited geographic area, and Ethernet's success contributed to the growth of networking in businesses and academic institutions.
5. **Commercialization and Standards (1980s-1990s):** The 1980s witnessed the commercialization of networking technologies. The development of networking standards by organizations like the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE) facilitated interoperability and compatibility among different vendors' equipment.
6. **World Wide Web (1990s):** The invention of the World Wide Web by Sir Tim Berners-Lee in 1989 and its subsequent development in the early 1990s marked a significant leap in the use of the Internet. The web made information more accessible and user-friendly, leading to a surge in Internet usage.
7. **Broadband and High-Speed Internet (2000s-2010s):** The 2000s saw a widespread adoption of broadband Internet connections, offering higher data transfer speeds compared to traditional dial-up connections. This facilitated the growth of multimedia content, online services, and the development of social media platforms.
8. **Mobile Networks and Wireless Technologies (2000s-Present):** The proliferation of mobile devices and wireless technologies, including 3G, 4G, and now 5G, has further expanded the reach of computer networks. Mobile networks enable ubiquitous connectivity, allowing users to access the Internet and communicate from virtually anywhere.

9. **Internet of Things (IoT) and Future Trends (2010s-Present):** The Internet of Things (IoT) has become a significant development, connecting various devices and sensors to the Internet. Future trends include the continued expansion of high-speed networks, increased security measures, and the exploration of emerging technologies like blockchain and edge computing.

Timeline of Computer Networks:

- In 1957, Advanced Research Project Agency was formed by the US.
- In 1961, the idea of ARPANET was proposed by Leonard Kleinrock.
- In 1965, the term packet was used by Donald Davies.
- In 1969, ARPANET became functional, and the internet was officially born, with the first data transmission sent between UCLA and SRI on October 29, 1969, at 10:30 p.m.
- In 1971, Ray Tomlinson sent the first email, and the foundation for Wi-Fi was laid with the use of ALOHAnet.
- In 1973, Robert Metcalfe developed Ethernet at Xerox PARC, and the first experimental VoIP call was made.
- In 1976, the first true IP router was developed by Ginny Strazisar.
- In 1978, Bob Kahn invented the TCP/IP protocol for networks developed.
- In 1981, Internet Protocol version 4, or IPv4, was officially defined in RFC 791 in 1981.
- In 1983, DNS was introduced by Paul Mockapetris.
- In 1988, details about network firewall technology were first published 1988.
- In 1996, IPv6 was introduced.
- In 1997, the first version of the 802.11 standards for Wi-Fi was introduced in June 1997, providing transmission speeds up to 2 Mbps.
- In 2002-2004, Web 2.0 was introduced.

Modern Computer Networks:

From the first computer network, Arpanet, to the latest Web 3.0, the computer network has evolved in speed, reliability, and user experience. In today's world, everything is Speed, and to increase the network's Speed. We are currently replacing copper coaxial cables with optical fiber cables. Some things that make the network better and better with time are described as follows -

Optical Fiber Cables: An optical fiber is a thin strand of pure glass that works as a long-distance waveguide for light. It works on the principle of total internal reflection. The core, which carries the actual light signal, and the cladding, a sheet of glass around the core, are the two layers of glass that make up the device. The refractive index of the cladding is lower than that of the core, and this results in TIR within the core. Two significant service providers that provide optical fiber-based internet are Reliance JIO and Indian Airtel Xstream Fiber. Both service providers claim to provide a speed of 1 GBPS, which is enormous.

LI-FI Technology: Li-Fi is light-based bi-directional, fully networked, wireless communication technology where the light source is used to transmit the data wirelessly. This is achieved by turning the LED ON and OFF very rapidly (Million times per second) so that the flicker is not observable by the human eye. In this way, the data is transferred between the two devices wirelessly. Features provided by the Li-Fi are:

- **Speed**: Li-Fi can provide speeds up to 100 Gbps.
- **Security**: Light can not cross the walls, so data cannot be hacked by outsiders, providing one more layer of security.
- **Safety**: Unlike radio waves, light exposure is safer for humans.
- **Congestion-free**: The bandwidth of the light spectrum is 1000 times more than the radio spectrum; hence, it is congestion-free and free of electromagnetic interference.
- **Efficiency**: It uses LED for transmission, which minimizes the overall energy consumption.

Blockchain Technology: A blockchain is a database that holds encrypted data blocks and links them together to build a chronological single source of truth for the information. Blockchains are well known for their critical function in keeping a secure and decentralized record of transactions in cryptocurrency systems like Bitcoin. The blockchain's novelty is that it ensures the accuracy and security of a data record while also generating trust without the requirement for a trusted third party.

Web 3.0: The third generation of web technologies is known as Web 3.0 (Web3). Web 3.0 is still evolving and being defined, and as such, there isn't a canonical, universally accepted definition. But one thing is certain: Web 3.0 will significantly emphasize decentralized applications and make considerable use of blockchain-based technologies. Machine Learning and Artificial Intelligence (AI) will be used in Web 3.0 to help empower more intelligent and adaptive applications.

Firewall: A firewall is a network security hardware or software application that monitors and filters incoming and outgoing network traffic according to a set of security rules. It serves as a firewall between internal private networks and public networks (such as the public internet). To route web traffic, firewalls generate 'choke points,' which are then examined against predefined parameters and acted upon accordingly. Some firewalls also keep track of traffic and connections in audit logs to see what is allowed and prohibited.

Advantages of Computer Networking:

Here are the fundamental benefits/pros of using Computer Networking:

- Helps you to connect with multiple computers together to send and receive information when accessing the network.
- Helps you to share printers, scanners, and email.
- Helps you to share information at very fast speed
- Electronic communication is more efficient and less expensive than without the network.

Disadvantages of Computer Networking:

Here are drawbacks/ cons of using computer networks:

- Investment for hardware and software can be costly for initial set-up
- If you don’t take proper security precautions like file encryption, firewalls then your data will be at risk.
- Some components of the network design may not last for many years, and it will become useless or malfunction and need to be replaced.
- Requires time for constant administration
- Frequent server failure and issues of regular cable faults

Networks Topologies:

What is Network Topology?

Network topology refers to the arrangement or layout of devices and links in a computer network. It defines how different network nodes (computers, servers, routers, etc.) are connected and communicate with each other.

Network topologies are often represented as graphs. We can use these network topology graphs to decide where to position each node and the best path for traffic flow. An organization can more easily identify and resolve faults with a well-defined and well-planned network topology.

Why is Network Topology Important?

The layout of the network **(network topology)** is important for several reasons. It plays an essential role in how a network functions. In other words, network performance is directly affected by the topology. A correctly chosen and maintained network topology increases energy efficiency and data transmission rates, which can help increase performance.

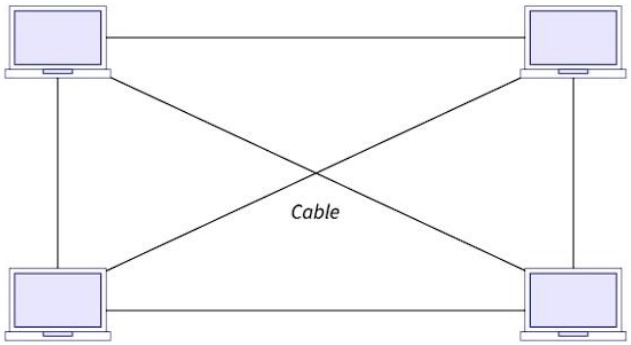
A **well-defined and well-planned network topology** makes it easier for network admins to locate faults, troubleshoot errors, and allocate resources across the network more effectively. Diagrams, which can show both logical and physical topology, are a vital source of information when diagnosing network issues.

Types of Network Topology:

There are **two** types of network topology in computer networks-

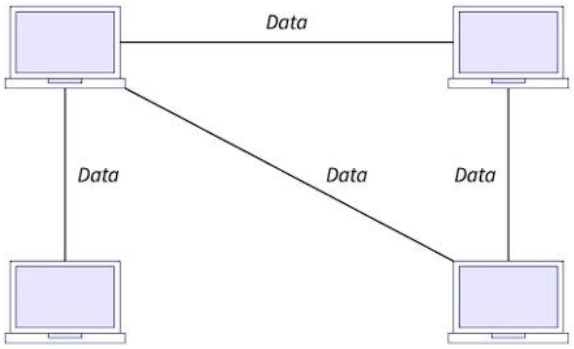
1. Physical Network Topology:

The physical network topology describes how these networking devices are connected with the help of cables or wires. Physical network knowledge is necessary for setup, maintenance, and provisioning tasks.

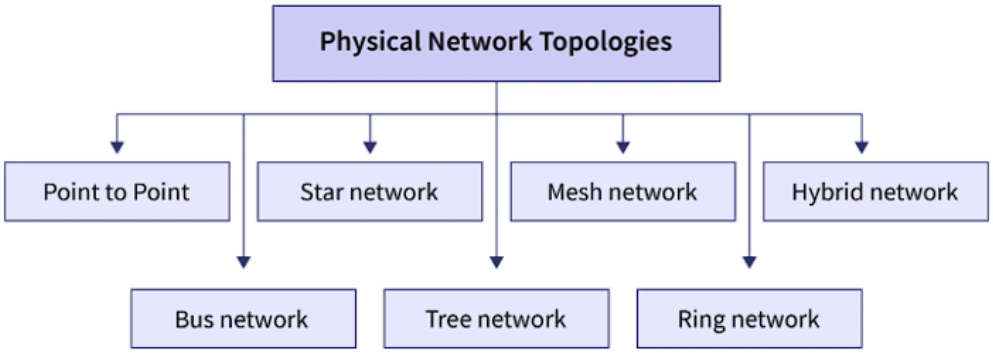


2. Logical Network Topology:

In networking, a logical topology defines the architecture of the communication mechanism for all nodes in a network. In other words, a logical topology describes the way how the **data flow from one node** (e.g., computer) to another. Logical topology differs from physical topology. A logical topology is how network devices appear connected to one another, while a physical topology is how they are physically connected with wires and cables.



Physical network topologies can be classified as follows:



1. Point to Point:

Point to Point is the simplest of all other network topologies. In this topology, **two network nodes** (e.g., computers) are **directly connected** to one another by LAN cables or another type of data transmission media. Point-to-Point provides high bandwidth.

Advantages:

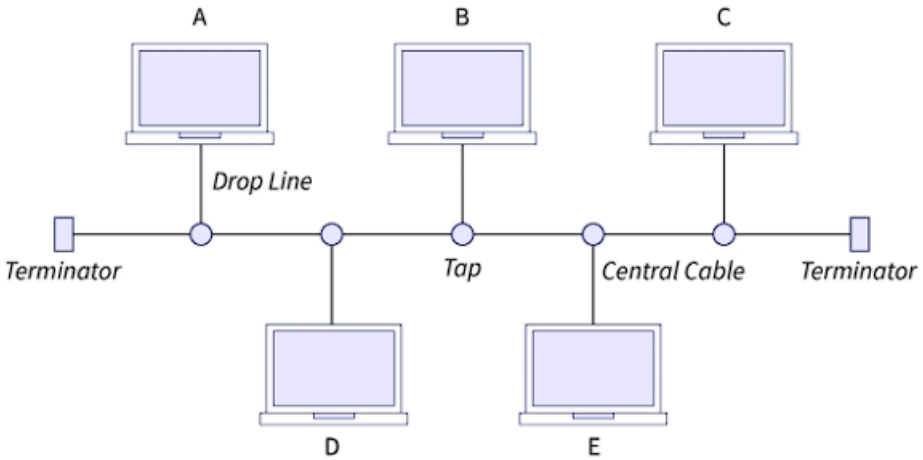
- Network operating system not required.
- The direct connection makes this connection faster and much more reliable than other connections.
- It does not require an expensive server as individual workstations are used to access the files.
- No dedicated network technicians are needed because each user manages their permissions.

Disadvantages:

- The main drawback is that it can only be used in smaller areas where computers are in close proximity.
- Centralized file and folder backups are not possible.
- Apart from permissions, there is no security. Users usually do not need to log onto their workstations.

2. Bus Topology:

All nodes in a bus topology are connected to a **central shared cable** known as a bus. Additionally, the bus connects these nodes to the Taps and Drop Lines. Drop Lines are the connection between the central wire or bus with the nodes. Taps are the 3-way connector that helps to attach the drop line to the main central cable.



Advantages:

- Although the cable is less expensive than other topologies, it is only utilized to build small networks.

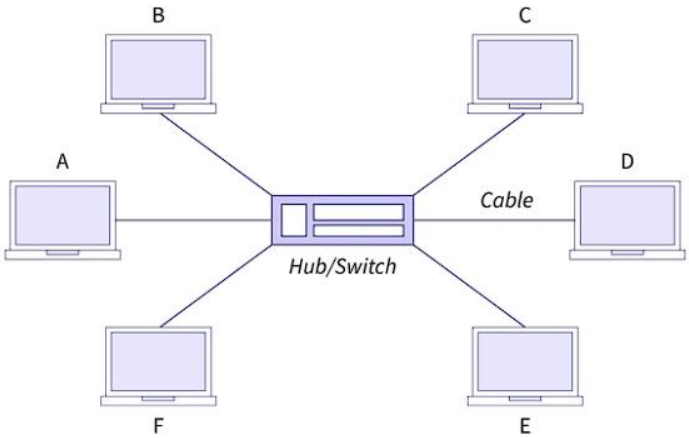
- It is famous for LAN (Local Area Network) because it is inexpensive and easy to install.
- It is frequently used when a network installation is small, simple, or temporary.

Disadvantages:

- The entire system will crash down if the common cable fails.
- Collisions occur in the network when network traffic is high.
- The length of cables is always limited.
- There could also be security issues because every node in the network can hear what data is transmitting to the other nodes.

3. Star Topology:

In star topology, all the nodes (e.g., computers) are connected to a **central hub with point-to-point** communication links. In this case, a point-to-point connection indicates that there is a cable connecting each node to the main hub. Data transfers between these nodes take place through the central device. It is most widely used on LAN networks since they are inexpensive and easy to install.



Advantages:

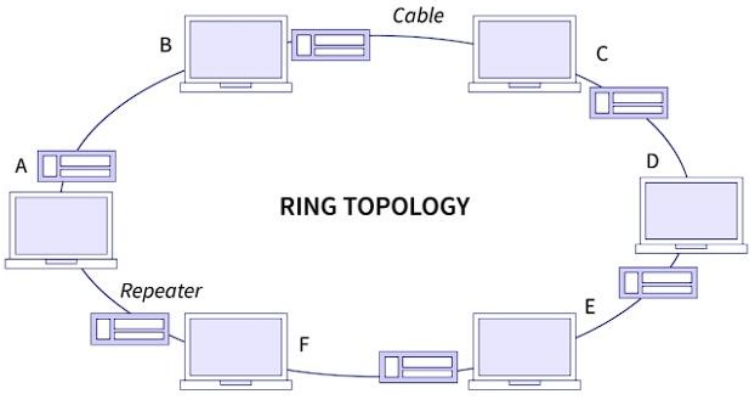
- By just checking the specific node that isn't working, it becomes easy to identify the faulty nodes.
- The failure of a single node has no impact on the network as a whole. Therefore, such fault can be tolerated and addressed later.
- Device addition, deletion, and movement are simple under a star topology.
- It has fast performance with few nodes and very low network traffic.

Disadvantages:

- The greatest drawback of star topology is this. The entire network would be down if the HUB/SWITCH itself experienced a problem.
- The number of physical ports offered by HUB/SWITCH limits the nodes linked to the star topology.
- The installation of a star topology is expensive.

4. Ring Topology:

There are many nodes in the Ring network, and each node is connected to **two of its neighbor nodes**. It is referred to as a ring topology because of its ring-like structure. Every computer in this topology is connected to every other computer. The last node and the first node are connected in this topology. This topology uses tokens to pass the information between the computers. All of the messages in this topology travel in the same direction through a ring.



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

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

Working of Token passing:

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

Advantages:

- Due to the simplicity of identifying defects in either nodes or cables, it is easier to manage and install.
- In this type of topology, the possibility of collision is minimum.
- Only two connections need to be moved to add or remove a device from a ring topology.
- Less cabling is required because each node manages the cable to its nearest neighbor.

Disadvantages:

- In this topology, troubleshooting is difficult.
- By removing or adding stations between other stations, the topology as a whole might be affected.
- It is less secure because the data packet passes through every workstation connected.
- Topology signals flow continuously in the ring, resulting in unwanted power consumption.

5. Mesh Topology:

The mesh topology has a unique network design in which each computer on the network connects to every other. It develops a P2P (point-to-point) connection between all the devices of the network. It offers a high level of redundancy, so even if one network cable fails, still data has an alternative path to reach its destination.

Mesh has **n(n-1)/2** physical channels to link **n** devices.

There are two techniques to transmit data over the Mesh topology, they are:

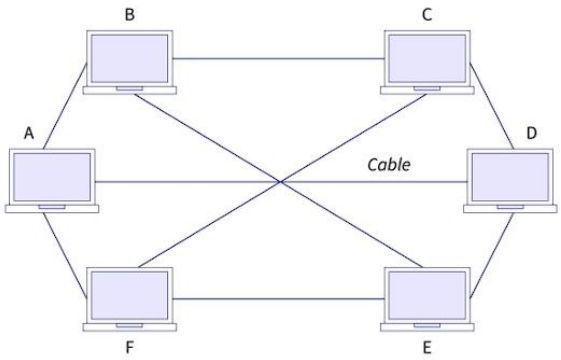
1. **Routing:** In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those nodes etc. We can even have routing logic, to re-configure the failed nodes.

2. **Flooding:** In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

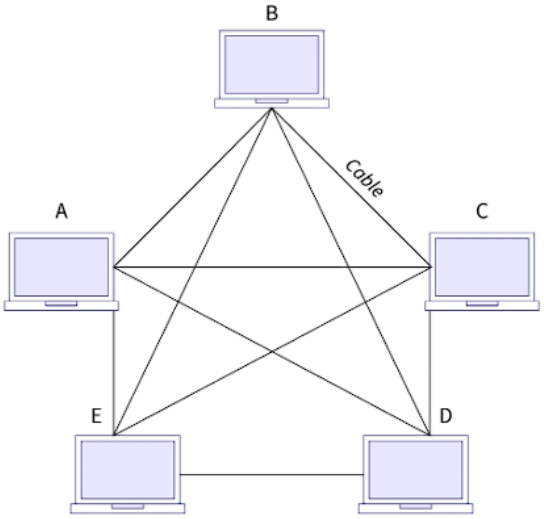
There are two different types of mesh topology.

1. Partial Mesh Topology 2. Full Mesh Topology

1. **Partial Mesh Topology:** In a partial mesh topology, all nodes may not be directly connected to every other node. Still, perhaps most nodes are connected by a point-to-point connection.



2. **Full Mesh Topology:** In Full Mesh Topology, every node or device has a direct point-to-point connection with all the other nodes in the network. Due to the direct connections between all the other nodes, it almost eliminates the possibility of network failure.



Advantages:

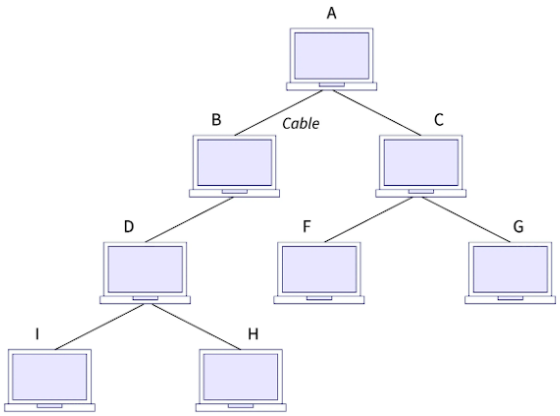
- There are so many links, so there is minimal or no chance of network failure in the mesh topology.
- Due to each node's separate links, each node can transfer data privately to any other node within the network.
- This topology has no traffic problem because each node has a dedicated link.
- Point-to-point connections make the fault identification isolation process easy.

Disadvantages:

- The cost of cables is high because it requires extra cables compared with other LAN topologies.
- There is a lot of cabling to handle, so mesh topology implementation might be challenging.
- More space is required for dedicated links.

6. Tree Topology:

Tree topologies have a root node, and all other nodes are connected which form a hierarchy. These node structures are used when a network needs to be **divided into a subnetwork**. So, it is also known as **hierarchical topology.** This topology integrates various star topologies together in a single bus, so it is known as a **Star Bus topology.** Tree topology is a very common network which is similar to a bus and star topology.



Advantages:

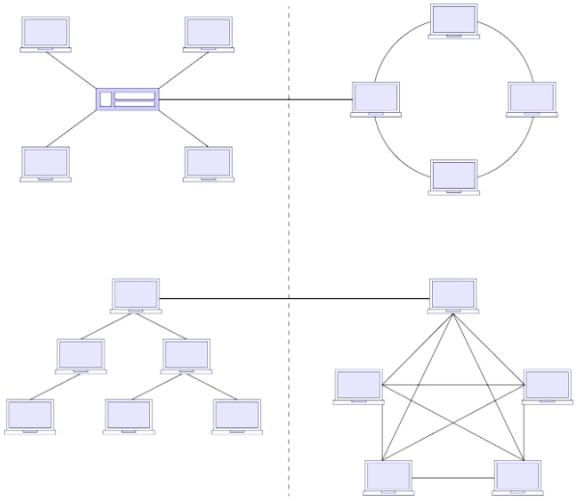
- Every node has access to the large and intermediate network.
- Expansion of nodes is fast and easy.
- The network as a whole is never affected when one node (leaf nodes) affects.
- It is easy to manage and maintain.

Disadvantages:

- It is possible that all the other nodes will become disconnected if the main central node experiences a failure.
- When more nodes are added, maintaining it becomes difficult.
- The topology is highly cabled, which increases the cost.

7. Hybrid Topology:

The **combination** of all the different types of topologies we have seen is known as hybrid technology. This structure is used in which the nodes can take any form. This means that it can only be a tree topology, a ring topology, or a star topology. Additionally, it may combine all the types of network topology we have seen.



Advantages:

- It is scalable, so you can expand the size of your network.
- It provides the simplest technique for identifying and resolving errors.
- It is a highly effective and flexible networking topology.

Disadvantages:

- The design of hybrid topology is complex.
- It is one of the most expensive processes.

8. Daisy Chain:

This topology connects all the hosts in a linear fashion. Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts. Means, if the end hosts in daisy chain are connected then it represents Ring topology.

Each link in daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for its immediate hosts.

How to Select a Network Topology?

No network topology is perfect or even inherently superior to the others. Therefore, choosing the best structure for your organization will rely on its requirements and network size. Here are the key factors to consider:

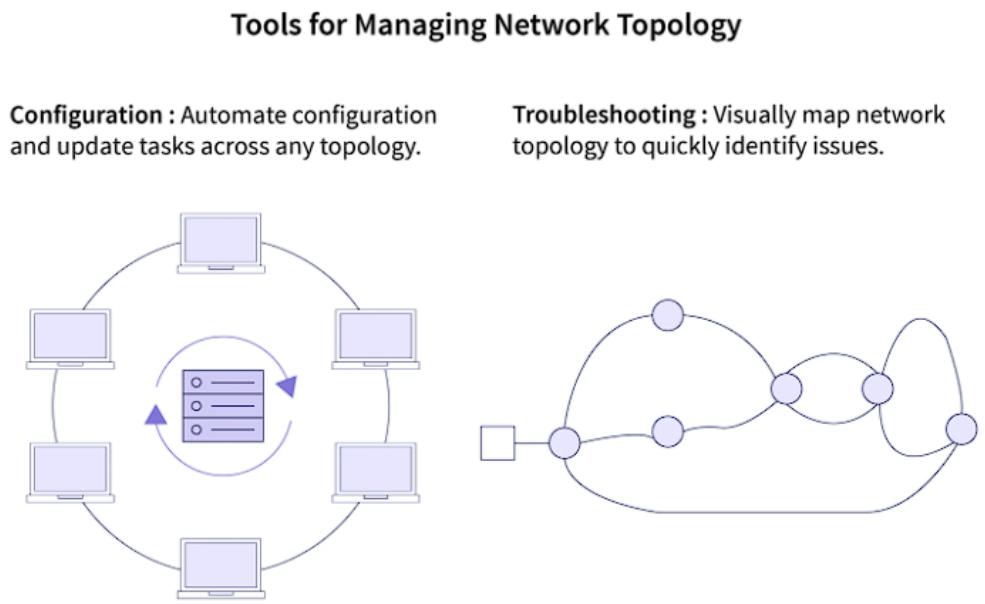
1. Length of cable required
2. Cable type
3. Cost
4. Scalability

Here are some topologies for the organization based on the above-mentioned factors.

- Undoubtedly, bus topology is the least expensive network installation, so you can choose this option if you want the least expensive topology.
- Star topology is the best option for you if you want to use a shorter cable or if you intend to extend the network in the future.
- Theoretically, a full mesh topology is the best option because every device is connected to every other device.
- Build star topologies if you want to use a twisted pair cable for networking.

What Tools Help Manage and Monitor Networks?

There are many network managing and monitoring tools available, including those that can be categorized as configuration and management tools and network performance tools.



Network configuration tools: Network configuration software automates repetitive tasks while helping in network configuration. These tools have the ability to detect network nodes and highlight potential vulnerabilities automatically, and they are frequently used to configure complicated network topologies.

Here are some network configuration management tools:

- SolarWinds Network Configuration Manager
- ManageEngine Network Configuration Manager
- WeConfig NCM
- BladeLogic Network Automation

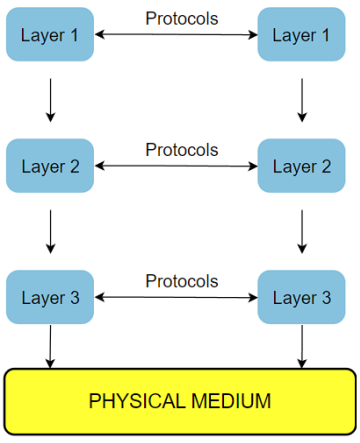
Network performance troubleshooting tools: Network performance monitoring and troubleshooting software keep track of and notify users of network-related performance problems and outages. Using a visual representation of the network topology, some of these tools may monitor performance. Users can track down, locate, and troubleshoot issues after setting baseline performance parameters.

Here are some network performance troubleshooting tools:

- Network Performance Monitor
- ManageEngine OpManager
- Wireshark
- PRTG Network Monitor

Layering:

The grouping of relevant communication functions into different hierarchical sets is known as **layering**. Every batch of operations is a separate layer.



A simple layering simulation

Functions of layers:

Each layer is responsible for the following functions:

- Perform a subset of different functions required for communication.
- Provide the services of its functions to the next higher layer in the hierarchy.
- Implementation of communication protocols with peer layers in another system.
- After implementing its operations, it relies on the next layer to perform additional functions.

Motivation of layering:

There are many reasons to use layering in communication, but some of them include:

- **Modularity:** It decomposes a significant problem into multiple small subproblems that can be managed easily. This gives you more flexibility in designing, modifying, and evolving the computer network. In simple words, it decreases complexity.

- **Reusability and controllability:** It's a standard layering functionality; the lower layer can be shared with many upper layers, increasing the reusability and controllability because of the segmentation of functions. The layering can support incremental modifications easily.

Layered Architecture:

The architecture of computer networks uses a layering mechanism in which data transmitted from one defined layer to another for processing is a **layered architecture**.

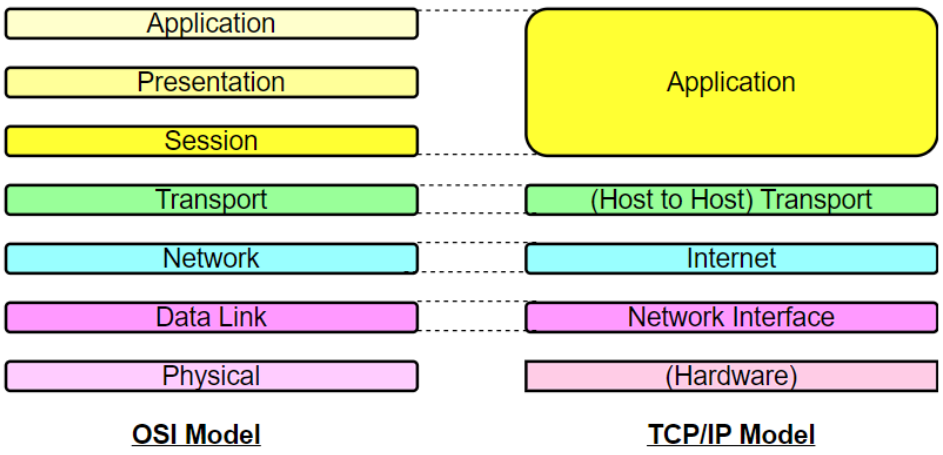
There are three major fundamental components of layered architecture:

- **Service**: A collection of functions provided by a layer to a higher layer.
- **Protocol**: A set of rules to share data with the peer layer.
- **Interface**: This is a means of transmitting a message from one layer to another.

The application of layered architecture:

Layered architecture is used for communication. There are two network models which use layering.

- OSI model
- IP/TCP model



The layered architecture of OSI & TCP/IP model

There's a correspondence between these models, and TCP can be explained in terms of the OSI model. Layers can only communicate in two modes:

1. Vertical communication:

The communication between adjacent layers requires mutual understanding of the services and information that the lower layer needs to provide to the upper layer.

2. Horizontal communication:

This is the communication between hardware or software that is running on the same layer but on different machines.

> **Note:** Communication between processes is done virtually through a medium.

Protocols:

Network protocols are a set of rules outlining how connected devices communicate across a network to exchange information easily and safely. Protocols serve as a common language for devices to enable communication irrespective of differences in software, hardware, or internal processes.

Types of network protocols:

Different protocols serve different functions to ensure efficient, quick, and secure network communication. Various types of network protocols can be categorized into the following three broad categories to help organizations operate seamlessly across different business scenarios:

1. Network Communication Protocols: These protocols determine the rules and formats to transfer data across networks. Communication protocols govern various aspects of analog and digital communications, such as syntax, authentication, semantics, and error detection, among others. Some key network communication protocols include:

- **Hyper-Text Transfer Protocol (HTTP)**: Commonly referred to as the protocol of the internet that allows communication between a server and browser.
- **Transmission Control Protocol (TCP)**: A reliable, connection-oriented protocol that helps in the sequential transmission of data packets to ensure data reaches the destination on time without duplication.
- **Internet Protocol (IP)**: Facilitates routing the data packets across networks. IP contains addressing and control information to deliver packets across a network. It works along with TCP. While it ensures delivering the packets to the right address, TCP aligns them in the right order.
- **User Datagram Protocol (UDP)**: Unlike TCP, UDP is a connectionless protocol that doesn't ensure a connection between the application and server before transmitting a message. It's effective for use cases such as broadcasts or multicast connections.
- **File Transfer Protocol (FTP)**: Allows file sharing between servers by establishing two TCP connections, one for data transfer and the other for control. The data transfer connection transfers the actual files while the control connection transfers control information such as passwords to ensure data retrieval in case of data loss.

Helps diagnose network connectivity issues. Network devices employ ICMP for sending error messages, highlighting congestion and timeouts, and transmitting other operational information to assist in network troubleshooting.

2. Network Security Protocols: These protocols ensure safe data transmission over the network connections. Network security protocols define the procedures to secure data from any unauthorized access. These protocols leverage encryption and cryptography to safeguard. Here are the most widely used network security protocols:

- **Secure File Transfer Protocol (SFTP)**: Helps securely transfer files across a network by using public-key encryption and authenticating the client and server.
- **Hyper-Text Transfer Protocol Secure (HTTPS)**: Overcomes the limitation of HTTP by ensuring the security of data transmitted between the browser and server through data encryption. HTTPS is a secure version of HTTP.
- **Secure Socket Layer (SSL)**: Primarily helps secure internet connections and safeguard sensitive data using encryption. SSL protocol enables both server-client communication and server-server communication.

3. Network Management Protocols: Network managers require standard policies and procedures to manage and monitor the network for maintaining smooth communication. Network management protocols ensure quick troubleshooting and optimal performance across the network. The following are essential network protocols management:

- **Simple Network Management Protocol (SNMP):** Helps administrators manage network devices by monitoring endpoint information to proactively track network performance and pinpoint network glitches for quick troubleshooting.
- **Internet Control Message Protocol (ICMP):** Helps diagnose network connectivity issues. Network devices employ ICMP for sending error messages, highlighting congestion and timeouts, and transmitting other operational information to assist in network troubleshooting.

How do network protocols work?

Understanding how network protocols work makes it crucial to see how connected devices communicate over a network. The most popular model, the Open Systems Interface (OSI), demonstrates how computer systems communicate over a network. This seven-layer model visualizes the communication process between two network devices across seven layers.

Network protocols split the communication process into discrete tasks across each OSI model layer. To enable network communication, one or more protocols operate at every layer. For example, the Internet Protocol (IP) routes data by managing the information such as data packets' source address and destination to enable network-to-network communications. Therefore, it's referred to as a network layer protocol.

OSI Model Layers and Protocols:

What is OSI Model?

The OSI Model is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. The Open System Interconnection (OSI Model) also defines a logical network and effectively describes computer packet transfer by using various layers of protocols.

Characteristics of OSI Model:

Here are some important characteristics of the OSI model:

- A layer should only be created where the definite levels of abstraction are needed.
- The function of each layer should be selected as per the internationally standardized protocols.

- The number of layers should be large so that separate functions should not be put in the same layer. At the same time, it should be small enough so that architecture doesn't become very complicated.
- In the OSI model, each layer relies on the next lower layer to perform primitive functions. Every level should able to provide services to the next higher layer
- Changes made in one layer should not need changes in other lavers.

Why of OSI Model?

- Helps you to understand communication over a network
- Troubleshooting is easier by separating functions into different network layers.
- Helps you to understand new technologies as they are developed.
- Allows you to compare primary functional relationships on various network layers.

History of OSI Model:

Here are essential landmarks from the history of OSI model:

- In the late 1970s, the ISO conducted a program to develop general standards and methods of networking.
- In 1973, an Experimental Packet Switched System in the UK identified the requirement for defining the higher-level protocols.
- In the year 1983, OSI model was initially intended to be a detailed specification of actual interfaces.
- In 1984, the OSI architecture was formally adopted by ISO as an international standard

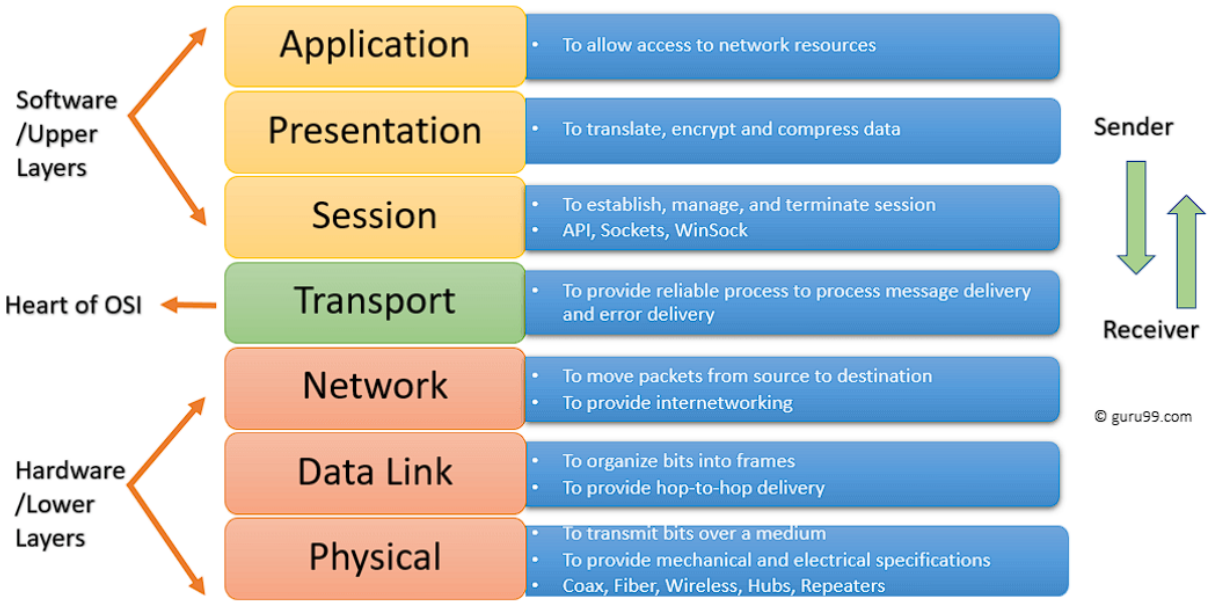
7 Layers of the OSI Model:

OSI model is a layered server architecture system in which each layer is defined according to a specific function to perform. All these seven layers work collaboratively to transmit the data from one layer to another.

- **The Upper Layers**: It deals with application issues and mostly implemented only in software. The highest is closest to the end system user. In this layer, communication from one end-user to another begins by using the interaction between the application layer. It will process all the way to end-user.
- **The Lower Layers**: These layers handle activities related to data transport. The physical layer and datalink layers also implemented in software and hardware.

Upper and Lower layers further divide network architecture into seven different layers as below -

1. Application
2. Presentation
3. Session
4. Transport
5. Network, Data-link
6. Physical layers



Network Layers Diagram

Let's Study each layer in detail:

1. Physical Layer:

The physical layer helps you to define the electrical and physical specifications of the data connection. This level establishes the relationship between a device and a physical transmission medium. The physical layer is not concerned with protocols or other such higher-layer items. One example of a technology that operates at the physical layer in telecommunications is PRI (Primary Rate Interface).

Examples of hardware in the physical layer are network adapters, ethernet, repeaters, networking hubs, etc.

2. Data Link Layer:

Data link layer corrects errors which can occur at the physical layer. The layer allows you to define the protocol to establish and terminates a connection between two connected network devices.

It is IP address understandable layer, which helps you to define logical addressing so that any endpoint should be identified.

The layer also helps you implement routing of packets through a network. It helps you to define the best path, which allows you to take data from the source to the destination.

The data link layer is subdivided into two types of sublayers:

1. **Media Access Control (MAC) layer** - It is responsible for controlling how device in a network gain access to medium and permits to transmit data.
2. **Logical link control layer** - This layer is responsible for identity and encapsulating network-layer protocols and allows you to find the error.

Important Functions of Datalink Layer:

- Framing which divides the data from Network layer into frames.
- Allows you to add header to the frame to define the physical address of the source and the destination machine
- Adds Logical addresses of the sender and receivers
- It is also responsible for the sourcing process to the destination process delivery of the entire message.
- It also offers a system for error control in which it detects retransmits damage or lost frames.
- Datalink layer also provides a mechanism to transmit data over independent networks which are linked together.

3. Transport Layer:

The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine. It is hosted using single or multiple networks, and also maintains the quality-of-service functions.

It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or desegmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

Important functions of Transport Layers:

- It divides the message received from the session layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

4. Network Layer:

The network layer provides the functional and procedural means of transferring variable length data sequences from one node to another connected in "different networks".

Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Layer-management protocols that belong to the network layer are:

1. routing protocols
2. multicast group management
3. network-layer address assignment.

5. Session Layer:

Session Layer controls the dialogues between computers. It helps you to establish starting and terminating the connections between the local and remote application.

This layer request for a logical connection which should be established on end user's requirement. This layer handles all the important log-on or password validation.

Session layer offers services like dialog discipline, which can be duplex or half-duplex. It is mostly implemented in application environments that use remote procedure calls.

Important function of Session Layer

- It establishes, maintains, and ends a session.
- Session layer enables two systems to enter into a dialog
- It also allows a process to add a checkpoint to steam of data.

6. Presentation Layer:

Presentation layer allows you to define the form in which the data is to exchange between the two communicating entities. It also helps you to handles data compression and data encryption.

This layer transforms data into the form which is accepted by the application. It also formats and encrypts data which should be sent across all the networks. This layer is also known as a **syntax layer**.

The function of Presentation Layers:

- Character code translation from ASCII to EBCDIC.
- Data compression: Allows to reduce the number of bits that needs to be transmitted on the network.
- Data encryption: Helps you to encrypt data for security purposes — for example, password encryption.
- It provides a user interface and support for services like email and file transfer.

7. Application Layer:

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means OSI application layer allows users to interact with other software application.

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.

Example of the application layer is an application such as file transfer, email, remote login, etc.

The function of the Application Layers are -

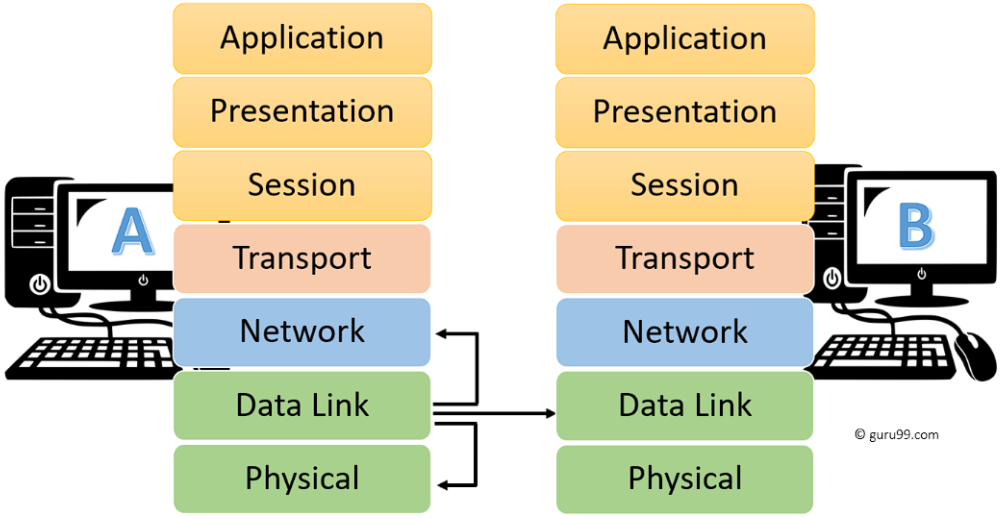
- Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- It allows users to log on to a remote host
- This layer provides various e-mail services
- This application offers distributed database sources and access for global information about various objects and services.

Interaction Between OSI Model Layers:

Information sent from a one computer application to another needs to pass through each of the OSI layers.

This is explained in the below-given example:

- Every layer within an OSI model communicates with the other two layers which are below it and its peer layer in some another networked computing system.
- In the below-given diagram, you can see that the data link layer of the first system communicates with two layers, the network layer and the physical layer of the system. It also helps you to communicate with the data link layer of, the second system.



Protocols supported at various levels:

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL, TLS
Layer 5	Session	NetBIOS, SAP
Layer 4	Transport	TCP, UDP
Layer 3	Network	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
Layer 1	Physical	RS232, 100BaseTX, ISDN, 11.

Advantages of the OSI Model:

Here, are major benefits/pros of using the OSI model:

- It helps you to standardize router, switch, motherboard, and other hardware
- Reduces complexity and standardizes interfaces
- Facilitates modular engineering
- Helps you to ensure interoperable technology
- Helps you to accelerate the evolution
- Protocols can be replaced by new protocols when technology changes.
- Provide support for connection-oriented services as well as connectionless service.
- It is a standard model in computer networking.
- Supports connectionless and connection-oriented services.
- Offers flexibility to adapt to various types of protocols

Disadvantages of the OSI Model:

Here are some cons/ drawbacks of using OSI Model:

- Fitting of protocols is a tedious task.
- You can only use it as a reference model.
- Doesn't define any specific protocol.
- In the OSI network layer model, some services are duplicated in many layers such as the transport and data link layers
- Layers can't work in parallel as each layer need to wait to obtain data from the previous layer.

TCP/IP Model:

What is the TCP/IP Model?

TCP/IP Model helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them. It helps you to create a virtual network when multiple computer networks are connected together. The purpose of TCP/IP model is to allow communication over large distances.

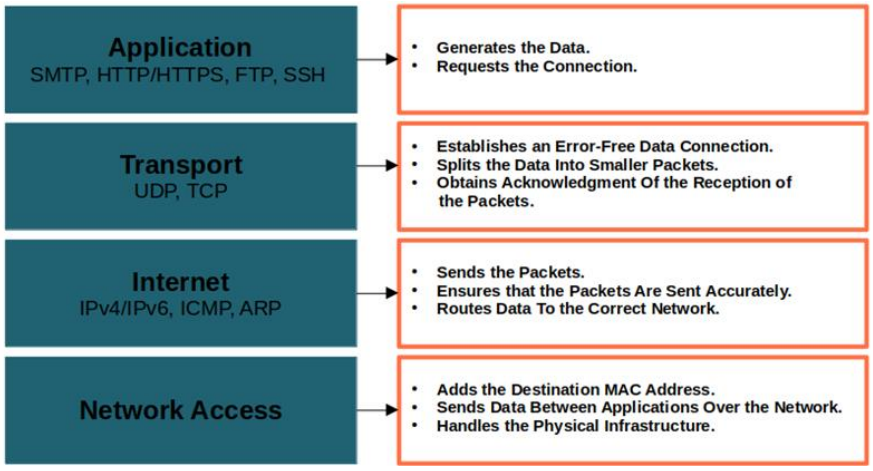
TCP/IP stands for Transmission Control Protocol/ Internet Protocol. TCP/IP Stack is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

TCP Characteristics:

Here, are the essential characteristics of TCP IP protocol:

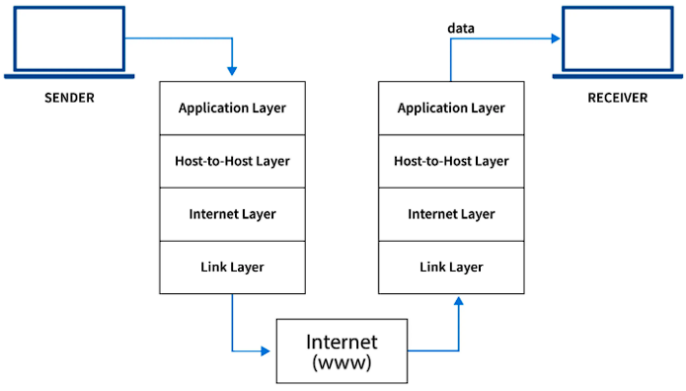
- Support for a flexible TCP/IP architecture
- Adding more system to a network is easy.
- In TCP IP protocols suite, the network remains intact until the source, and destination machines were functioning properly.
- TCP is a connection-oriented protocol.
- TCP offers reliability and ensures that data which arrives out of sequence should put back into order.
- TCP allows you to implement flow control, so sender never overpowers a receiver with data.

Four Layers of TCP/IP model:



How Does the TCP/IP Protocol Work?

Whenever we send things like a simple text message, a file, or a video message over the internet, the TCP/IP model divides the data into packets, according to four-layered architecture. The data goes in order from the sender's side, and on the receiver's side, it follows the reverse order and is finally reassembled.



TCP/IP is based on the client-server communication model, which means that a user of a first computer (the client) sends a service request to a second network computer or web hosting provider(server), such as forwarding a Web page. TCP/IP also uses point-to-point communication, which means that data is sent from one host computer to another within a defined network border. In TCP/IP model, each client request is unique and unrelated to previous ones. Hence, it is called stateless, and being stateless allows network channels to be used indefinitely.

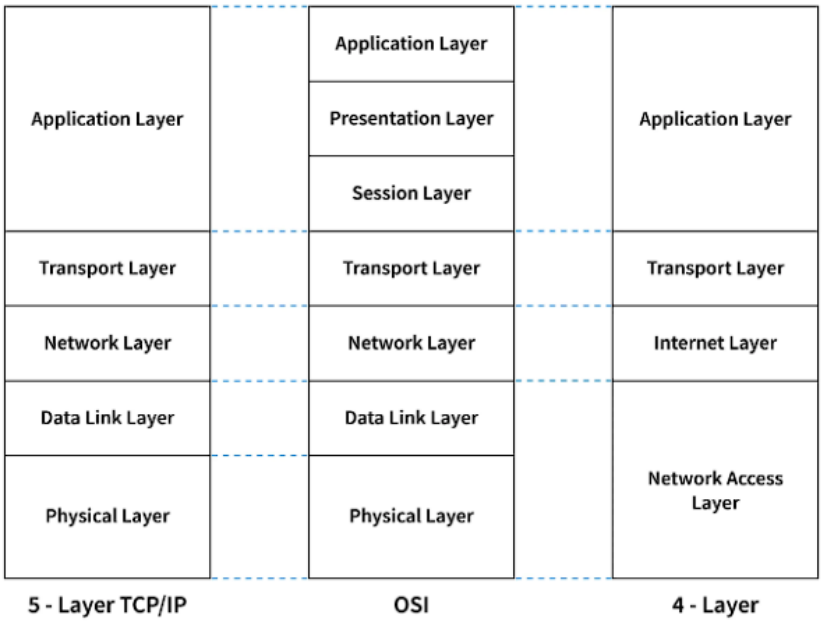
Because the entire process is standardized, the TCP/IP model works. Without standardization, communication would go haywire, and fast internet service relies on efficiency. The TCP/IP model provides both efficiency and standardization. The TCP/IP model is the most effective way to send internet data because it is the global standard.

Layers in TCP/IP Model:

The TCP/IP model generally consists of four essential layers

1. Application Layer
2. Host-To-Host Layer/Transport Layer
3. Internet Layer/Network Layer
4. Network Access Layer/Link Layer

Since TCP/IP is an implementable model, it can be further classified into a five-layer model in which the data link layer and the physical layer are separated from the Link layer. It is done to achieve the client's requirements with efficiency. To understand better, let's have a look at the diagram given below, which compares four-layer and five-layer TCP/IP Models with the standard OSI Model.



The 4 Layers of the TCP/IP Protocol Suite:

1. Application Layer: This layer performs the functions of the top three layers of the OSI model, i.e., the Application, Presentation, and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Its protocols include HTTP, Post Office Protocol 3, Simple Mail Transfer Protocol, and File Transfer Protocol. At the application layer, the payload is the actual application data. Some of the protocols of the application layer are described below.

- **HTTP**: It stands for **Hypertext transfer protocol**. This protocol enables us to access data via the internet. It sends data in plain text, audio, and video formats. It's called a hypertext transfer protocol because it's efficient enough to use in a hypertext environment where there are rapid jumps from one document to another.
- **TELNET**: It establishes a connection between the local and remote computers in such a way that the local computer seems to be a remote terminal.
- **SMTP**: The **Simple Mail Transfer Protocol (SMTP)** is the TCP/IP protocol that handles e-mail. The data is sent to another e-mail address using this protocol.
- **FTP**: The **FTP (File Transfer Protocol)** is a standard internet protocol for transferring data from one computer to another.

2. Host-to-Host/Transport Layer: This layer is similar to the OSI model's Transport layer. It specifies how much data should be sent, when, and where at what rate. The message from the application layer is built upon this layer. This layer ensures that data units are supplied in a timely and error-free manner. Through error control, flow control, and segmentation or de-segmentation, the transport layer helps to control the link's reliability. The transport layer also acknowledges the successful data transmission and sends the next data if no errors occur. The two important protocols present in this layer are

- **Transmission Control Protocol (TCP)**: It is known for offering error-free and reliable communication between end systems. It does data segmentation and sequencing. It also features an acknowledgment feature and uses a flow control method to govern data flow. It is a very effective protocol, but it has a lot of overhead because of these features. Increased overhead translates to higher costs. TCP uses three-way handshaking to establish and acknowledge the connection between the two devices.
- **User Datagram Protocol (UDP)**: On the other side, it doesn't have any of these properties. If your application does not require dependable transmission, one must use this protocol because it is relatively cost-effective. UDP is a connectionless protocol, so it does not provide assurance of data delivery.

3. Internet Layer: This layer is also known as the **network layer**. The Internet layer's primary function is to send packets from the source or computer to their destination, regardless of their route. The Internet layer or Network Layer provides a functional and procedural means for sending variable-length data sequences between nodes across multiple networks. Message delivery at the Internet layer does not guarantee reliable network layer protocol. The main protocols lie in the layer are

- **IP**: The Internet Protocol (IP) is in charge of sending packets from a source host to a destination host based on the IP addresses in the packet headers. There are two variations of IP IPv6 and IPv4.
- **ARP**: Address Resolution Protocol (ARP) is a protocol for resolving conflicts between computers. Its task is to determine a host's hardware address from an IP address. ARP's primary function is to convert 32-bit addresses to 48-bit addresses and vice versa. ARP is necessary because IP addresses in IP version 4 (IPv4) are 32 bits long, but MAC addresses are 48 bits long.

4. Network Access Layer/Link Layer: Network access or Link layer specifies the physical transmission of data over the network. This layer handles data transmission between two adjacent devices on the same network. It also determines how bits should be optically signaled by hardware devices that interface directly with a network media such as coaxial, optical, fiber, or twisted-pair cables.

Uses Of TCP/IP Model:

The various uses of the TCP/IP Model are described below -

1. It provides a suite of communication protocols that allows data exchange between two devices possible or in general we can say that it makes the internet possible.
2. We all are aware of the importance of text communication in today's environment. For text communication, flow control, and error control are mandatory because the text message's size is minimal, and it must be delivered with minimal error to the right person. A small mistake in the text message can change the meaning of the whole message. So, TCP/IP model handles the following operations to ensure the transition between sender and receiver is in order and error-free. Examples of text communication are WhatsApp, Instagram, Google Chat, and iMessage.
3. Internet banking is possible due to this model because it provides reliability, efficiency, and security, making it possible for users to use such facilities online.
4. Online gaming and video streaming are also possible because TCP/IP model provides flexibility in choosing connection-oriented or connectionless transmission. Due to this flexibility, broadcasting sports and events to a mass audience is possible.
5. TCP/IP provides various functions like DNS, DHCP, Virtual Private Networking, Piggybacking, Error control, etc. This feature allows end-user to use the internet without fear of losing their privacy and integrity.

Advantages of TCP/IP Model:

1. It's a set of open protocols. As any one institution does not own it, it can be used by anybody or any group.
2. It's a client-server architecture and highly scalable. It allows the addition of new networks without disrupting existing services.
3. It's an industry-standard model that can be used to solve real-world networking problems.
4. It is interoperable, allowing two different systems to communicate via a heterogeneous network.
5. It assigns a unique IP address to each device in a network such that each device has its own unique identity over the internet.
6. It is challenging for humans to remember numerical values compared to alphabetical names. So, to solve this, TCP/IP models also provide DNS service to provide resolution between alphabetical domain names and IP addresses.

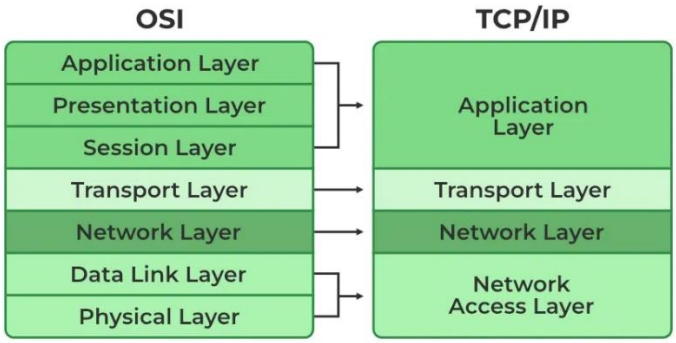
Disadvantages of the TCP/IP Model:

1. Concepts like "services," "interfaces," and "protocols" are not distinguished. As a result, describing new technologies in new networks is not appropriate.
2. This model was created to be used in wide-area networks. It is not designed for tiny networks such as **LANs** and **PANs** (pervasive area networks) (personal area networks).
3. It's not generic. As a result, it can't represent any protocol stack other than TCP/IP. It cannot, for example, define a Bluetooth connection.
4. It is not easy to replace protocols.

Relationship between OSI and TCP/IP Models:

The TCP/IP model is often considered a practical implementation of the OSI model. The four layers of the TCP/IP model map loosely to the seven layers of the OSI model. The relationship is as follows:

- **Network Access Layer (TCP/IP) ≈ Data Link and Physical Layers (OSI)**
- **Internet Layer (TCP/IP) ≈ Network Layer (OSI)**
- **Transport Layer (TCP/IP) ≈ Transport Layer (OSI)**
- **Application Layer (TCP/IP) ≈ Application, Presentation, and Session Layers (OSI)**



While the OSI model provides a more detailed and comprehensive framework, the TCP/IP model is widely adopted and serves as a practical guide for the development and implementation of Internet protocols. The Internet, as we know it, is largely based on the TCP/IP protocol suite.

Differences between OSI and TCP/IP models:

OSI Model	TCP/IP model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI model use two separate layers physical and data link to define the functionality of the bottom layers.	TCP/IP uses only one layer (link).
OSI layers have seven layers.	TCP/IP has four layers.
OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are not a part of the TCP model.	There is no session and presentation layer in TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	Minimum header size is 20 bytes.

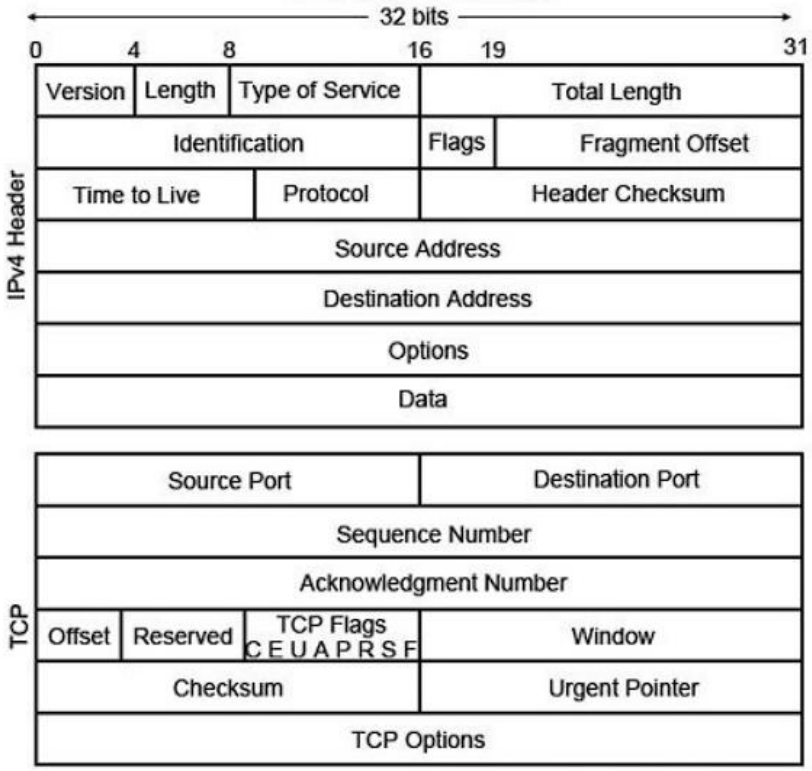
Basics of Packet:

What Does Packet Mean?

In computer networks, a packet is a container or box that carries data over a TCP/IP network and internetworks. A packet is the most fundamental logical arbitration of data that is passed over a network.

A packet normally represents the smallest amount of data that can traverse over a network at a single time. A TCP/IP network packet contains several pieces of information, including the data it is carrying, source destination IP addresses, and other constraints required for quality of service and packet handling.

Structure of a Data Packet:



A network packet is comprised of three main parts:

1. **Packet Header**: The header is the initial information of the packet. This is the first part of the packet the receiving device sees. There are 8 components to an IPv6 packet header:
    1. **Version:** 4-bit identifier of the Internet Protocol version.
    2. **Traffic Class:** Indicates the priority of the packet.
    3. **Flow Label:** Indicates that the packet belongs to a specific series of packets.
    4. **Payload Length:** Specifies the length of everything in the packet following the header.

5. **Next Header:** Specifies what type of payload the packet contains.
6. **Hop Limit:** Ensures the packet doesn't fall into an infinite loop. Each time it passes a router, the Hop Limit decreases by one.
7. **Source Address:** Indicates the address of the device sending the packet.
8. **Destination Address:** Indicates the address of the destination device of the packet.

2. **Payload**: The payload is the actual data that is being transmitted to the destination. To ensure the packet is the proper size, the payload may be padded with blank data.
3. **Trailer**: At times, some network protocols will attach a trailer or end part to a packet. For example, Ethernet frames contain trailers, but IP packets do not. This is often done to denote the end of a network packet or perform error correction.

What is packet loss?

Packet loss happens as a result of a single or multiple packets of data traversing a computer network, but failing to arrive at their intended destination. Such a failure can be caused by errors in the transmission of the data over a wireless or wired network. It can also be the result of network congestion. Packet loss is defined as the percentage of packets lost compared to the number of packets sent.

Transmission Control Protocol (TCP) is an important tool for detecting and remedying packet loss. When network packet loss is detected by the TCP, retransmission of the packets is attempted to ensure messages are completed. In some cases, packet loss is intentionally introduced through the TCP connection in order to reduce throughput and alleviate network congestion.

Packet loss can adversely impact a user's quality-of-experience (QoE), particularly in real-time applications, such as online gaming and streaming media.

What is a Packet Broker?

A packet broker is a hardware or software appliance that directs network traffic from multiple SPAN ports and manipulates the traffic to allow more efficient use of network tools and monitoring devices on the network. Packet brokers are tasked with gathering traffic from numerous network links, then filtering and redirecting the individual packets to the optimal network monitoring tool. By improving the delivery of data across the network, the effectiveness of network monitoring and security tools is attained.

What is a packet analyzer, protocol analyzer or network analyzer?

A packet analyzer is a software program or computer hardware (packet capture appliance) that is used to catch and then log traffic traversing a computer network or part of that network. A packet analyzer may also be referred to as a network analyzer, packet sniffer, or protocol analyzer. (The terms network analyzer and protocol analyzer can also have other meanings.)

Packet capture occurs when the analyzer intercepts each packet as the data streams flow throughout the network. In some cases, the analyzer is tasked with decoding raw data found in the packet in order to reveal the values of certain fields found in the packet. The contents of the packet are analyzed per the applicable specifications.

When a packet analyzer is employed to capture traffic on a wireless network, it is referred to as a wireless analyzer.

What is an IP packet?

IP (Internet Protocol) is a network layer protocol that has to do with routing. It is used to make sure packets arrive at the correct destination.

Packets are sometimes defined by the protocol they are using. A packet with an IP header can be referred to as an "IP packet." An IP header contains important information about where a packet is from (its source IP address), where it is going (destination IP address), how large the packet is, and how long network routers should continue to forward the packet before dropping it. It may also indicate whether or not the packet can be fragmented, and include information about reassembling fragmented packets.

Packets vs. datagrams:

"Datagram" is a segment of data sent over a packet-switched network. A datagram contains enough information to be routed from its source to its destination. By this definition, an IP packet is one example of a datagram. Essentially, datagram is an alternative term for "packet."

What is network traffic? What is malicious network traffic?

Network traffic is a term that refers to the packets that pass through a network, in the same way that automobile traffic refers to the cars and trucks that travel on roads.

However, not all packets are good or useful, and not all network traffic is safe. Attackers can generate malicious network traffic — data packets designed to compromise or overwhelm a network. This can take the form of a distributed denial-of-service (DDoS) attack, a vulnerability exploitation, or several other forms of cyber-attack.

Cloudflare offers several products that protect against malicious network traffic. Cloudflare Magic Transit, for instance, protects company networks from DDoS attacks at the network layer by extending the power of the Cloudflare global cloud network to on-premise, hybrid, and cloud infrastructure.

Packet Switching and Delays:

Packet Switching: Packet Switching is a method of transferring data to a network in form of packets. In order to transfer the file fast and efficiently manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**. At the destination, all these small parts (packets) have to be reassembled, belonging to the same file. A packet composes of a payload and various control information. No pre-setup or reservation of resources is needed.

Packet Switching uses **Store and Forward** technique while switching the packets; while forwarding the packet each hop first stores that packet than forward. This technique is very beneficial because packets may get discarded at any hop due to some reason. More than one path is possible between a pair of sources and destinations. Each packet contains the Source and destination address using which they independently travel through the network. In other words, packets belonging to the same file may or may not travel through the same path. If there is congestion at some path, packets are allowed to choose different paths possible over an existing network.

Packet-Switched networks were designed to overcome the ***weaknesses*** of Circuit-Switched networks since circuit-switched networks were not very effective for small messages.

Packet switching is a technique used in computer networks to transmit data in the form of packets, which are small units of data that are transmitted independently across the network. Each packet contains a header, which includes information about the packet's source and destination, as well as the data payload.

One of the main advantages of packet switching is that it allows multiple packets to be transmitted simultaneously across the network, which makes more efficient use of network resources than circuit switching. However, packet switching can also introduce delays into the transmission process, which can impact the performance of network applications.

Delay:

A **network delay** is the amount of time required for one packet to go from its source to a destination. It is also called the **end-to-end delay**, and it comprises the following 4 types of delays:

- Transmission delay
- Propagation delay
- Queuing delay
- Processing delay

1. Transmission Delay:

The **transmission delay** is the time from when the first bit of a file reaches a link to when the last bit reaches the link. The transmission delay is calculated as the ***size of the file*** divided by ***the data rate of the link***.

$$\text{transmission delay} = \frac{L\,(\text{bits})}{R\,(\text{bits/sec})} = \frac{\text{Length / Size of data packet}}{\text{Bandwidth of Network}}$$

2. Propagation Delay:

The **propagation delay** is the amount of time a bit on the link needs to travel from the source to the destination, where the speed is dependent on the medium of communication.

$$\text{Propagation delay} = \frac{d\,(\text{m})}{s\,(\text{m/s})} = \frac{\text{Distance between sender and receiver}}{\text{Transmission speed}}$$

3. Queuing Delay:

If a packet arrives at its destination and the destination is busy, it will not handle that packet immediately.

Instead, the packet has to wait in the buffer of the switch, which is called the **queuing delay**. This delay depends on the following factors:

- The number of packets arriving in a short time interval.
- The transmission capacity.
- The size of the queue.

4. Processing Delay:

The **processing delay** is the time taken by a processor to process the data packet. This delay depends on the speed of the processor.

> Queuing and processing delays do not have any calculable formulas because they are dependent on the speed of the processor.

Important Points -

Note-01:

Total delay in sending one data packet or End to End time

= Transmission delay + Propagation delay + Queuing delay + Processing delay

Note-02:

In optical fibre, transmission speed of data packet = 2.1×10^8 m/sec

- In optical fibre, signals travel with 70% speed of light.

$$\text{70\% speed of light}$$

$$= 0.7 \times 3 \times 10^8 \text{ m/sec}$$

$$= 2.1 \times 10^8 \text{ m/sec}$$

- So, consider transmission speed = 2.1×10^8 m/sec for calculations when using optical fibre.

Note-03:

Both queuing delay and processing delay are dependent on the state of the system.

This is because-

- If destination host is busy doing some heavy processing, then these delays will increase.
- If destination host is free, then data packets will be processed immediately and these delays will decrease.

Note-04:

- For any particular transmission link, bandwidth and transmission speed are always constant.
- This is because they are properties of the transmission medium.

Note-05:

Bandwidth is always expressed in powers of 10 and data is always expressed in powers of 2. (Remember while solving numerical problems). **Examples-**

- 1 kilo bytes = 2^{10} bytes
- 1 kilo bits = 2^{10} bits
- 1 Mega bytes = 2^{20} bytes
- 1 kilo bytes per second = 10^3 bytes per second
- 1 kilo bits per second = 10^3 bits per second
- 1 Mega bytes per second = 10^6 bytes per second

Switching:

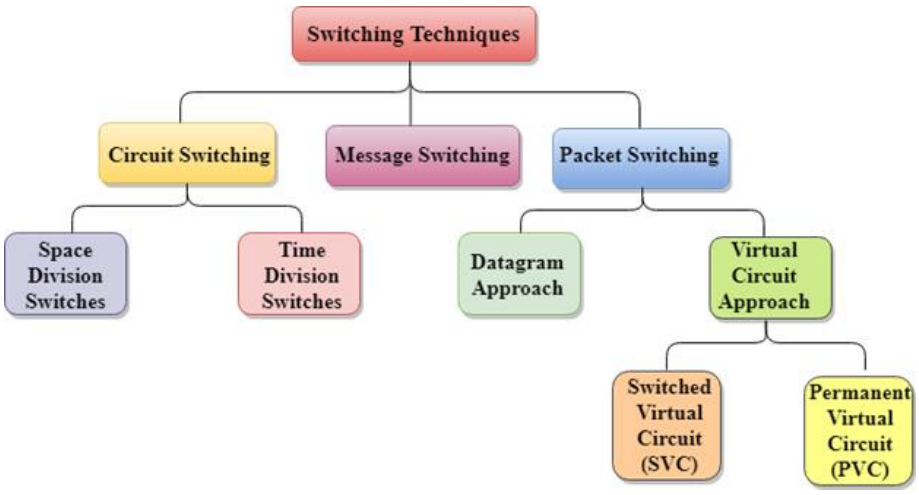
The process of moving the data packets towards their destination by forwarding them from one port to the other port is called as **switching**.

Switching Techniques:

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques:

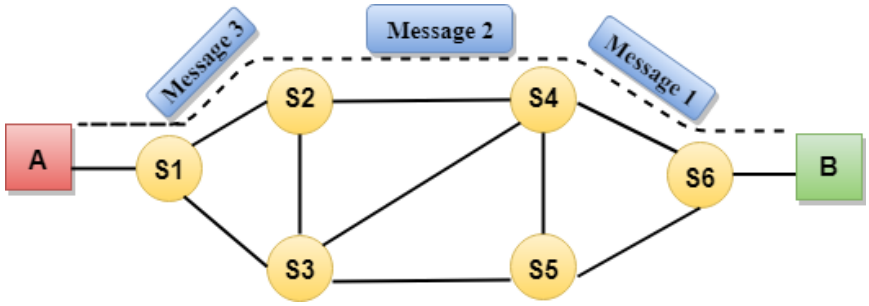


1. Circuit Switching:

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

This switching technique operates in the following three phases-

1. Establishing a circuit
2. Transferring the data
3. Disconnecting the circuit



1. Establishing A Circuit-

In this phase,

- A circuit is established between the two ends.
- Circuit provides a dedicated path for data to travel from one to the other end.
- Resources are reserved at intermediate switches which are used during the transmission.
- The intermediate switches are connected by the physical links.

2. Transferring the Data: After the circuit is established, The entire data travels over the dedicated path from one end to the other end.

3. Disconnecting the Circuit: After the data transfer is completed, the circuit is torn down i.e. disconnected.

Space Division Switches can be categorized in two ways:

- Crossbar Switch
- Multistage Switch

1. Crossbar Switch:

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

2. Multistage Switch:

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Total Time –

Total time taken to transmit a message in circuit switched network

= Connection set up time + Transmission delay + Propagation delay + Tear down time

Where:

- Transmission delay = Message size / Bandwidth
- Propagation delay = (Number of hops on way x Distance between 2 hops) / Propagation speed

Advantages-

- A well-defined and dedicated path exists for the data to travel.
- There is no header overhead.
- There is no waiting time at any switch and the data is transmitted without any delay.
- Data always reaches the other end in order.
- No re ordering is required.

Disadvantages-

- The channel is blocked for two ends only.
- It is inefficient in terms of utilization of system resources.
- The time required for establishing the circuit between the two ends is too long.
- Dedicated channels require more bandwidth.
- It is more expensive than other switching techniques.
- Routing decisions cannot be changed once the circuit is established.

Important Notes-

- Circuit switching is implemented at physical layer.
- Circuit switching is now outdated.

PRACTICE PROBLEM BASED ON CIRCUIT SWITCHING TECHNIQUE-

Problem-

Consider all links in the network use TDM with 24 slots and have a data rate of 1.536 Mbps. Assume that host A takes 500 msec to establish an end-to-end circuit with host B before begin to transmit the file. If the file is 512 kilobytes, then how much time will it take to send the file from host A to host B?

Solution-

Given-

- Total bandwidth = 1.536 Mbps
- Bandwidth is shared among 24 slots
- Connection set up time = 500 msec
- File size = 512 KB

Calculating Bandwidth Per User-

Total bandwidth = Number of users x Bandwidth per user

So, Bandwidth per user = Total bandwidth / Number of users

= 1.536 Mbps / 24 = 0.064 Mbps = 64 Kbps

Calculating Transmission Delay-

Transmission delay (T_t) = File size / Bandwidth = 512 KB / 64 Kbps

= (512 x 2^{10} x 8 bits) / (64 x 10^3 bits per sec) = 65.536 sec = 65536 msec

Calculating Time Required to Send File-

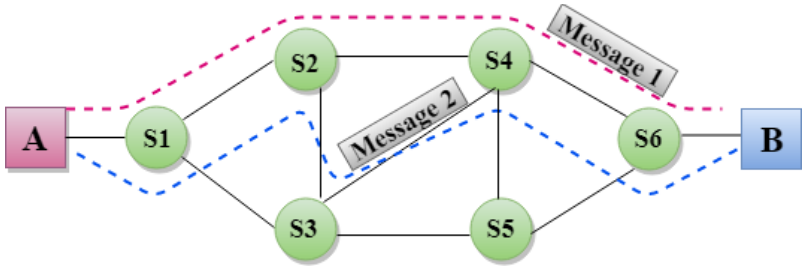
Time taken to send a file in circuit switched network

= Connection set up time + Transmission delay = 500 msec + 65536 msec

= 66036 sec = 66.036 msec

2. Message Switching:

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages-

1. It improves the channel efficiency over **Circuit Switched Network**. In circuit switched network, the channel is blocked for two ends only. But here, more devices can share the channel.

2. It is helpful in reducing traffic congestion. The message may be temporarily stored in the route and then forwarded whenever required.

3. It is helpful in setting the message priorities due to store and forward technique.

Disadvantages-

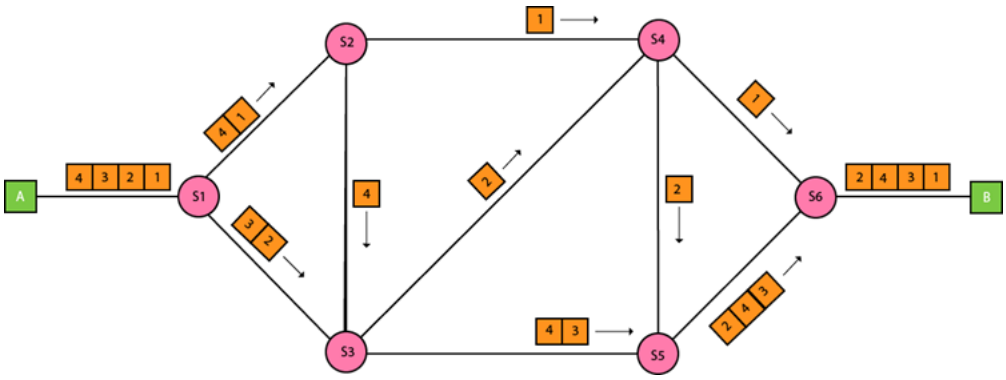
1. It requires enough storage at every switch to accommodate the entire message during the transmission.

2. It is extremely slow due to store and forward technique. Also, the message has to wait until sufficient resources become available to transfer it to the next switch.

❖ Message switching is replaced by Packet switching.

3. Packet Switching:

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Optimal Packet Size -

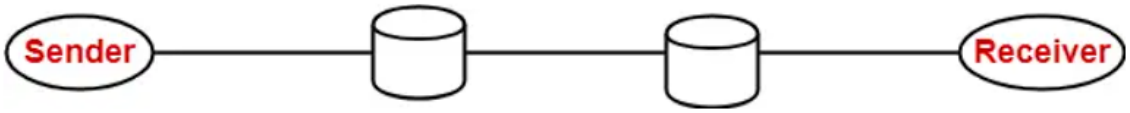
If the packet size is not chosen wisely, then-

- It may result in adverse effects.
- It might increase the time taken to transmit the message.

So, it is very important to choose the packet size wisely.

Example-

Consider- There is a network having bandwidth of 1 MBps. A message of size 1000 bytes has to be sent. Packet switching technique is used. Each packet contains a header of 100 bytes.



Out of the following, in how many packets the message must be divided so that total time taken is minimum-

1. 1 packet 2. 5 packets 3. 10 packets 4. 20 packets

NOTE:

- While calculating the total time, we often ignore the propagation delay.
- The reason is in packet switching, transmission delay dominates over propagation delay.
- This is because each packet is transmitted over the link at each hop.

Case-01: Sending Message in 1 Packet -

In this case, the entire message is sent in a single packet.

Size Of Packet-

Packet size = 1000 bytes of data + 100 bytes of header = 1100 bytes

Transmission Delay-

Transmission delay = Packet size / Bandwidth = 1100 bytes / 1 MBps

$= 1100 \times 10^{-6}$ sec = 1100 μsec = 1.1 msec

Total Time Taken-

Total time taken to send the complete message from sender to receiver

= 3 x Transmission delay = 3 x 1.1 msec = 3.3 msec

Case-02: Sending Message in 5 Packets-

In this case,

- The entire message is divided into total 5 packets.
- These packets are then sent one after the other.

Data Sent in One Packet-

Data sent in one packet = Total data to be sent / Number of packets

= 1000 bytes / 5 = 200 bytes

Size Of One Packet-

Packet size = 200 bytes of data + 100 bytes of header = 300 bytes

Transmission Delay-

Transmission delay = Packet size / Bandwidth = 300 bytes / 1 MBps

= 300 x 10^{-6} sec = 300 μsec = 0.3 msec

Time Taken By First Packet-

Time taken by the first packet to reach from sender to receiver

= 3 x Transmission delay = 3 x 0.3 msec = 0.9 msec

Time Taken By Remaining Packets-

Time taken by the remaining packets to reach from sender to receiver

= Number of remaining packets x Transmission delay = 4 x 0.3 msec = 1.2 msec

Total Time Taken-

Total time taken to send the complete message from sender to receiver

= 0.9 msec + 1.2 msec = 2.1 msec

Case-03: Sending Data in 10 packets-

In this case,

- The entire message is divided into total 10 packets.
- These packets are then sent one after the other.

Data Sent in One Packet-

Data sent in one packet = Total data to be sent / Number of packets

= 1000 bytes / 10 = 100 bytes

Size Of One Packet-

Packet size = 100 bytes of data + 100 bytes of header = 200 bytes

Transmission Delay-

Transmission delay = Packet size / Bandwidth = 200 bytes / 1 MBps

= 200 x 10^{-6} sec = 200 μsec = 0.2 msec

Time Taken By First Packet-

Time taken by the first packet to reach from sender to receiver = 3 x Transmission delay

= 3 x 0.2 msec = 0.6 msec

Time Taken By Remaining Packets-

Time taken by the remaining packets to reach from sender to receiver

= Number of remaining packets x Transmission delay = 9 x 0.2 msec = 1.8 msec

Total Time Taken-

Total time taken to send the complete message from sender to receiver

= 0.6 msec + 1.8 msec = 2.4 msec

Case-04: Sending Data in 20 Packets-

In this case, The entire message is divided into total 5 packets. And These packets are then sent one after the other.

Data Sent in One Packet-

Data sent in one packet = Total data to be sent / Number of packets

= 1000 bytes / 20 = 50 bytes

Size Of One Packet-

Packet size = 50 bytes of data + 100 bytes of header = 150 bytes

Transmission Delay-

Transmission delay = Packet size / Bandwidth = 150 bytes / 1 MBps

= 150 x 10^{-6} sec = 150 μsec = 0.15 msec

Time Taken By First Packet-

Time taken by the first packet to reach from sender to receiver

= 3 x Transmission delay = 3 x 0.15 msec = 0.45 msec

Time Taken By Remaining Packets-

Time taken by the remaining packets to reach from sender to receiver

= Number of remaining packets x Transmission delay = 19 x 0.15 msec = 2.85 msec

Total Time Taken-

Total time taken to send the complete message from sender to receiver

= 0.45 msec + 2.85 msec = 3.3 msec

Observations-

- When data is sent in 1 packet, total time taken = 3.3 msec
- When data is sent in 5 packets, total time taken = 2.1 msec
- When data is sent in 10 packets, total time taken = 2.4 msec
- When data is sent in 20 packets, total time taken = 3.3 msec

Conclusion- We conclude-

- Total time decreases when packet size is reduced but only up to a certain limit.
- If the packet size is reduced beyond a certain limit, then total time starts increasing.

From the given choices,

- Sending the message in 5 packets would be most efficient.
- In other words, packet size = 300 bytes would be the best choice.

Types/Modes/Approaches of Packet Switching:

Packet switching may be carried out in the following 2 ways-

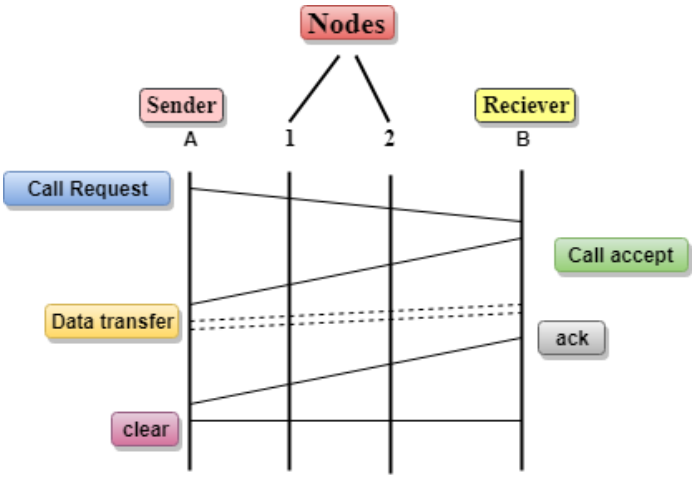
1. Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as **Connectionless Switching**.

2. Virtual Circuit Switching:

- Virtual Circuit Switching is also known as **Connection-Oriented Switching**.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.

- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

Difference Between Circuit Switching and Packet Switching -

Circuit Switching	**Packet Switching**	
	Virtual Circuit Switching	**Datagram Switching**
Connection oriented service	Connection oriented service	Connection less service
Ensures in order delivery	Ensures in order delivery	Packets may be delivered out of order
No reordering is required	No reordering is required	Reordering is required
A dedicated path exists for data transfer	A dedicated path exists for data transfer	No dedicated path exists for data transfer
All the packets take the same path	All the packets take the same path	All the packets may not take the same path
Resources are allocated before data transfer	Resources are allocated on demand using 1st packet	No resources are allocated
Stream oriented	Packet oriented	Packet oriented
Fixed bandwidth	Dynamic Bandwidth	Dynamic bandwidth
Reliable	Reliable	Unreliable
No header overheads	Only label overheads	Higher overheads
Implemented at physical layer	Implemented at data link layer	Implemented at network layer
Inefficient in terms of resource utilization	Provides better efficiency than circuit switched systems	Provides better efficiency than message switched systems
Example- Telephone systems	Examples- X.25, Frame relay	Example- Internet

PART – 2 : PHYSICAL LAYER

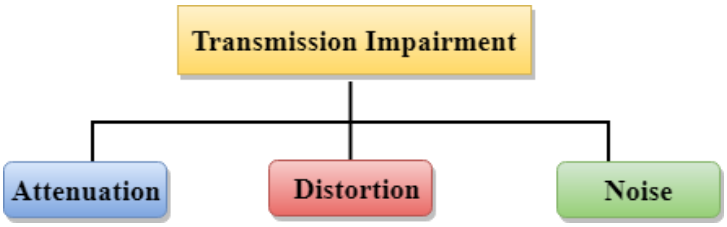
Transmission Media:

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN** (Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre-based network, the bits in the form of light pulses.
- In **OSI** (Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Some factors need to be considered for designing the transmission media:

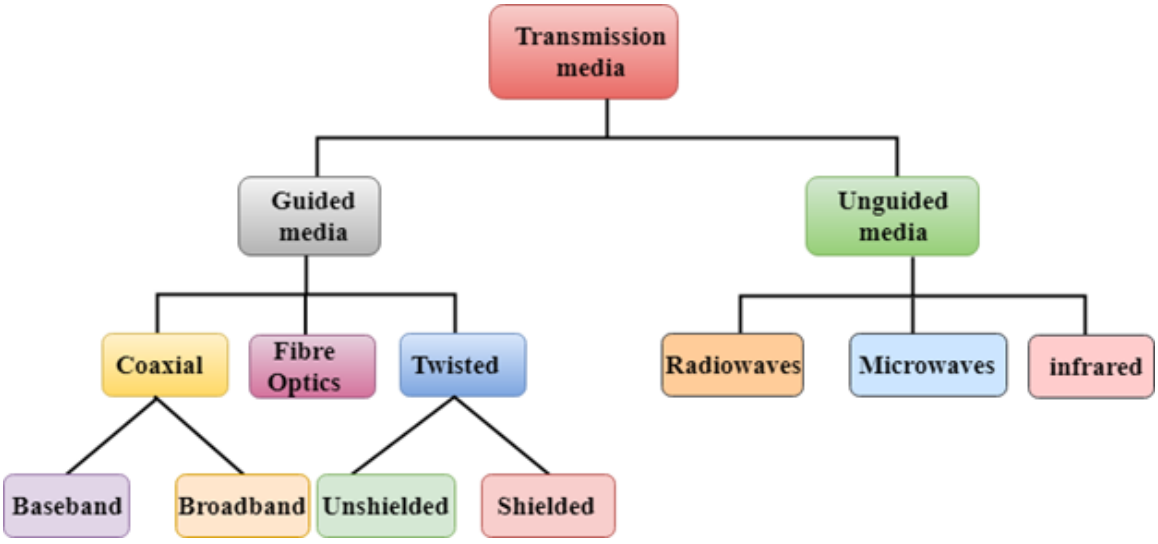
- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment:



- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Classification Of Transmission Media:



1. Guided Transmission Media:

Guided Transmission Media, also known as **Wired or Bounded transmission media**, is the physical medium through which the signals are transmitted. The transmitted signals are directed and confined in a narrow pathway using physical links.

It provides us with features like higher speeds, and better security and is used preferably for comparatively shorter distances. A signal traveling along any such media is directed and contained by the physical limits of the medium.

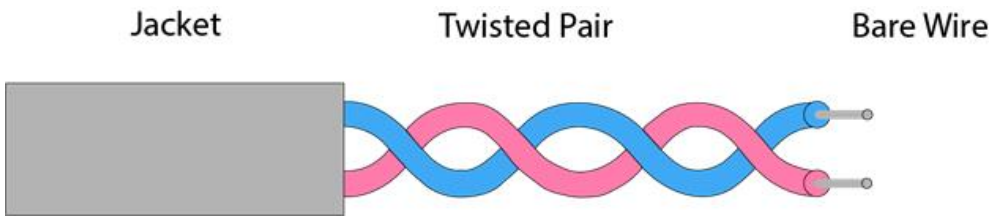
Types Of Guided media:

1. Twisted Pair:

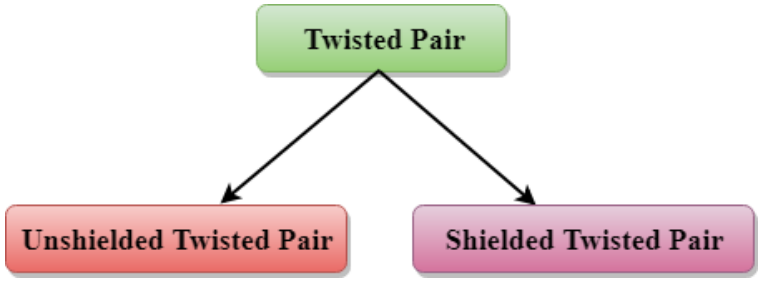
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:



1. Unshielded Twisted Pair:

UTP stands for **Unshielded Twisted Pair** cable. UTP cable is a 100-ohm copper cable that consists of 2 to 1800 unshielded twisted pairs surrounded by an outer jacket. They do not have any metallic shield. This makes the cable smaller in diameter but unprotected against electrical interference. The twist helps to improve its immunity to electrical noise and EMI. They are made up of two or four pairs of twisted cables.

Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.

Advantages of Unshielded Twisted Pair Cable:

- Easy to set up and install.
- Flexible and low-cost
- It has a high-speed capacity
- It has a 100-meter limit.
- Short-distance transmission due to attenuation.
- Sensitive to external interference.

Disadvantages of Unshielded Twisted Pair Cable:

- Limited bandwidth than Coaxial Cable
- Lesser protection from interference.
- Susceptible to noise and cross-talk.
- They can only be used for shorter distances because of attenuation.

2. Shielded Twisted Pair Cable:

STP stands for Shielded Twisted Pair cable. STP Cabling is twisted-pair cabling with additional shielding to reduce crosstalks and other forms of electromagnetic interference (EMI). This cable has a metal foil covering which encases each pair of insulated conductors. A metal casing prevents electromagnetic noise penetration.

Advantages of Shielded Twisted Pair Cable:

- It has better performance at a higher data rate than UTP.
- It eliminates crosstalk.
- Its performance is adequate.
- It can be used for Analog and Digital transmission both.
- It increases the signaling rate.
- It increases the pace of signaling.
- It has a higher capacity than protected twisted pair.

Disadvantages of Shielded Twisted Pair Cable:

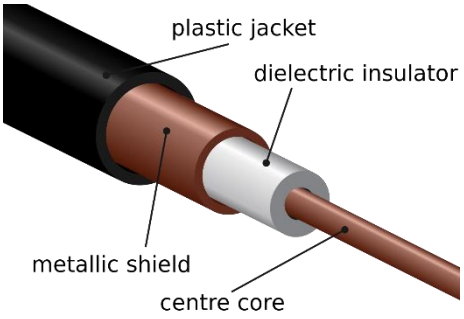
- It is more expensive and bulkier than UTP and coaxial cable.
- It has a higher attenuation rate.
- It is comparatively difficult to manufacture and install.

2. Coaxial Cable:

Coaxial cable, also known as **coax**, consists of an inner conductor surrounded by a concentric conducting shield. Coaxial Cables have an outer plastic covering containing an insulation layer made of PVC or Teflon and two parallel conductors, each having a separate insulated protection cover. The coaxial cable transmits information in baseband mode (dedicated cable bandwidth) and Broadband mode (cable bandwidth is split into distinct ranges). Cable TVs and analog television networks widely use Coaxial cables.

The most common coaxial standards are:

50-Ohm RG-7 or RG-11	Used with thick Ethernet
50-Ohm RG-58	Used with thin Ethernet
75-Ohm RG-59	Used with cable television
93-Ohm RG-62	Used with ARCNET



Coaxial cables are also classified into two types

1. Baseband Coaxial Cable
2. Broadband Coaxial Cable

1. Baseband Coaxial cable:

This is a 50 ohm (Ω) coaxial cable used for digital transmission. It is mainly used for Local Area Net. Baseband transmits one signal at a time at a very high speed. The major drawback with this is that it needs amplification after every 1000 feet.

Advantages of Baseband Coaxial cable

There are some advantages of using baseband coaxial cable:

- Baseband coaxial cable has a high bandwidth, which means it can transmit data at high speeds.
- Baseband coaxial cable is less susceptible to electromagnetic interference (EMI) than other types of cables.

- Baseband coaxial cable can transmit data over longer distances than twisted-pair cables.
- Baseband coaxial cable is highly durable and resistant to damage from physical stress or harsh environments.
- Baseband coaxial cable is relatively easy to install, as it requires fewer connectors and is less complex than other types of cables.

Disadvantages of Baseband Coaxial cable

Along with its advantages, baseband coaxial cable also has some disadvantages:

- While baseband coaxial cable can transmit data over longer distances than twisted-pair cables, it still has a limited distance capability.
- Baseband coaxial cable is thicker and less flexible than other types of cables, which can make it difficult to install, particularly in tight spaces or around corners.
- Baseband coaxial cable is more expensive than other types of cables, such as twisted-pair cables.
- Baseband coaxial cable is vulnerable to moisture and other environmental factors, which can cause signal degradation and other issues.
- Baseband coaxial cable is not compatible with all types of devices or systems, which can limit its usefulness in certain applications.

2. Broadband Coaxial Cable:

This is accomplished by using analog transmission over conventional cable television wiring. It sends several signals at the same time at various frequencies. When compared to Baseband Coaxial Cable, it covers a larger region.

Advantages of Broadband Coaxial cable

There are some advantages of using broadband coaxial cable:

- Broadband coaxial cable has a high bandwidth, transmitting data at high speeds.
- Broadband coaxial cable is thinner and more flexible than baseband coaxial cable, which makes it easier to install, particularly in tight spaces or around corners.
- Broadband coaxial cable is less susceptible to electromagnetic interference (EMI) than other types of cables.
- Broadband coaxial cables can transmit data over longer distances than twisted-pair cables.

Disadvantages of Broadband Coaxial cable

- While broadband coaxial cable can transmit data over longer distances than twisted-pair cables, it still has a limited distance capability.
- Broadband coaxial cable is not compatible with all types of devices or systems, which can limit its usefulness in certain applications.
- Broadband coaxial cable can experience signal loss or attenuation, particularly over longer distances or when multiple devices are connected to the same cable.
- Broadband coaxial cable is vulnerable to moisture and other environmental factors, which can cause signal degradation and other issues.
- Broadband coaxial cable can be difficult to troubleshoot when problems arise, particularly when multiple devices are connected to the same cable.

3. 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.

Diagrammatic representation of fibre optic cable:

Basic elements of Fibre optic cable:

- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.

- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Advantages of Fibre Optic Cable:

- Fiber optic cable offers high-speed transmission.
- They are not affected by any electromagnetic interference.
- Fiber optic cables are immune to attenuation and do not require regenerating signals even after 50+ km.
- They are lighter in weight and cannot be tapped easily.
- They are resistant to corrosive materials

Disadvantages of Fibre Optic Cable:

- Fiber optic cables are costly and difficult to install and maintain.
- They are unidirectional and provide one-way communication. To have bidirectional communication, you have to install two cables.
- They are fragile compared to standard cables.

Applications of Fibre Optic Cable:

- Telecommunications companies use optical fiber to transmit telephone signals, Internet communication, and cable television signals.
- They are also used in other industries, including medical, defense, government, industrial and commercial.
- In addition to serving the purposes of telecommunications, it is used as light guides, for imaging tools, lasers, hydrophones for seismic waves, SONAR, and as sensors to measure pressure and temperature.

2. UnGuided/ Wireless Transmission Media:

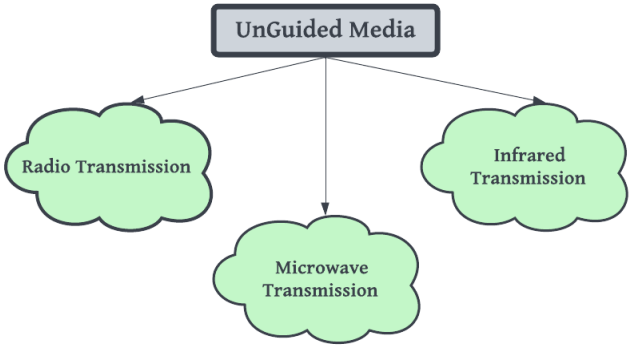
Unguided transmission media, also called **Wireless or Unbounded media**, are used to transmit data over the air or electromagnetic waves without the use of physical cables.

They offer mobility and flexibility but are also prone to interference, attenuation, and security risks. The efficiency of wireless communication can be improved by using techniques such as modulation, coding, multiple access, and smart antenna systems. Wireless communication has become increasingly important in modern society due to the growing popularity of mobile devices, IoT, and cloud computing.

Characteristics of Unguided Media:

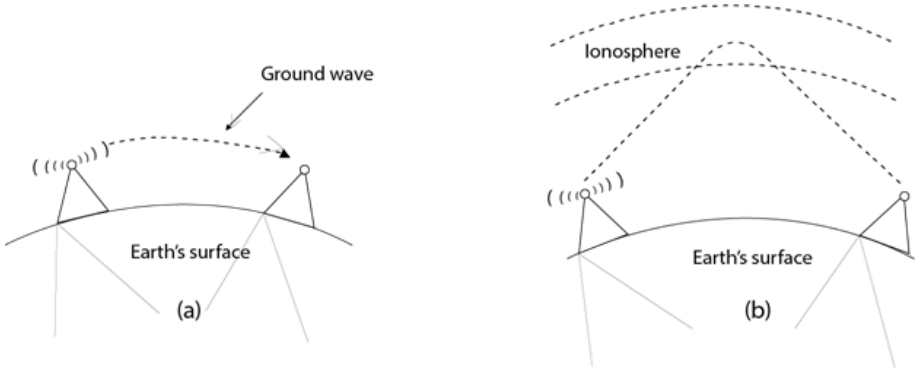
- Air is the medium through which electromagnetic energy can easily flow without any hindrance or intrusion
- Unguided signals can travel in three ways: sky propagation, ground propagation, and line-of-sight propagation
- The electromagnetic spectrum used for wireless communication ranges from 3 kHz to 900 THz
- The unguided media makes use of an **antenna** first for transmitting and receiving the electromagnetic wave

Types of Unguided Media:



1. Radio Transmission:

- Radio waves are electromagnetic waves that travel through free space in all directions.
- Radio waves are ***omnidirectional***, which means that the signals are propagated in all directions. Because radio waves are omnidirectional, they are susceptible to interference if another transmitting antenna transmits a signal with the same frequency or bandwidth.
- Radio waves have a frequency range of ***3 kHz to 1 GHz.***
- The sending and receiving antennas are not aligned in the case of radio waves, so the wave sent by the sending antenna can be received by any receiving antenna.



Advantages of Radio Transmission:

- Radio waves travel in all directions (propagated in all directions).
- It is capable of penetrating walls.

Uses of Radio Transmission:

- Wide area networks and mobile cellular phones are the most common applications.
- Multicasting is done using radio waves (one to many).

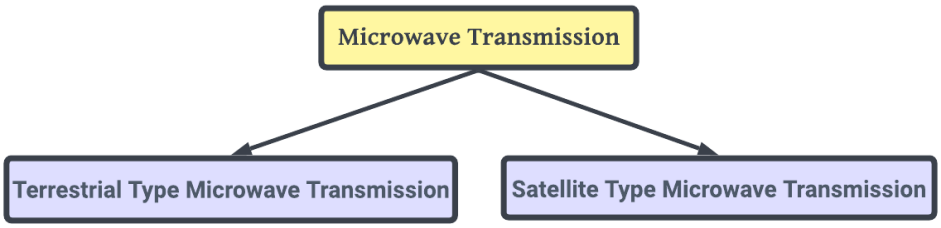
Examples of Radio Transmission

- Television
- FM radio

2. Microwave Transmission:

- Microwave transmission consists of an electromagnetic wave with a frequency range of about (1-300GHz).
- Electromagnetic waves propagate in one direction with respect to sight, preventing any intrusion.
- When the transmission medium is aligned with each other, communication between the two endpoints and the line of sight becomes much easier to establish.

Microwave Transmission is further divided into two categories:



1. Terrestrial Transmission:

- Terrestrial microwave transmission is a method of transmitting a radio signal's focused beam from one ground-based microwave transmission antenna to another
- Antennas are mounted on the towers, in this case, to send a beam to another antenna located km away
- It uses line-of-sight transmission, which means that the antennas on the towers are in direct line of sight of each other

Characteristics of Terrestrial Microwave:

- Uses high-frequency radio waves for transmission
- Requires a clear line of sight between the transmitting and receiving antennas
- It can transmit data over long distances, up to 30 miles or more
- Has a high bandwidth, allowing for fast data transfer rates

Advantages Of Terrestrial Microwave:

- Provides high-speed communication over long distances
- Has a high bandwidth, allowing for fast data transfer rates
- Offers a reliable alternative to wired communication in remote or difficult-to-access areas
- It can be quickly deployed and installed, reducing the need for expensive infrastructure
- Does not require expensive rights-of-way, as it can be installed on existing structures such as towers or buildings

Disadvantages Of Terrestrial Microwave:

- Requires a clear line of sight between the transmitting and receiving antennas, which can be obstructed by physical obstacles such as buildings or mountains
- It can be affected by weather conditions such as rain, snow, and fog, which can weaken the signal
- Requires regular maintenance to ensure the proper functioning of equipment and signal quality
- Vulnerable to interference from other microwave systems or radio devices operating on the same frequency
- Has a limited coverage area compared to satellite communication and can only transmit data up to a certain distance, typically up to 30 miles or less

2. Satellite Transmission:

- A satellite is a physical object that travels around the Earth at a set altitude
- Satellite communication is now more dependable than cable and fibre optic technologies because it is more adaptable
- We can communicate with any location on the planet using satellite communication

How Does Satellite work?

Satellites work by receiving signals from ground-based antennas and retransmitting those signals back to Earth. They orbit the Earth at a specific altitude and speed, allowing them to remain in a fixed position relative to the ground. The signals are sent to the satellite from one ground station, then relayed to another ground station to reach the desired destination. Satellites can be used for communication, weather monitoring, GPS navigation, and other applications.

Advantages Of Satellite Transmission:

- Offers a wide coverage area, making it suitable for global communication and remote areas without access to other communication infrastructure
- Provides high-speed data transfer rates, which are useful for applications such as video streaming and high-resolution imaging
- It can operate independently of existing communication infrastructure, reducing the need for expensive installations and maintenance
- It is not affected by physical obstacles, such as buildings or mountains, that can obstruct other types of communication

Disadvantages Of Satellite Transmission:

- It can be affected by atmospheric conditions, such as rain, clouds, and solar storms, which can weaken or disrupt the signal
- It can be susceptible to interference from other satellite or ground-based systems operating on the same frequency
- It can have higher latency or delay in signal transmission due to the distance between the satellite and ground stations, which can affect some applications such as real-time gaming or voice communication
- It is generally more expensive than other types of communication infrastructure, such as terrestrial or underwater cables, especially for high-bandwidth applications

3. Infrared Transmission:

- Infrared transmission is a short-range wireless communication technique
- Infrared wave transmission has a frequency range of 300 GHz to 400 THz
- It's used for short-range communication like data transmission between two cell phones, TV remote control operation, and data transfer between a computer and a mobile phone in the same confined area
- Infrared waves are regarded as a far safer form of unguided transmission medium

- Infrared waves are powerful because there is no risk of sniffing, spoofing, or other unwanted activities, as well as a low risk of vulnerable attacks

Characteristics Of Infrared:

- Infrared is an electromagnetic radiation that has a wavelength longer than visible light but shorter than radio waves
- Infrared radiation can be emitted, reflected or absorbed by an object, depending on the object's temperature and physical properties
- Infrared transmission requires a clear line of sight between the transmitter and receiver, as it cannot penetrate solid objects

Advantages Of Infrared:

- Infrared waves are used for high-frequency short-range communication
- It cannot penetrate walls

Uses Of Infrared:

- Infrared Data Association (IrDA) is a standard for communicating between devices like computers, keyboards, mice, and printers
- Wireless keywords can communicate with a computer via the IrDA port

Disadvantages Of Infrared:

- Infrared signals require a clear line of sight between the transmitter and receiver, as they cannot penetrate solid objects, which limits their range and coverage area
- Infrared communication can be affected by interference from other infrared sources or bright light sources, such as the sun or fluorescent lamps
- Infrared communication has limited bandwidth, which restricts its usefulness for applications requiring high data transfer rates
- Infrared communication is affected by weather conditions such as fog, rain, and snow, which can scatter or attenuate the signal

---