

SUBJECT: NETWORK TECHNOLOGY AND ADMINISTRATION(CS-20)

Unit 1 : Basic of Network, Network Models and LAN Sharing

Talking Point :

- ❖ Network concepts - What is network?, Use of network
- ❖ Network model -peer –to –peer, client –server
- ❖ Network Services – File ,Print ,Communication , DB, Security, Application service
- ❖ Network Access Methods - CSMA /CD, CSMA /CA ,Token passing, Polling
- ❖ Network Topologies :Bus, Ring, Star, Mesh ,Tree ,Hybrid
- ❖ Advanced Network Topologies: Ethernet, CDDI,FDDI
- ❖ Communication Methods- Unicasting, Multicasting Broadcasting
- ❖ OSIreference model
- ❖ TCP/IP network model

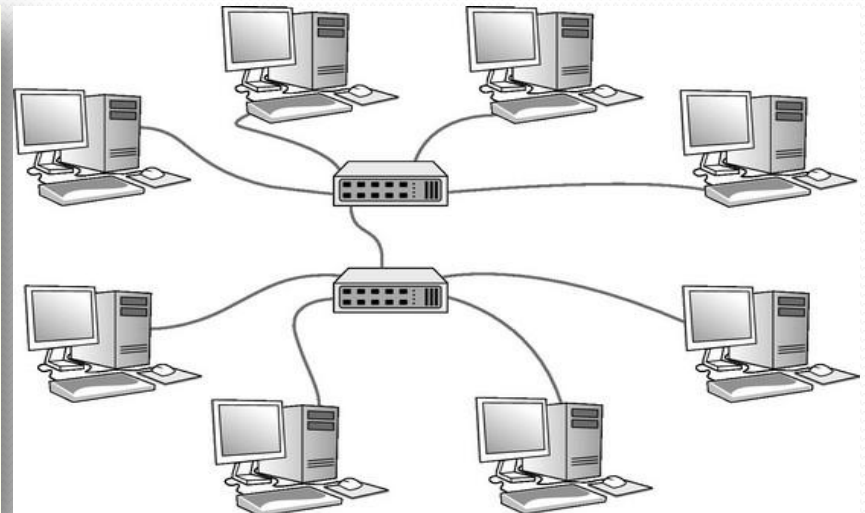
What is Network?

- A group or system of interconnected people or things.
- **Example:**
 - ✓ Group of People (Social media)
 - ✓ Railway tracks
 - ✓ Highways
 - ✓ Branch offices connected with Head Office



What is Computer Network?

- Two or more computer systems connected with each other is known as computer network.
- A computer network is a system that connects two or more computing devices (Computers, Servers, mainframes, network devices, peripherals or other devices) for transmitting and sharing information.
- **Example:**
 - ✓ Intranet



Uses of Computer Network

- Home Application

- Access to sharing remote information
On-line Publishing, digital library, www
- Person-to-person Communication
Email, instant messaging, video conferencing , E-learning
- Interactive entertainment
Video on demand(VOD), games
- E-commerce
Home shopping, electronic banking and investment, on-line Auction

- Business Application

- Resource Sharing (Printers)
- Travel Agency

- Mobile Users

Mobile computers such as notebook computers and personal digital assistants(PDAs) are one of the fastest growing segment of the computer industry.

- Many owners of these computers have desktop machines back at the office and want to be connected to their home base even when away from home.

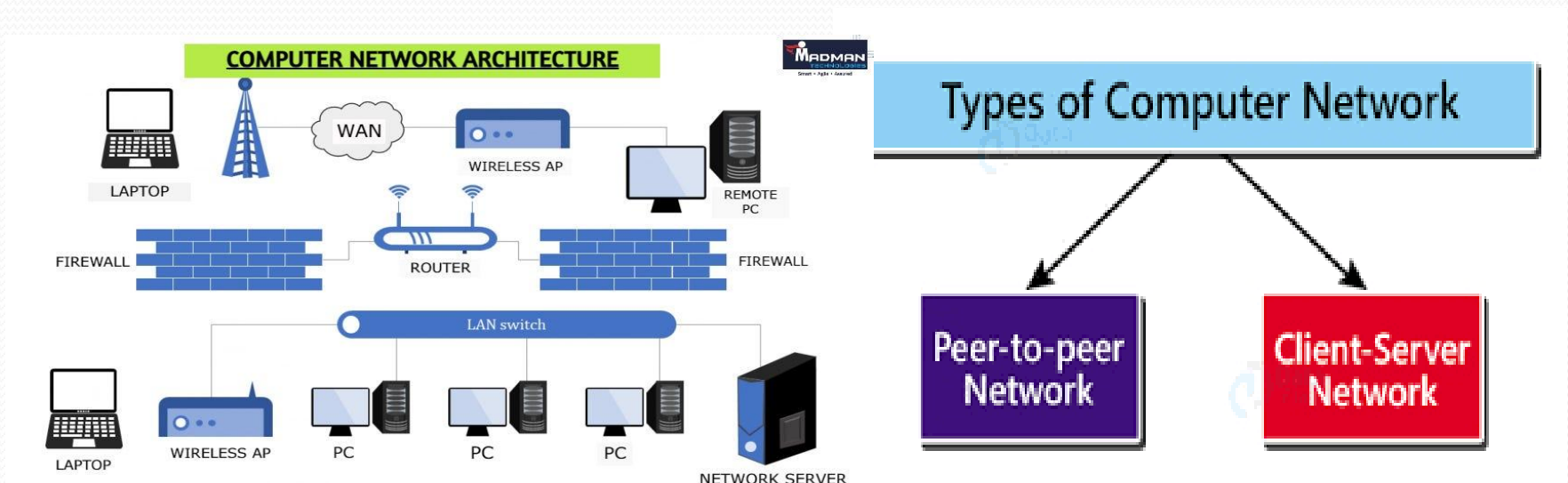
Social Issues

- Social network messages boards, content sharing sites and a host of other application allow people to share their views with different minded individual.

What are the types of computer network architecture?

What is a Computer Network Architect?

- A computer network architect sets up the computer and communication systems for a company. “Network architecture” means network layout that tells us how computers are arranged and how tasks are allocated to the computer.
- “Network architecture” means the rules, tools, and software that help people in the company stay connected without any problems.



1.Client-server architecture

- Client-server architecture also known as **request-response architecture**.
- In this architecture client makes a request to the server and server will fulfil the response.
- **Client:** When we say the word Client, it means to talk of a person or an organization using a particular service. Similarly in the digital world, a Client is a computer (Host) i.e. capable of receiving information or using a particular service from the service providers (Servers).
- **Servers:** Similarly, when we talk about the word Servers, It means a person or medium that serves something. Similarly in this digital world, a Server is a remote computer that provides information (data) or access to particular services.

Advantages:

It has a centralized system, from which data can be easily backed up.

Security is better in this network.

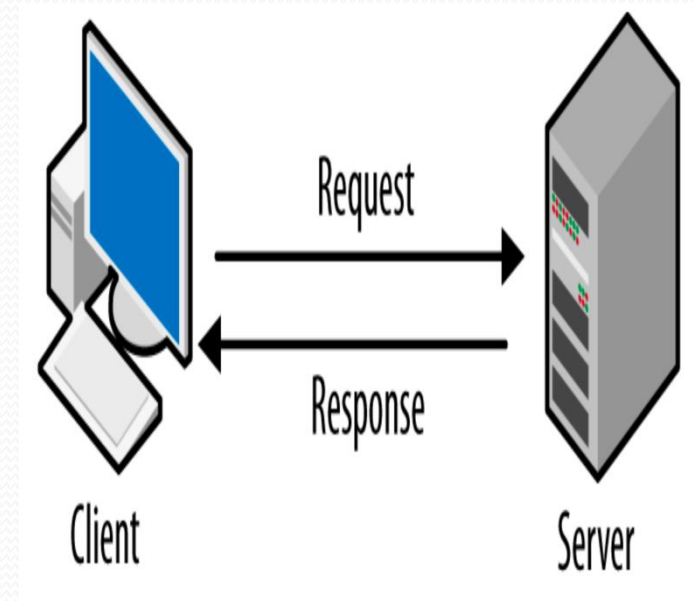
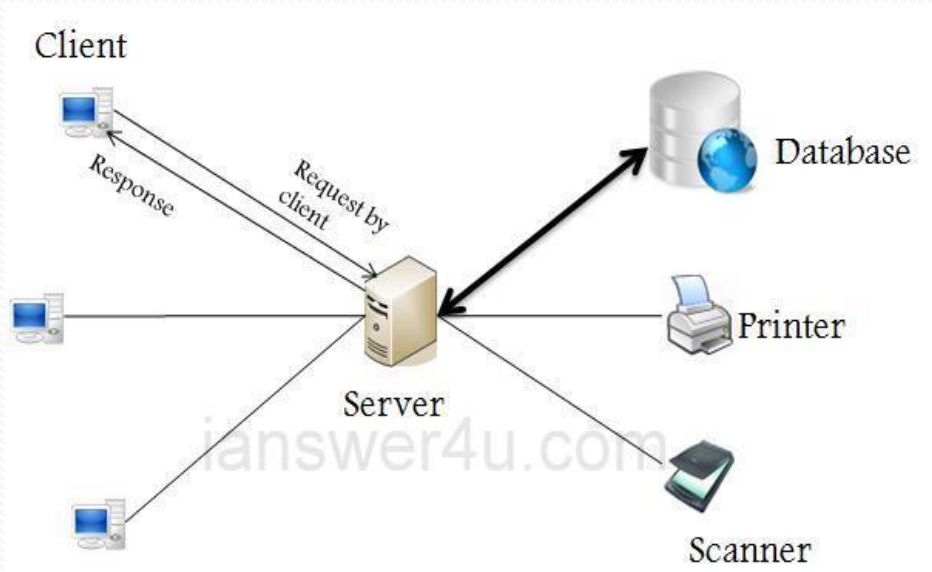
Entire system is maintained by the server.

It also increase the speed of resource sharing.

Disadvantages:

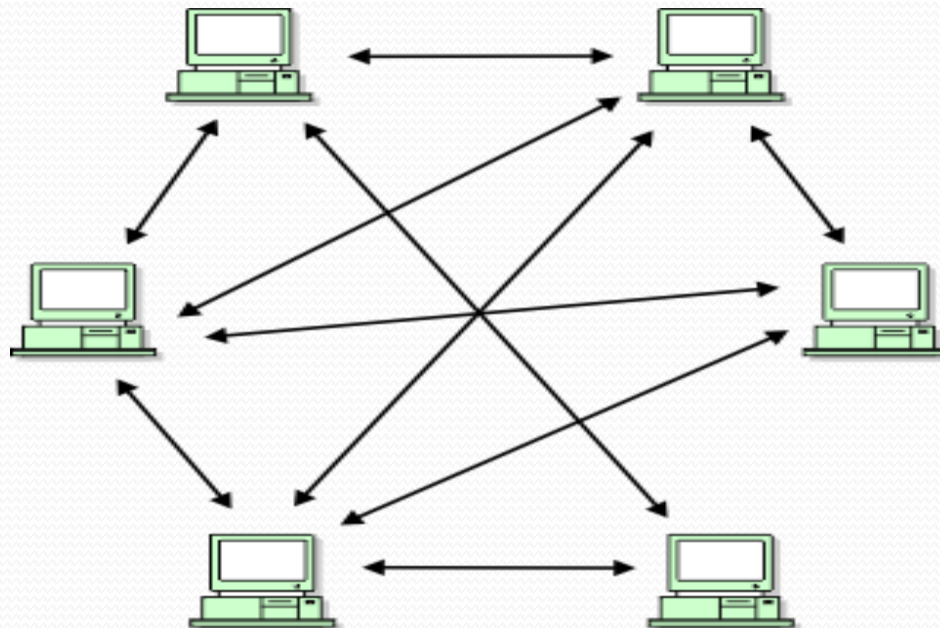
In case of server failure entire network will be failed.

Server maintenance cost is high.



2. Peer-to-Peer(P2P) architecture

- Peer-to-Peer also known as Point-to-Point network in which all the computes are directly linked together with equal privileges and responsibilities for sharing the data.
- There is no server in it.
- This P2P network is generally useful in various fields such as business, education, military , Offices etc.



Advantages

- P2P network is less costly and cheaper. It is affordable.
- P2P is very simple and not complex. This is because all computers that are connected in network communication in an efficient and well-mannered with each other.
- It is very easy and simple to set up and manage as installation and setup is less painful and computer manages itself.

Disadvantages

- Security is one of major issues in this type of network.
- We cannot backup the data because there is no server in this network.
- As the network expands in size, it may become inefficient.

Types of Network

The size of a network can be expressed by the geographic area.

•Main types

Local Area Networks (LAN)

Metropolitan Area Networks (MAN)

Wide Area Networks (WAN)

•Revised types

Personal Area Networks (PAN)

Home Area Networks (HAN)

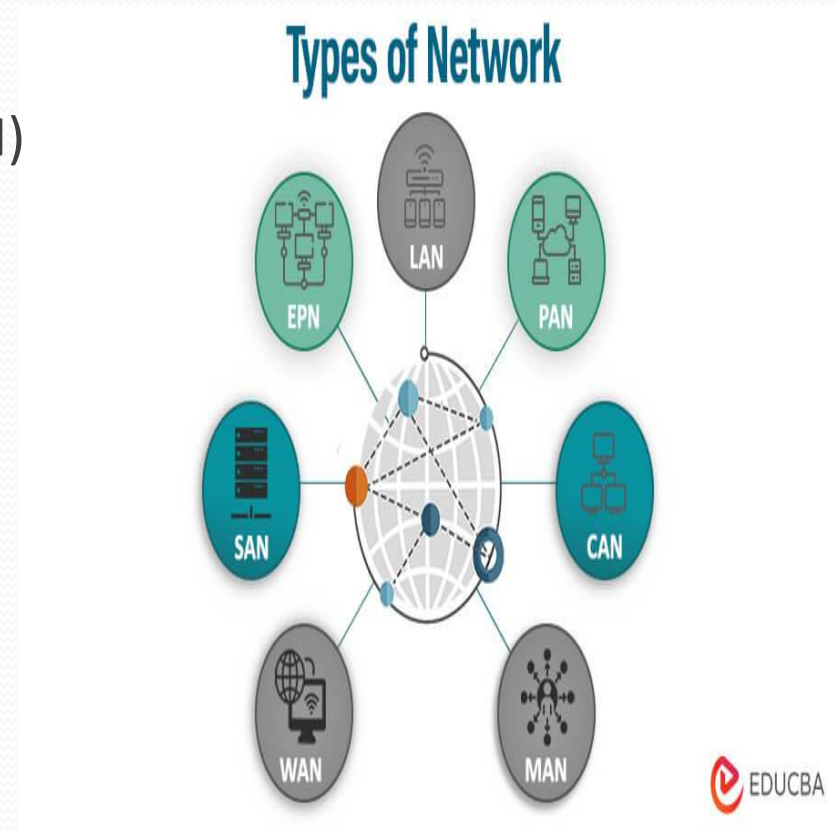
Campus Networks

Enterprise Private Networks

Backbone Networks (BBN)

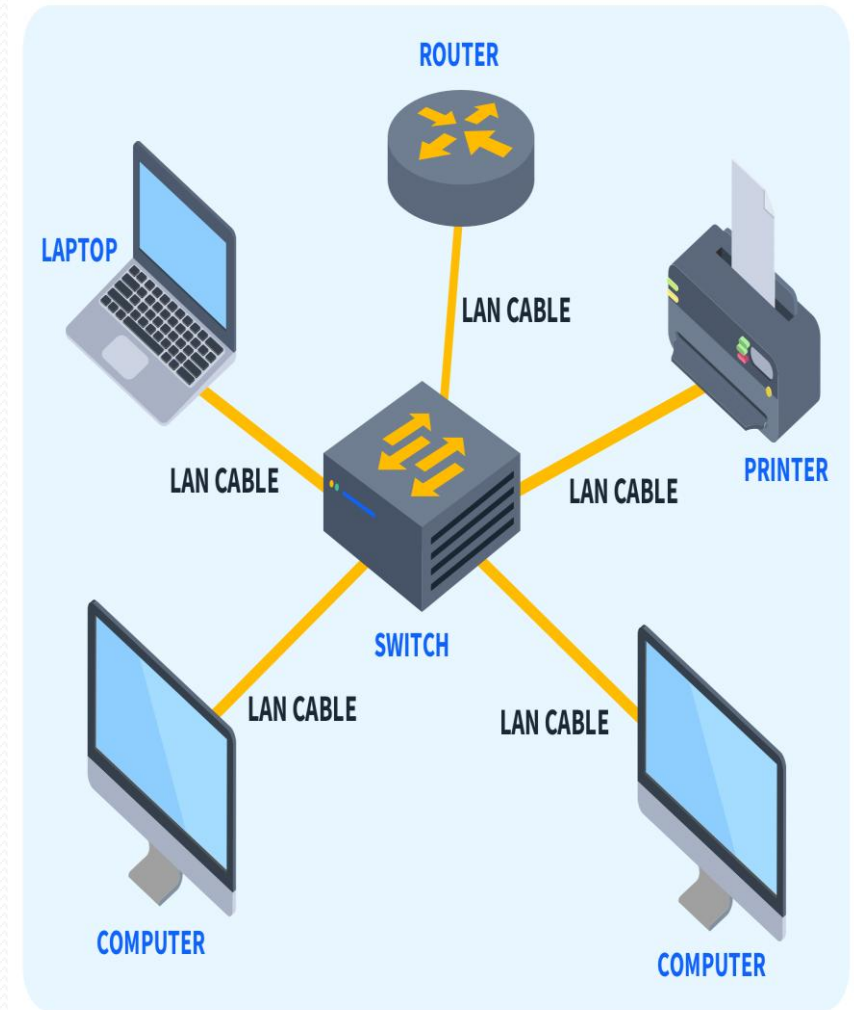
Global Area Networks (GAN)

Prepared by: Kanval Maheshwari



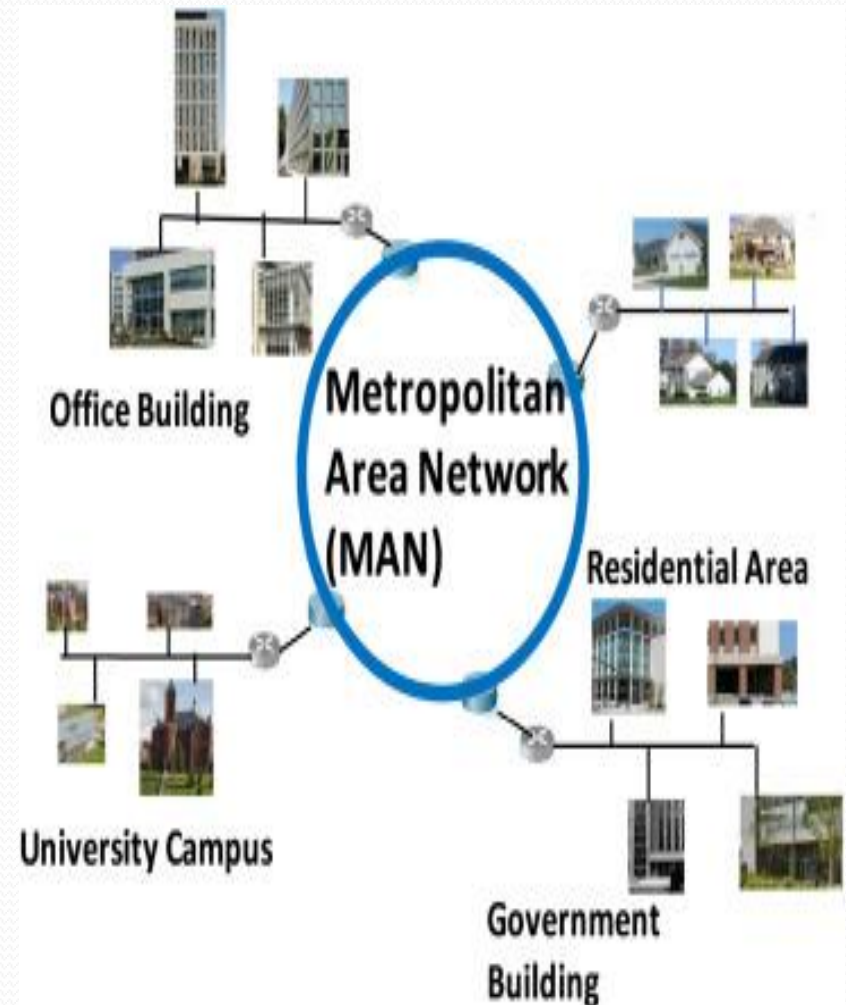
Local Area Networks (LAN)

- LAN is a group of computer and associated devices that share a common Communication line or wireless link.
- It used in small level company or organization or institute.
- Personal computers, printers, etc., are connected through LAN.
- LANs are very easy to design and troubleshoot.



MAN(Metropolitan Area Network)

- A MAN is a large computer network that usually spans a city.
- A MAN usually interconnects a number of local area network using high capacity and hi-speed technology.
- A MAN is a group of LANs. The best example of these types of network is cable television network.
- Range of MAN is 10 km to 100 km.



WAN(Wide Area Network)

- A WAN spans a large geographic area, such as a state area country.
- The World's most popular WAN is the Internet.
- WAN generally utilize different and much more expensive networking equipment than do LANs or MANs.



NETWORK SERVICES

File Services

- ❖ File services include sharing and transferring files over the network.

❖ File Sharing

- ❖ One of the reason which gave birth to networking was file sharing. File sharing enables its users to share their data with other users. User can upload the file to a specific server, which is accessible by all intended users. As an alternative, user can make its file shared on its own computer and provides access to intended users.

❖ File Transfer

- ❖ This is an activity to copy or move file from one computer to another computer or to multiple computers, with help of underlying network. Network enables its user to locate other users in the network and transfers files.

Print Service

- ❖ A print server allows printers to be shared by everyone on the network.
- ❖ Printer sharing is not as important as file sharing, but it is a useful network service.
- ❖ The advantages of printer sharing are:
 - ❖ Fewer printers are needed, and less money is spent on printers and supplies. Reduced maintenance. There are fewer machines to maintain, and fewer people spending time fiddling with printers. Access to special printers.
 - ❖ Very high-quality colour printers and very high-speed printers are expensive and needed only occasionally. Sharing these printers makes the best use of expensive resources.

Communication Services

❖ Email

- ❖ Electronic mail is a communication method and something a computer user cannot work without. Email system has one or more email servers. All its users are provided with unique IDs. When a user sends email to other user, it is actually transferred between users with help of email server.

❖ Social Networking

- ❖ Recent technologies have made technical life social. The computer savvy peoples, can find other known peoples or friends, can connect with them, and can share thoughts, pictures, and videos.

❖ Internet Chat

- ❖ Internet chat provides instant text transfer services between two hosts. Two or more people can communicate with each other using text based Internet Relay Chat services. These days, voice chat and video chat are very common.

❖ Discussion Boards

- ❖ Discussion boards provide a mechanism to connect multiple peoples with same interests. It enables the users to put queries, questions, suggestions etc. which can be seen by all other users. Other may respond as well.

Database service

- ❖ Database servers are the most common type of application servers. Because database services enable applications to be designed in separate client and server components, such applications frequently are called client/server databases.
- ❖ With a client/server database, the client and server applications are designed to take advantage of the specialized capabilities of client and database systems.
- ❖ The client application manages data input from the user, generation of screen displays, some of the reporting, and data- retrieval requests sent to the database server.
- ❖ The database server manages the database files; adds, deletes, and modifies records in the database; queries the database and generates the results required by the client; and transmits results back to the client. The database server can service requests for multiple clients at the same time.

security services

- ❖ Network security services are an intricate defensive system created to protect any computer devices and systems from potential cyber threats, data leakage, or other malicious activity. More specifically, network security protects against the following:
 - ❖ **Phishing Attacks:** Attackers steal sensitive data like passwords or credit card information.
 - ❖ **Malware:** Malware such as viruses, Trojans, and other malicious programs damage or disrupt a computer network.
 - ❖ **Unauthorized Access:** Unauthorized users gain network access.
 - ❖ **Data Leakage:** Private data is shared or made available to unauthorized parties.
 - ❖ **Brute Force:** Hackers will bombard a network with numerous and repeated login attempts.
- ❖ Security services range from proactive firewalls and malware protection to more advanced strategies such as intrusion detection and prevention, network monitoring, and identity management.

Application Services

- ❖ These are nothing but providing network based services to the users such as web services, database managing, and resource sharing.

❖ Resource Sharing

- ❖ To use resources efficiently and economically, network provides a mean to share them. This may include Servers, Printers, and Storage Media etc.

❖ Databases

- ❖ This application service is one of the most important services. It stores data and information, processes it, and enables the users to retrieve it efficiently by using queries. Databases help organizations to make decisions based on statistics.

❖ Web Services

- ❖ World Wide Web has become the synonym for internet. It is used to connect to the internet, and access files and information services provided by the internet servers.

Network Access Methods

- Network access refers to the different methods that computers use to place data on the network.
- CSMA/CD (Carrier Sense Multiple Access/Collision Detection)
- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
- Token Passing
- Polling

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

- In CSMA/CD, every host has equal access to the wire and can place data on the wire when the wire is free from traffic. When a host want to place data on the wire, it will “sense” the wire to find whether there is a signal already on the wire.
- If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium.
- if two systems place data on the medium at the same instance, they will collide with each other, destroying the data.
- If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted, to avoid collision again.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

- In CSMA/CA, before a host sends real data on the wire it will “sense” the wire to check if the wire is free.
- If the wire is free, it will send a piece of “dummy” data on the wire to see whether it collides with any other data.
- If it does not collide, the host will assume that the real data also will not collide.

Token Passing

- In CSMA/CD and CSMA/CA the chances of collisions are there. As the number of hosts in the network increases, the chances of collisions also will become more.
- In token passing, when a host want to transmit data, it should hold the token, which is an empty packet. The token is circling the network in a very high speed.
- If any workstation wants to send data, it should wait for the token. When the token has reached the workstation, the workstation can take the token from the network, fill it with data, mark the token as being use and place the token back to the ne

Polling

- The message which is sent by the primary station consists of the address of the station which is selected for granting access.
- The point to remember is that all the nodes receive the message but the addressed one responds and sends data in return, but if the station has no data to transmit then it sends a message called **Poll Reject or NAK (negative acknowledgment)**.
- But this method has some drawbacks like the high overhead of the polling messages and high dependence on the reliability of the primary station.

NETWORK TOPOLOGY

- In Computer Networking “topology “is basically defined as layout or design of the connected devices.
- The physical arrangement of the computer system/node, which is connected to each other via communication medium is called topology.
- These topology can be either physical or logical design.
- There are six different Networking Topologies :
 1. Ring Topology
 2. Star Topology
 3. Bus Topology
 4. Tree Topology
 5. mesh Topology
 6. Hybrid Topology

RING TOPOLOGY:

- Ring topology network first implement in **IBM company network**.
- Ring topology computers and other networking devices are connected to each other in a circular way, forming a closed loop.
- In this setup, each device is connected to exactly two other devices(adjacent node), creating a continuous pathway for data transmission.



Advantages:

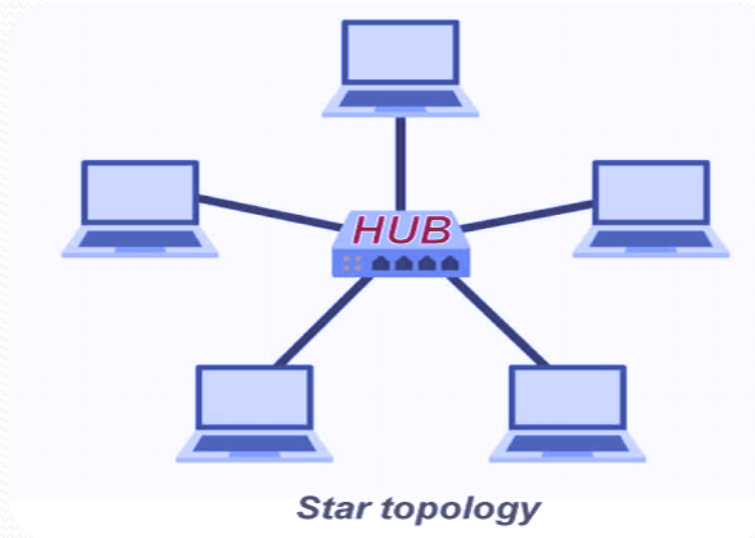
- The Ring network works well where there is no central site computer system.
- The data sent through ring topology will be broadcast.
- Transmission rate of data is very speed.

Disadvantages:

- If we want to send data from source to destination machine then data will unnecessarily be passed to all nodes.
- It is very difficult to recover the ring, if any particular machine is not working properly.
- We can't send private messages.
- Single point of failure, that means if a node goes down entire network goes down.

STAR TOPOLOGY :

- This is the most commonly used network topology design in the network topologies.
- A Star topology is a type of network topology in which all the devices or nodes are physically connected to a central device **hub, router or switches** using **unshielded twisted Pair(UTP) or Shielded Twisted Pair (STP) cable**.
- The central node (hub) acts as a server, and the connecting nodes act as clients.



Advantages:

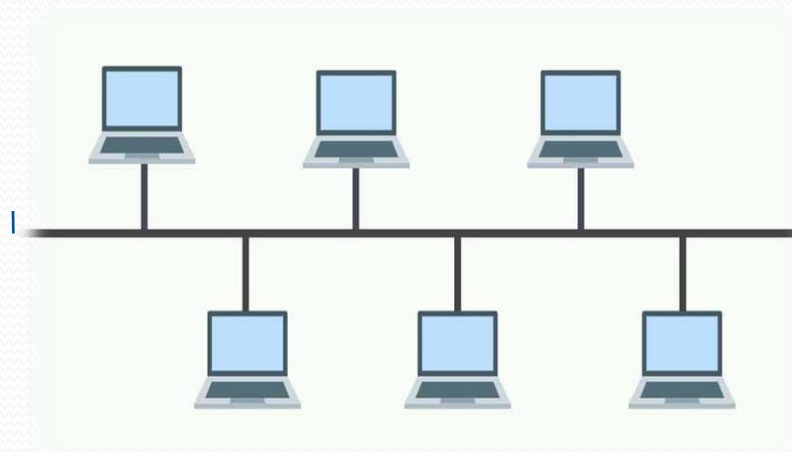
- Easy to connect new nodes without affecting rest of the network.
- Easy to delete faults.
- It broadcast the messages.

Disadvantages:

- Require more cable length than a bus topology.
- Central device failure, entire network failure.
- More Expensive than bus topology because of the cost of the hubs, switches or etc...
- If two nodes want to share the data, sharing is only possible through HUB.

BUS TOPOLOGY :

- A bus topology known as **line topology** is a topology for a Local Area Network (LAN) in which all the nodes are connected to a single cable.
- The Bus topology is one of the simplest from all types of topology. In the bus network topology, every computer is connected to a main cable .
- **The cable to which the nodes connect is called a "backbone".** If the backbone is broken, the entire segment fails.



Advantages:

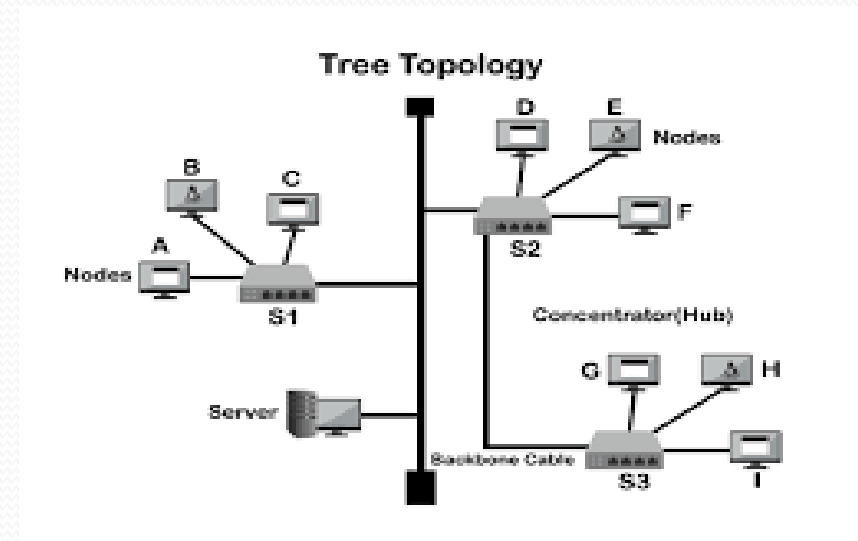
- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripherals in a linear fashion.
- it is less expensive and easy to maintain.

Disadvantages:

- The message are broadcast so, we can't send private messages.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- **Terminators** are required for both ends of the main cable.
- The length of cable is limited.
- If a main cable is damaged, the network fails or splits into two.
- In this topology data is transmitted only one direction.

TREE TOPOLOGY :

- A tree combine characteristics of bus and star topology.
- It consists of different groups of computers attached in star topology.
- The groups are then connected to a bus backbone cable.
- The topology is named tree because its shape looks like a tree with different branches of nodes.
- Tree topology is used for expansion of an existing network.



Advantages:

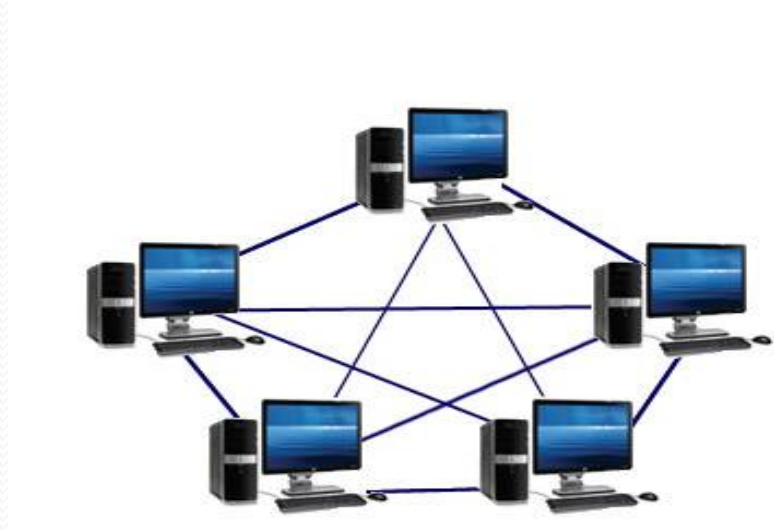
- It provides point-to-point for individual segments.
- It is supported by several hardware & software vendors.

Disadvantages:

- Overall length of each segment is limited by the type of cabling used.
- It is backbone line breaks , the entire segment goes down.
- It is more difficult to configure and wire than other topologies.

MESH TOPOLOGY :

- Mesh topology is a network configuration where devices are interconnected in a decentralized manner.
- Instead of relying on a central hub or switch, each device connects directly to multiple other devices, forming a mesh-like structure.
- In mesh topology each and every computer directly connected with all nodes ,so we can directly send the data to the destination machine without going to intermediate machine.



Advantages:

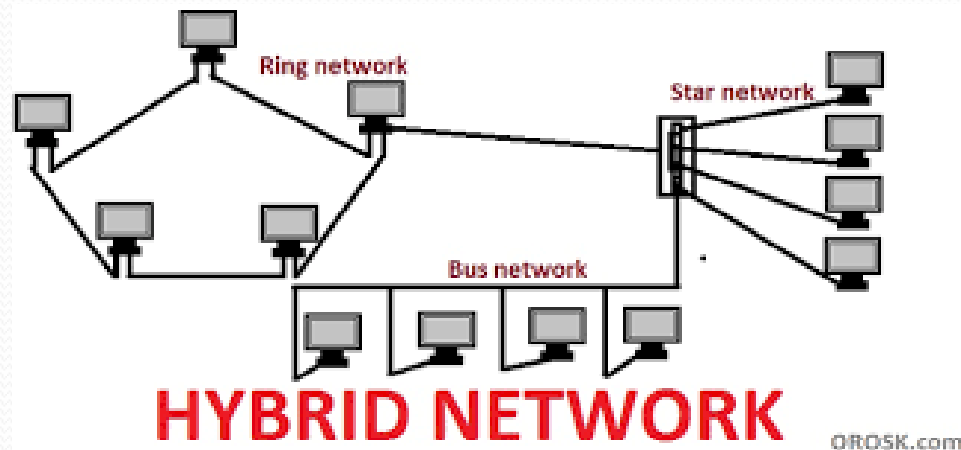
- It is very good topology to send private messages.
- All nodes are directly associated with another node so, it provide point-to-point connection.
- Un-like ring topology , if a particular machine is failed the entire network will not fail.
- Multiple devices can send or receive data simultaneously.

Disadvantages:

- It is most expensive system from the point of view of line cost. if there are (n) nodes in the network.
- Additions of the new nodes to the network are difficult.
- Configuration and maintenance cost of mesh topology is high.

HYBRID TOPOLOGY :

- A hybrid network topology is an interconnection of two or more basic network topologies, each of which contains its own nodes.
- The resulting topology will exhibit characteristics of all the constituent topologies, thereby limiting the inherent weaknesses of each topology.
- Hybrid structures are most commonly found in larger companies where individual departments have personalized network topologies adapted to suit their needs and network usage.



Advantages:

- Unlike other networks, fault detection and troubleshooting is easy in this type of topology.
- Its easy to increase the size of network by adding new components, without disturbing existing architecture.
- Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources.
- Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while there weaknesses are neutralized.

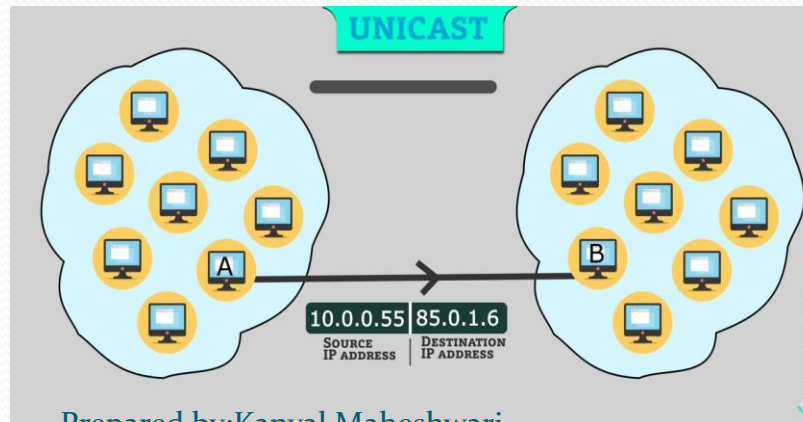
Disadvantages:

- One of the biggest drawback of hybrid topology is its design.
- Configuration and installation process needs to be very efficient.
- The hubs used to connect two distinct networks, are very expensive.

Communication Methods:

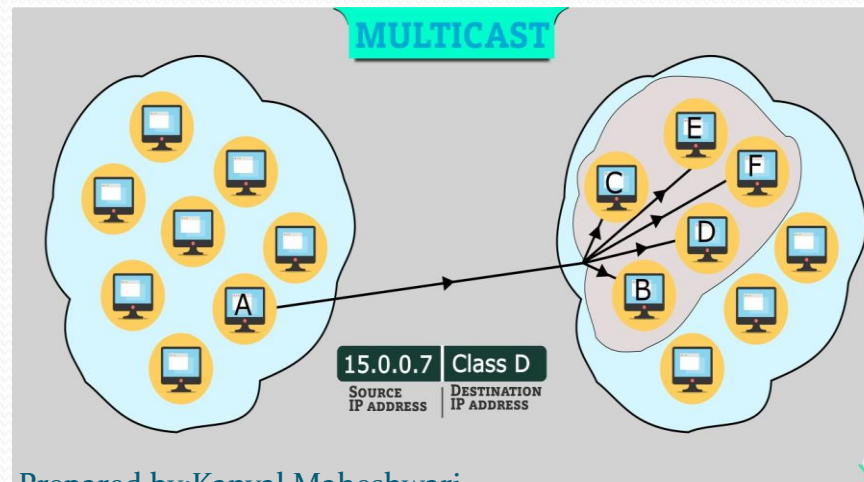
Unicast:

- This type of information transfer is useful when there is a participation of single sender and single recipient. So, in short, you can term it as a one-to-one transmission.
- For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets) to the device with IP address 20.12.4.2 in the other network, then unicast comes into the picture.
- This is the most common form of data transfer over the networks.



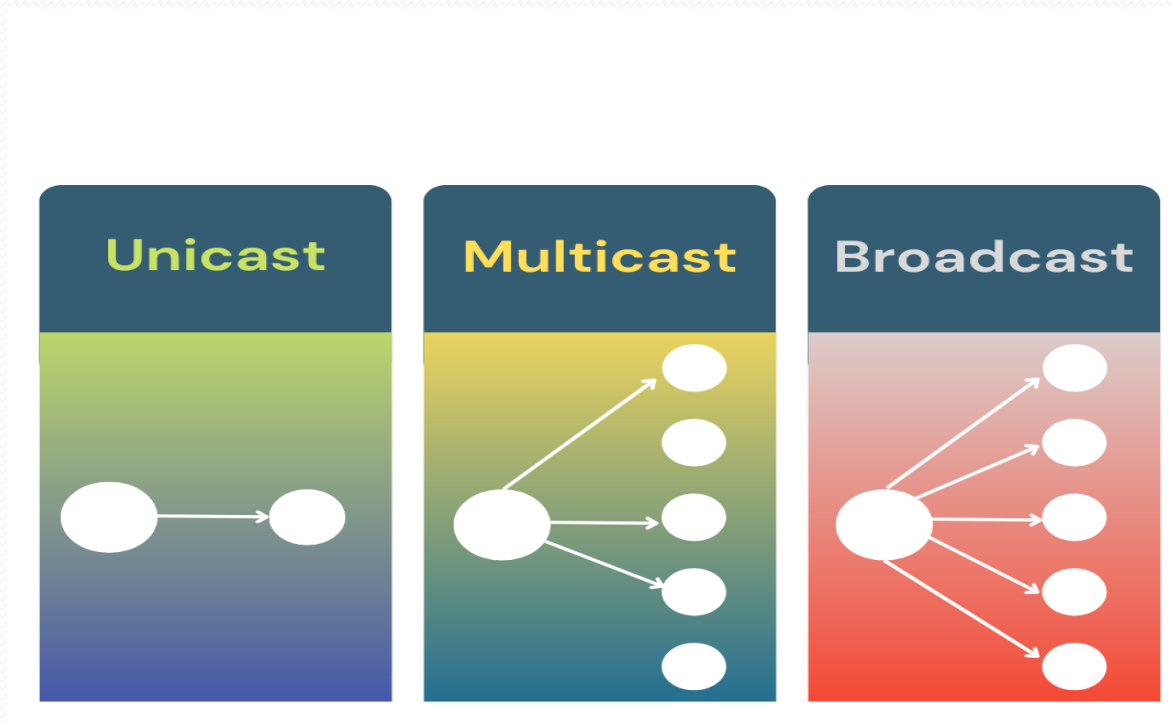
Multicast:

- In multicasting, one/more senders and one/more recipients participate in data transfer traffic.
- In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets server's direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols like IGMP (Internet Group Management Protocol), Multicast routing for its working. Also in Classful IP addressing Class D is reserved for multicast groups.



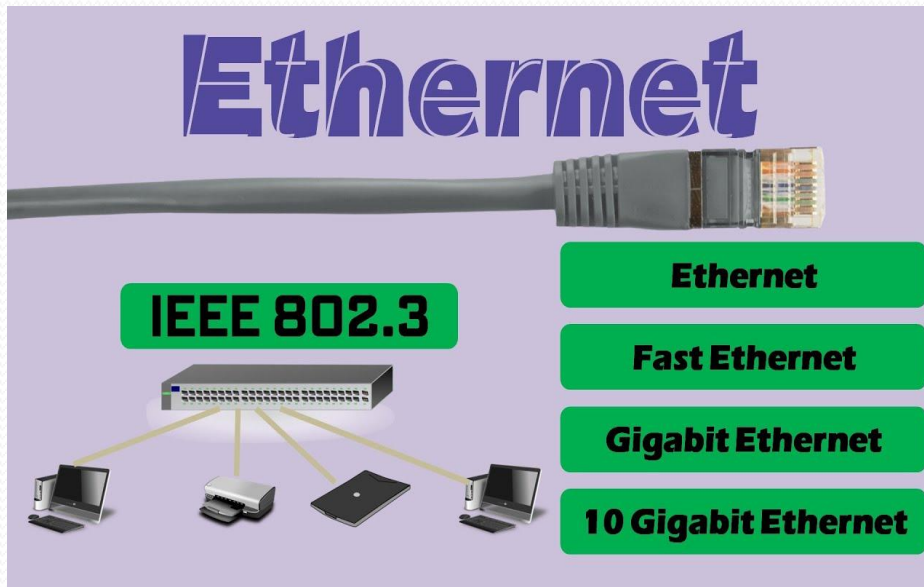
Broadcast:

- Broadcast is the term used to describe communication where a piece of information is sent from one point to all other points. In this case there is just one sender, but the information is sent to all connected receivers.

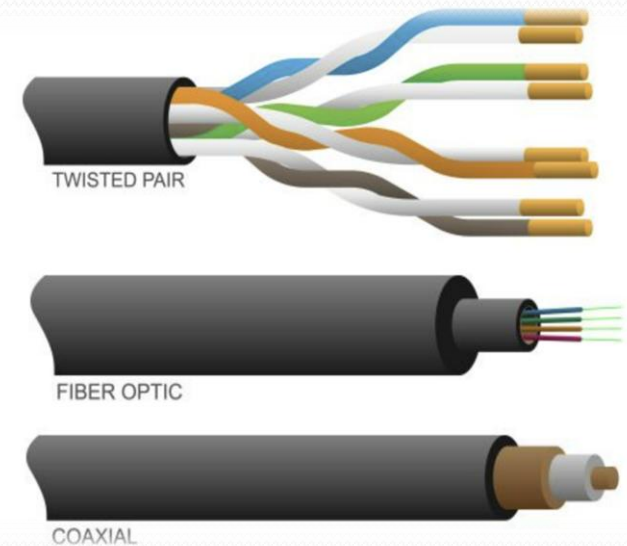


Ethernet

- Ethernet is defined as a networking technology that includes the protocol, port, cable, and computer chip needed to plug a desktop or laptop into a local area network (LAN) for speedy data transmission via coaxial or fiber optic cables.
- Introduced in 1993 and standardized in 1985 as IEEE standard project 802.3
- Types of Ethernet:

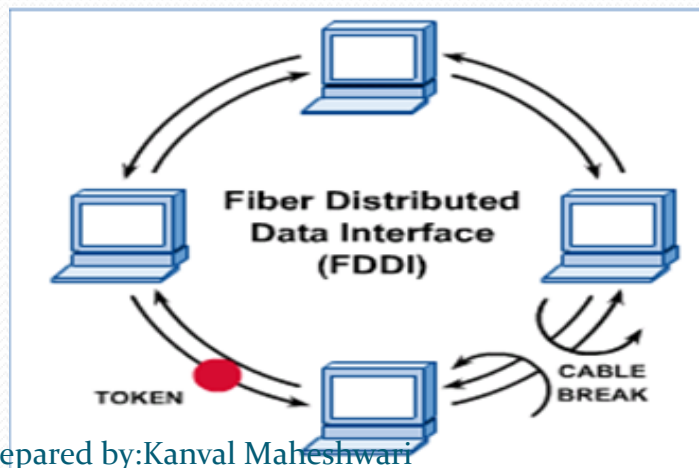


* Types of Cable:



FDDI

- **Fiber Distributed Data Interface** is a network technology that works on the OSI model's physical and data link layer.
- It derives its transmission protocol from IEEE 802.4 and follows the ANSI standard. It transmits data faster than existing ethernet technology, which was 10 Mbps ethernet.
- The **Fiber Distributed Data Interface** is suitable for LANs, MANs, and CANs but not ideal for a WAN due to some limitations, like low coverage (can extend in range up to 200 kilometres (124 miles).) and the requirement of repeaters at frequent intervals.



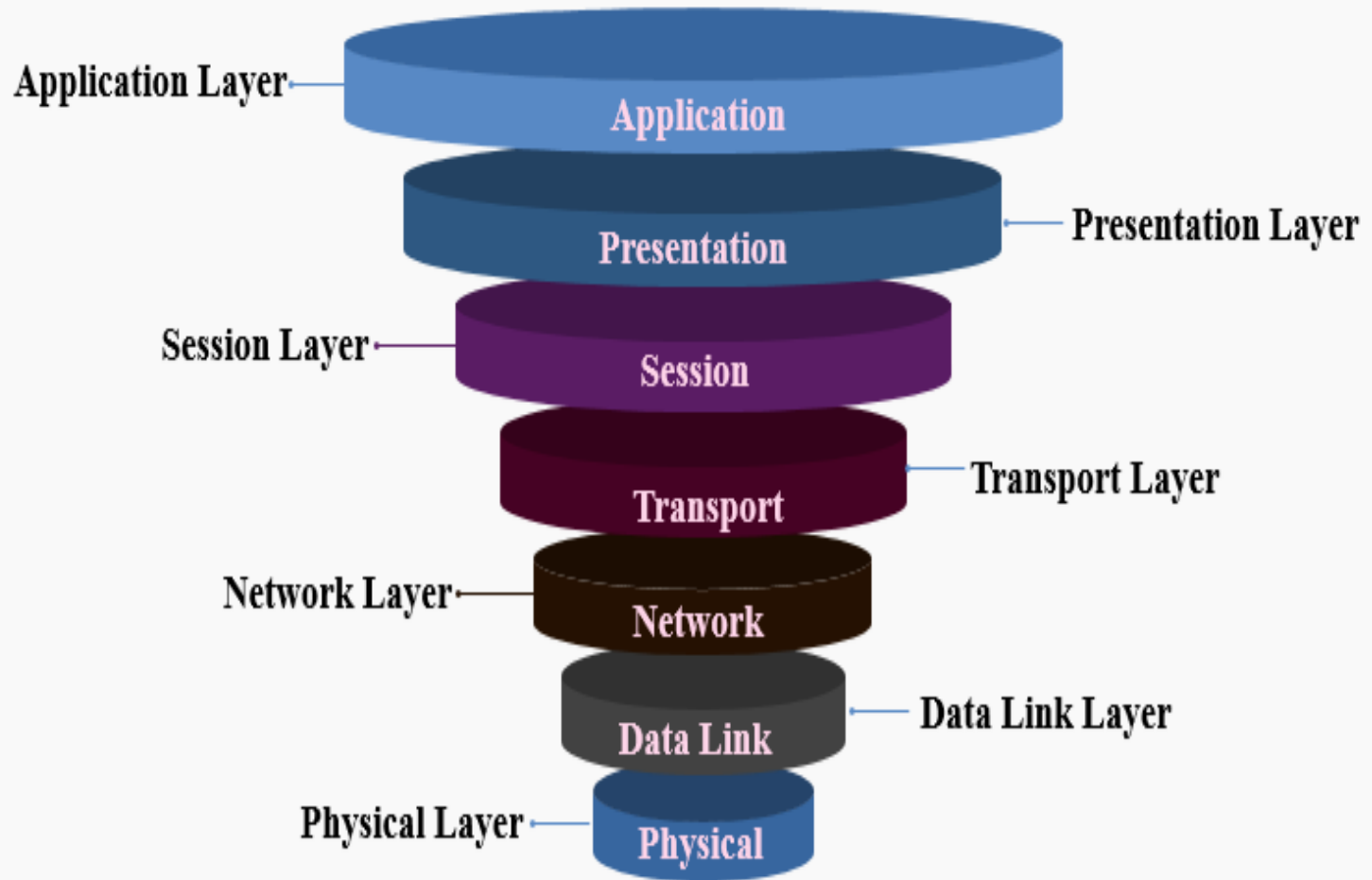
CDDI

- Copper data distribution interface (CDDI) is an implementation of fiber distributed data interface (FDDI) networking.
- CDDI uses cabling, which is unshielded twisted pair cables (UTP) made of copper. CDDI also uses the same protocols and constructs as FDDI, but uses copper wire as the medium.
- CDDI/FDDI was considered a good system for implementing a campus network backbone in the early to mid 1990s. However, it has since been rendered obsolete by Ethernet and then Gigabit Ethernet and is no longer used.
- CDDI is commonly implemented in a wide geographical area.

OSI REFERENCE MODEL

- Open System Interconnection(OSI)Model is a reference model developed by International Organization for Standardization(ISO) in 1984.
- Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- This model define 7 Layers that describe how application running upon network aware devices many communicate with each other.
- the seven layers of the OSI model can be divided into two groups:
- upper layers 7,6, & 5)and Lower layers 4,3,2,1).
- The upper layers of the OSI model deal with application issues and generally are implemented only in software.
- The lower layers of the OSI model deal with data communication using different hardware's like hub, switch, and routers.

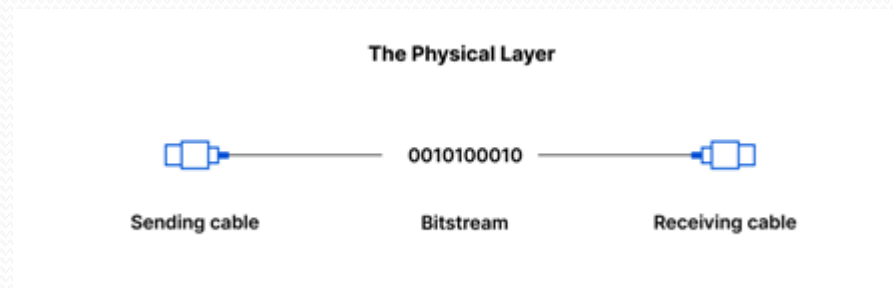
OSI Model



LAYER-1 PHYSICAL LAYER

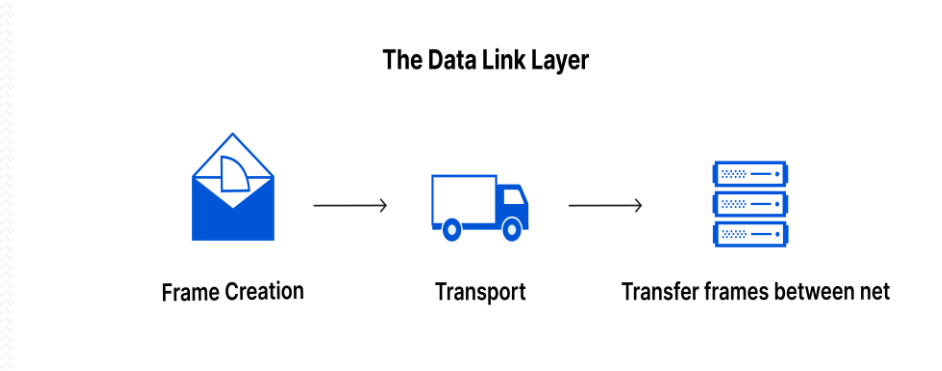
- This layer includes the physical equipment involved in the data transfer, such as the cables and switches.
- This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s.
- The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

Note: The Physical Layer of the OSI model is only part of a LAN (Local Area Network)



LAYER-2 DATA LINK LAYER

- The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the same network.
- The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).



LAYER-3 NETWORK LAYER

- The network layer is responsible for facilitating data transfer between two different networks.
- If the two devices communicating are on the same network, then the network layer is unnecessary.
- The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.
- Network layer protocols include IP, the Internet Control Message Protocol (ICMP), the Internet Group Message Protocol (IGMP), and the IPsec suite.

The Network Layer



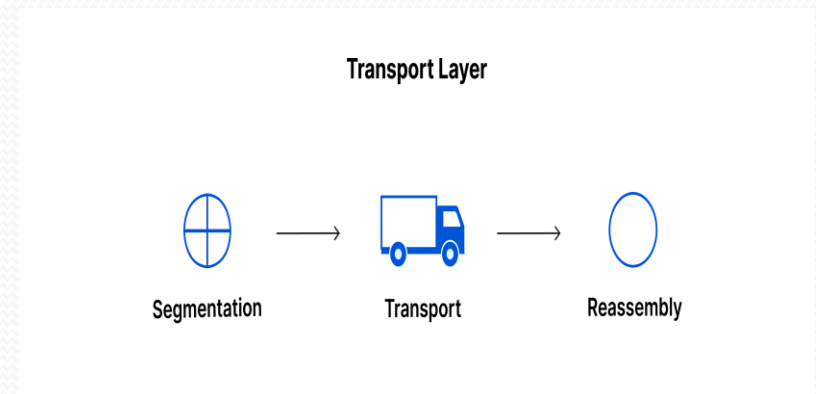
Packets Creation

Transport

Packets Assembly

LAYER-4 TRANSPORT LAYER

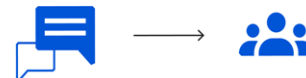
- Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3.
- The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.
- The transport layer is also responsible for flow control and error control. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.
- Transport layer protocols include the Transmission Control Protocol (TCP) & the User Datagram Protocol (UDP).



LAYER-5 SESSION LAYER

- This is the layer responsible for opening and closing communication between the two devices. **The time between when the communication is opened and closed is known as the session.** The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.
- The session layer also synchronizes data transfer with checkpoints. **For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.**

The Session Layer



Session of communication

LAYER-6 PRESENTATION LAYER

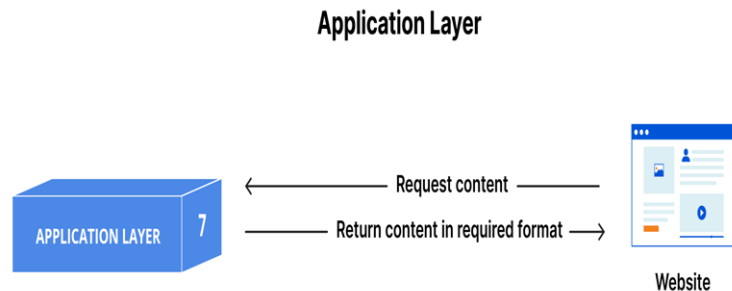
- This layer is primarily responsible for preparing data so that it can be used by the application layer. **The presentation layer is responsible for translation, encryption, and compression of data.**
- Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.
- If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.
- Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

The Presentation Layer

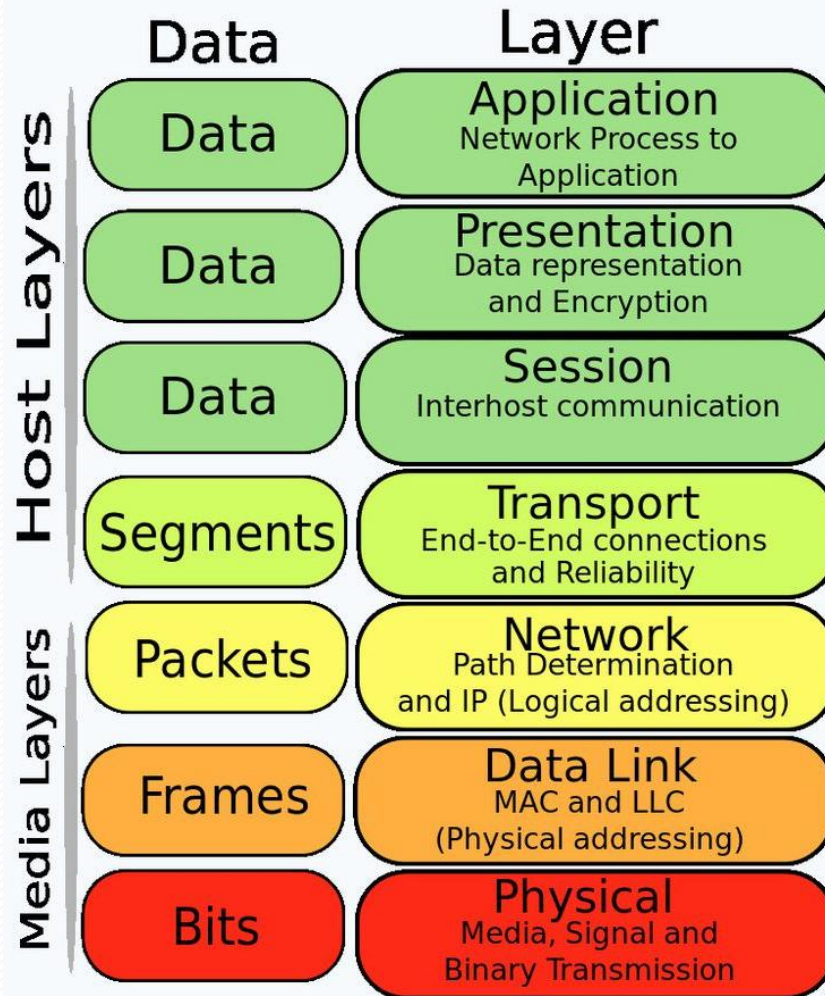


LAYER-7 APPLICATION LAYER

- This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications.
- But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user.
- Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email (communications))

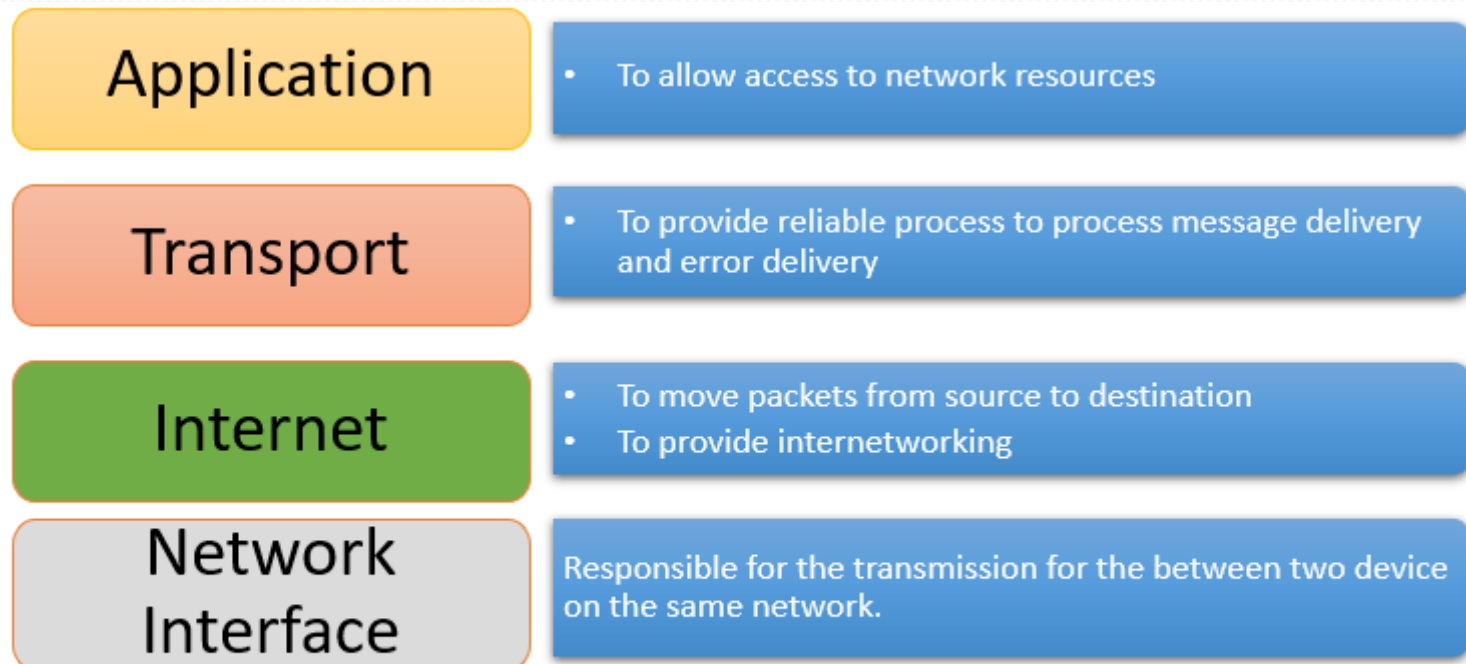


OSI Model



TCP/IP

- TCP/IP model, it was designed and developed by Department of Defence (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. **The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.**



Four Layers of TCP/IP model

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.
- Application layer interacts with software applications to implement communicating component. 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.

TRANSPORTLAYER

- Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. 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 de-segmentation.
- 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.

INTERNET LAYER

- An internet layer is a second layer of TCP/IP layers of the TCP/IP model. It is also known as a network layer.
- The main work of this layer is to send the packets from any network, and any computer should reach the destination irrespective of the route they take.
- The Internet layer offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks.
- Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Network Interface LAYER

- This layer is also called a network access layer. It helps you to defines details of how data should be sent using the network.
- It also includes how bits should optically be signaled by hardware devices which directly interfaces with a network medium, like coaxial, optical, coaxial, fiber , or twisted-pair cables.
- A network layer is a combination of the data link and physical layer of OSI. This layer defines how the data should be sent physically through the network.
- This layer is responsible for the transmission of the data between two devices on the same network.