1. Network Concepts, Classification and Components

A) Introduction, Features and Advantages of Network, Networking Criteria:-

A **network** is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data. An excellent example of a network is the Internet, which connects millions of people all over the world. Below is an example image of a home network with multiple computers and other **network devices** all connected to each other and the Internet.

List of Advantages of Computer Networking

1. **It enhances communication and availability of information.**

Networking, especially with full access to the web, allows ways of communication that would simply be impossible before it was developed. Instant messaging can now allow users to talk in real time and send files to other people wherever they are in the world, which is a huge boon for businesses. Also, it allows access to a vast amount of useful information, including traditional reference materials and timely facts, such as news and current events.

2. **It allows for more convenient resource sharing.**

This benefit is very important, particularly for larger companies that really need to produce huge numbers of resources to be shared to all the people. Since the technology involves computer-based work, it is assured that the resources they wanted to get across would be completely shared by connecting to a computer network which their audience is also using.

3. **It makes file sharing easier.**

Computer networking allows easier accessibility for people to share their files, which greatly helps them with saving more time and effort, since they could do file sharing more accordingly and effectively.

4. **It is highly flexible.**

This technology is known to be very flexible, as it gives users the opportunity to explore everything about essential things, such as software without affecting their functionality. Plus, people will have the accessibility to all information they need to get and share.

5. **It is an inexpensive system.**

Installing networking software on your device would not cost too much, as you are assured that it lasts and can effectively share information to your peers. Also, there is no need to change the software regularly, as mostly it is not required to do so.

6. **It increases cost efficiency.**

With computer networking, you can use a lot of software products available on the market which can just be stored or installed in your system or server, and can then be used by various workstations.

7. **It boosts storage capacity.**

Since you are going to share information, files and resources to other people, you have to ensure all data and content are properly stored in the system. With this networking technology, you can do all of this without any hassle, while having all the space you need for storage.

List of Disadvantages of Computer Networking

1. It lacks independence.

Computer networking involves a process that is operated using computers, so people will be relying more of computer work, instead of exerting an effort for their tasks at hand. Aside from this, they will be dependent on the main file server, which means that, if it breaks down, the system would become useless, making users idle.

2. It poses security difficulties.

Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.

3. It lacks robustness.

As previously stated, if a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To deal with these problems, huge networks should have a powerful computer to serve as file server to make setting up and maintaining the network easier.

4. It allows for more presence of computer viruses and malware.

There would be instances that stored files are corrupt due to computer viruses. Thus, network administrators should conduct regular check-ups on the system, and the stored files at the same time.

5. Its light policing usage promotes negative acts.

It has been observed that providing users with internet connectivity has fostered undesirable behavior among them. Considering that the web is a minefield of distractions—online games, humor sites and even porn sites—workers could be tempted during their work hours. The huge network of machines could also encourage them to engage in illicit practices, such as instant messaging and file sharing, instead of working on work-related matters. While many organizations draw up certain policies on this, they have proven difficult to enforce and even engendered resentment from employees.

6. It requires an efficient handler.

For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.

7. It requires an expensive set-up.

Though computer networks are said to be an inexpensive system when it is already running, its initial set up cost can still be high depending on the number of computers to be connected. Expensive devices, such as routers, switches, hubs, etc., can add up to the cost. Aside from these, it would also need network interface cards (NICs) for workstations in case they are not built in.

Criteria for a Data Communication Network

The major criteria that a Data Communication Network must meet are:

1. **Performance**

   Performance is the defined as the rate of transferring error free data. It is measured by the Response Time. Response Time is the elapsed time between the end of an inquiry and the beginning of a response. Request a file transfer and start the file transfer. Factors that affect Response Time are:

i. Number of Users: More users on a network - slower the network will run
ii. Transmission Speed: speed that data will be transmitted measured in bits per second (bps)
iii. Media Type: Type of physical connection used to connect nodes together
iv. Hardware Type: Slow computers such as XT or fast such as Pentiums
v. Software Program: How well is the network operating system (NOS) written

2. **Consistency**

   Consistency is the predictability of response time and accuracy of data. Users prefer to have consistent response times, they develop a feel for normal operating conditions. For example: if the "normal" response time is 3 sec. for printing to a Network Printer and a response time of over 30 sec happens, we know that there is a problem in the system! Accuracy of Data determines if the network is reliable! If a system loses data, then the users will not have confidence in the information and will often not use the system.

3. **Reliability**

   Reliability is the measure of how often a network is useable. MTBF (Mean Time Between Failures) is a measure of the average time a component is expected to operate between failures. Normally provided by the manufacturer. A network failure can be: hardware, data carrying medium and Network Operating System.

4. **Recovery**

   Recovery is the Network's ability to return to a prescribed level of operation after a network failure. This level is where the amount of lost data is nonexistent or at a minimum. Recovery is based on having Back-up Files.

5. **Security**

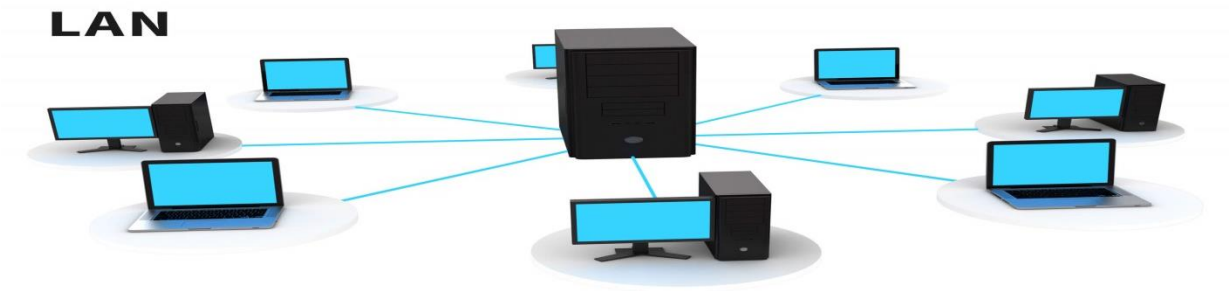
   Security is the protection of Hardware, Software and Data from unauthorized access. Restricted physical access to computers, password protection, limiting user privileges and data encryption are common security methods. Anti-Virus monitoring programs to defend against computer viruses are a security measure.

B) Types of Network

i. LAN

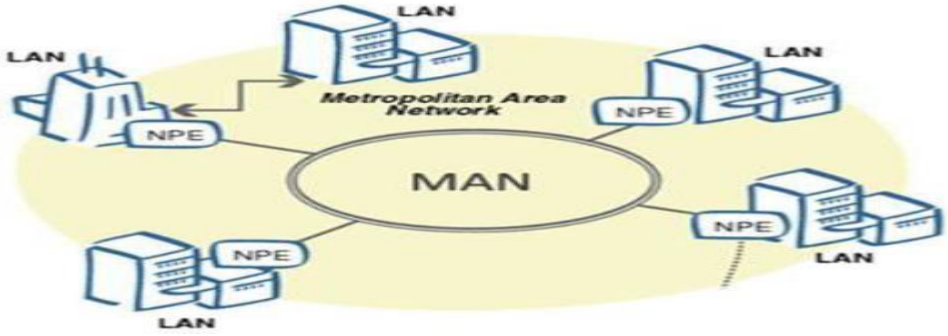
LAN refers to a group of computers that all belong to the same organization and that are linked within a small geographic area using a network and often the same technology (the most widespread being Ethernet).

A local area network is a network in its simplest form. Data transfer speeds over a local area network can reach up to 10 Mbps, such as for an Ethernet network, and 1 Gbps, as with FDDI or Gigabit Ethernet. A local area network can reach as many as 100, or even 1000, users.
By expanding the definition of a LAN to the services that it provides, two different operating modes can be defined: in a "peer-to-peer" network, in which communication is carried out from one computer to another, without a central computer, and where each computer has the same role; or in a "client/server" environment, in which a central computer provides network services to users.



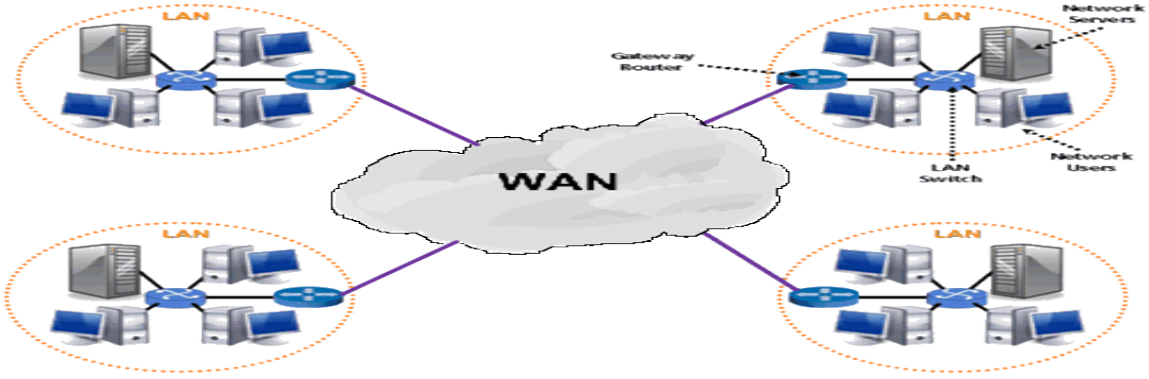
ii. MANs

MANs connect multiple geographically close LANs (over an area of up to several dozen miles) to one another at high speeds. Thus, a MAN lets two remote nodes communicate as if they were part of the same local area network. A MAN is made from switches or routers connected to one another with high-speed links (usually fiber optic cables).



iii. WANs

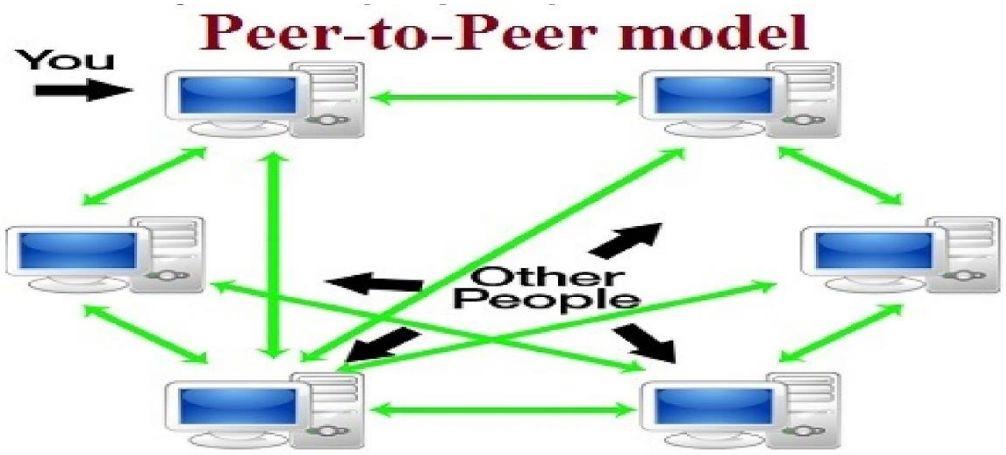
A WAN connects multiple LANs to one another over great geographic distances. The speed available on a WAN varies depending on the cost of the connections, which increases with distance, and may be low. WANs operate using routers, which can "choose" the most appropriate path for data to take to reach a network node. The most well-known WAN is the Internet.



BASIS	LAN	MAN	WAN
Full Form	Local Area Network	Metropolitan Area Network	Wide Area Network
Range	A communication network linking a number of stations in same local area. Range is 1 to 10 km	This network shares the characteristics of packet broadcasting networks. Range is100 km	A communication network distinguished from a Local Area Network. Range is Beyond 100 km
Media Used	Uses guided media(copper twisted pair, copper coaxial cable, optical fiber)	Uses guided as well as unguided media	Uses unguided media(wireless)
Speed	A high speed i.e. 100kbps to 100mbps	Optimized for a large geographical area than LAN.	Long distance communications, which may or may not be provided by public packet network.
Cost	cheaper	costly	expensive
Equipment needed	NIC, switch and hub	Modem and router	Microwave, radio, transmitters and receivers
protocols	Attached Resource	Frame relay and	ATM, FDDI, SMDS

iv. Peer-To-Peer Network (P2P Network)

A peer-to-peer (P2P) network is group of computers, each of which acts as a node for sharing files within the group. Instead of having a central server to act as a shared drive, each computer acts as the server for the files stored upon it. When a P2P network is established over the Internet, a central server can be used to index files, or a distributed network can be established where the sharing of files is split between all the users in the network that are storing a given file.



v. Client-Server Model

A server manages most processes and stores all data. A client requests specified data or processes. The server relays process output to the client. Clients sometimes handle processing, but require server data resources for completion.

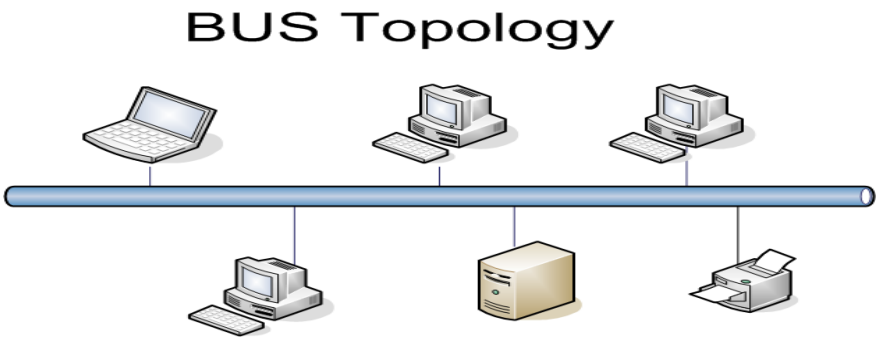
The client-server model differs from a peer-to-peer (P2P) model where communicating systems are the client or server, each with equal status and responsibilities. The P2P model is decentralized networking. The client-server model is centralized networking.

One client-server model drawback is having too many client requests underrun a server and lead to improper functioning or total shutdown. Hackers often use such tactics to terminate specific organizational services through distributed denial-of-service (DDoS) attacks.

C) LAN Topologies

i. Bus Topology

The physical bus topology is the simplest and most widely used of the network designs. It consists of one continuous length of cabling (trunk) and a terminating resistor (terminator) at each end. The data communications message travels along the bus in both directions until it is picked up by a workstation or server NIC.



If the message is missed or not recognized, it reaches the end of the cabling and dissipates at the terminator. All nodes in the bus topology have equal access to the trunk – no discriminating here. This is accomplished using short drop cables or direct T-connectors.

This design is easy to install because the backbone trunk traverses the LAN as one cable segment. This minimizes the amount of transmission media required. Also, the number of devices and length of the trunk can be easily expanded. **Logical Topology: BUS, Physical Topology: BUS.**

Advantages of Bus Topology:

1. It uses established standards and it is relatively easy to install.
2. Requires fewer media than other topologies.

Disadvantages of Bus Topology:

1. The bus networks are difficult to reconfigure, especially when the acceptable number of connections or maximum distances have been reached.
2. They are also difficult to troubleshoot because everything happens on a single media segment. This can have dangerous consequences because any break in the cabling brings the network to its knees.

ii. Ring Topology

As its name implies, the physical ring topology is a circular loop of point-to-point links. Each device connects directly or indirectly to the ring through an interface device or drop cable. Messages travel around the ring from node to node in very organized manner. Each workstation checks the messages for a matching destination address. **Logical Topology: RING, Physical Topology: RING.**

If the address doesn't match, the node simply regenerates the message and sends it on its way. If the address matches, the node accepts the message and sends a reply to the originating sender. Initially, ring topologies are moderately simple to install; however, they require more media than bus systems because the loop must be closed.

Once your ring has been installed, it's a bit more difficult to reconfigure. Ring segments must be divided or replaced every time they're changed. Moreover, any break in the loop can affect all devices on the network.

Advantages of Ring Topology:

1. They are very easy to troubleshoot because each device incorporates a repeater.
2. A special internal feature called becoming, allows the troubled workstation to identify themselves quickly.

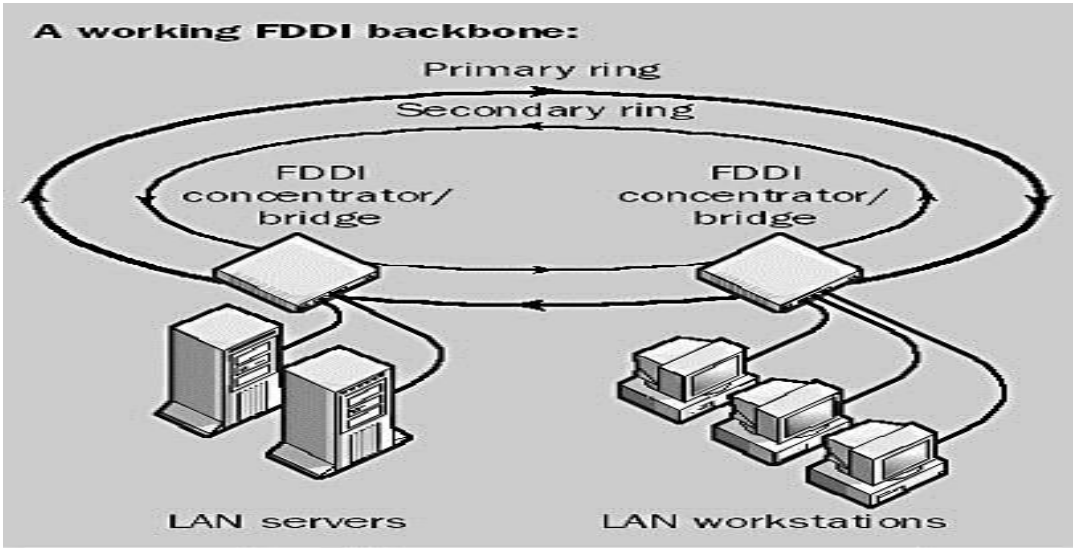
Disadvantages of Ring Topology:

1. It is considerably difficult to install and reconfigure ring topology.
2. Media failure on unidirectional or single loop causes complete network failure.

Fiber Distributed Data Interface (FDDI):

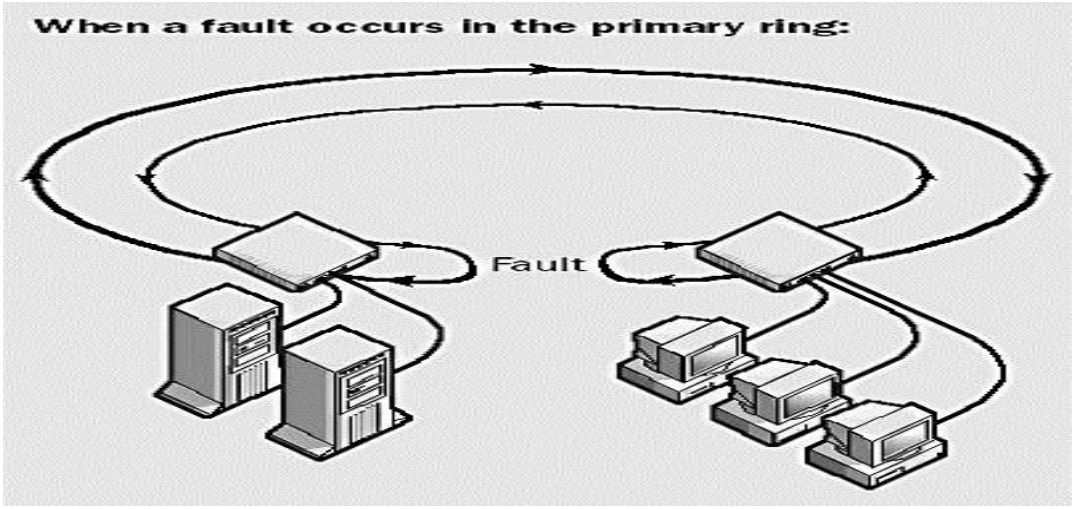
Stands for "Fiber Distributed Data Interface." FDDI is a group of networking specifications standardized by ANSI in the mid-1980s. An FDDI network supports data transfer speeds of 100 Mbps over a fiber optic cable and uses a rotating token to define which system can send data at any given time.

FDDI networks are comprised of two physical paths, or "rings," that transfer data in opposite directions. The primary ring carries data between systems, while the secondary ring is used for redundancy. If a system on the network causes an interruption in the primary data path, the secondary ring is used until the primary ring is functional again. A variation of FDDI, called FDDI Full Duplex Technology (FFDT), uses the secondary ring as an additional primary channel. This type of FDDI network has no redundancy, but supports data transfer rates up to 200 Mbps.



FDDI was designed in the 1980s to provide faster networking than the 10 Mbps Ethernet and 16 Mbps token ring standards available at the time. Because of its high bandwidth, FDDI became a popular choice for high-

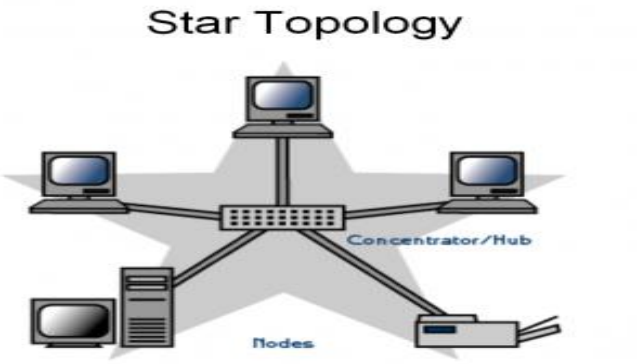
speed backbones used by universities and businesses. While FDDI was the fastest LAN technology for several years, it was eventually superseded by Fast Ethernet, which offered 100 Mbps speeds at a much lower cost. Today, many networks use Gigabit Ethernet, which supports speeds up to 1,000 Mbps.



FDDI uses a timed token-passing technology similar to that of token ring networks as defined in the IEEE 802.5 standard. FDDI stations generate a token that controls the sequence in which other stations will gain access to the wire. The token passes around the ring, moving from one node to the next. When a station wants to transmit information, it captures the token, transmits as many frames of information as it wants (within the specified access period), and then releases the token. This feature of transmitting multiple data frames per token capture is known as a capacity allocation scheme, in contrast to the priority mechanism used in the IEEE 802.5 token ring standard. Every node on the ring checks the frames. The recipient station then reads the information from the frames, and when the frames return to the originating station, they are stripped from the ring.

iii. Star Topology

The Physical star topology uses a central controlling hub with dedicated legs pointing in all directions – like points of a star. Each network devices has a dedicated point-to-point link to the central hub. This strategy prevents troublesome collisions and keeps the line of communication open and free of traffic.



Star topologies are somewhat difficult to install because each device gets its own dedicated segment. Obviously, they require a great deal of cabling. This design provides an excellent platform for reconfiguration and troubleshooting. **Logical Topology: STAR, Physical Topology: BUS.**

Changes to the network are as simple as plugging another segment into the hub. In addition, a break in the LAN is easy to isolate and doesn't affect the rest of the network.

Advantages of Star Topology:

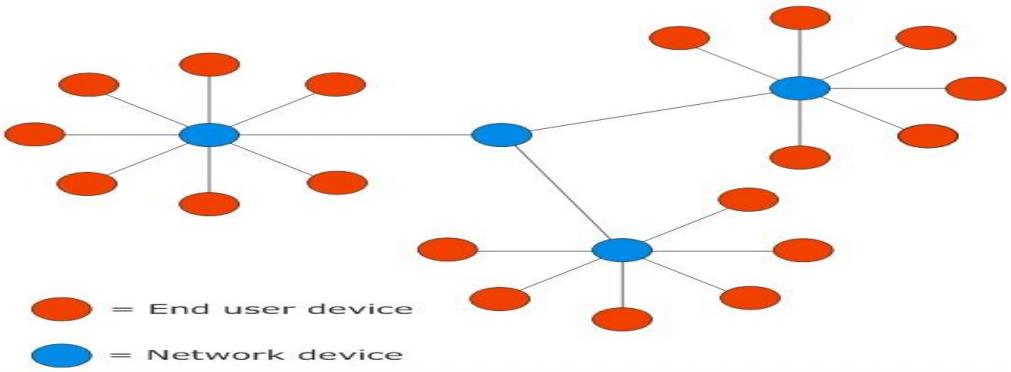
1. Relatively easy to configure.
2. Easy to troubleshoot.
3. Media faults are automatically isolated to the failed segment.

Disadvantages of Star Topology:

1. Requires more cable than most topologies.
2. Moderately difficult to install.'

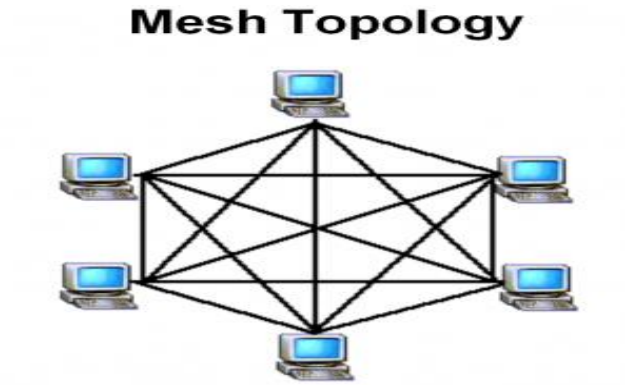
Extended Star Topology:

The extended star topology combines two or more stars. It is used to create large Local Area Networks.
For example in a school or college the workstations in each computer room could form one of the stars within an extended star topology. **Logical Topology: BUS, Physical Topology: E-STAR.**
Alternatively each of the extended stars could be in a different location in a Wide Area Network (WAN).



iv. Mesh Topology

The mesh topology is the only true point-to-point design. It uses a dedicated link between every device on the network. This design is not very practical because of its excessive waste of transmission media. This topology is difficult to install and reconfigure.

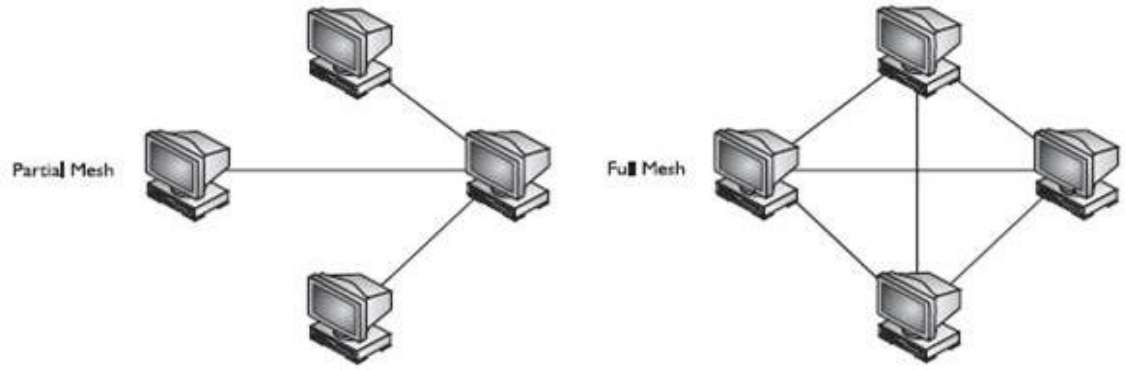


Moreover, as the number of devices increases geometrically, the speed of communication also become slow. ATM (Asynchronous Transfer Mode) and switched Hubs are the example of high-speed Mesh implementation.

There are two types of mesh topologies: full mesh and partial mesh:

- **Full mesh t**opology occurs when every node has a circuit connecting it to every other node in a network. Full mesh is very expensive to implement and yields the greatest amount of redundancy, so in the event that one of those nodes fails, network traffic can be directed to any of the other nodes. Full mesh is usually reserved for backbone networks. **A fully connected mesh topology** has all the nodes connected to every other node. If you know the graph theory, then it is like a fully connected graph where all the nodes are connected to every other node.
- With **partial mesh**, some nodes are organized in a full mesh scheme but others are only connected to one or two in the network. Partial mesh topology is commonly found in peripheral networks connected to a full meshed backbone. It is less expensive to implement and yields less redundancy than full mesh topology. On the other hand, a partially connected mesh topology does not have all the nodes connected to each other.

Total no of connections required for full mesh is given by **n/2(n-1)**, where n is the no of devices or nodes.



Advantages of Mesh Topology:

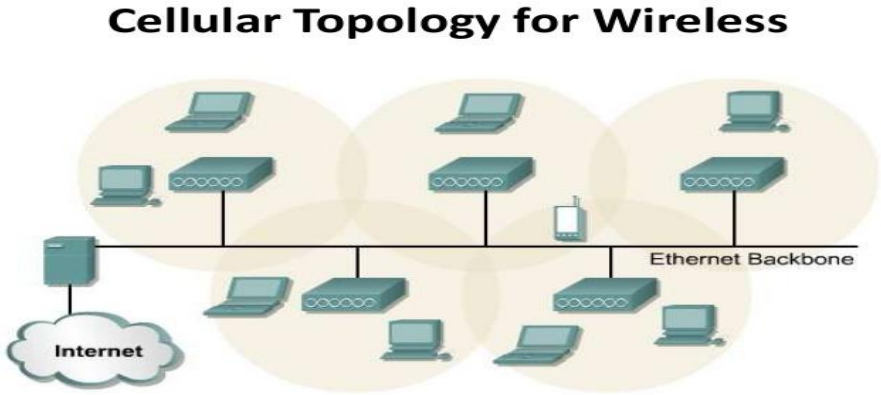
1. Easy to troubleshoot because each link is independent of all others.
2. You can easily identify faults and isolate the affected links. Because of the high number of redundant paths, multiple links can fail before the failure affects any network device.

Disadvantages of Mesh Topology:

1. It is difficult to install and reconfigure especially as the number of devices increases.

v. Cellular Topology

A cellular topology combines wireless point-to-point and multipoint designs to divide a geographic area into cells. Each cell represents the portion of the total network area in which a specific connection operates. Devices within the cell communicate with a central station or hub. Hubs are then interconnected to route data between cells.



The cellular topology relies on the location of wireless media hubs. Cellular networks exhibit interesting characteristics since this topology do not depend on cables. Troubleshooting is easy because each hub interacts independently with each device. A cellular installation depends on the accessibility hub locations.

Advantages of Cellular Topology:

1. It is relatively easy to install.
2. It does not require media reconfiguration when adding or removing users.
3. Fault isolation and troubleshooting is fairly simple.

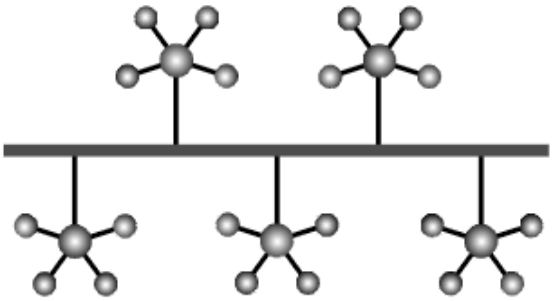
Disadvantages of Cellular Topology:

1. All devices using a particular hub are affected by a hub failure.

vi. Hybrid Topology

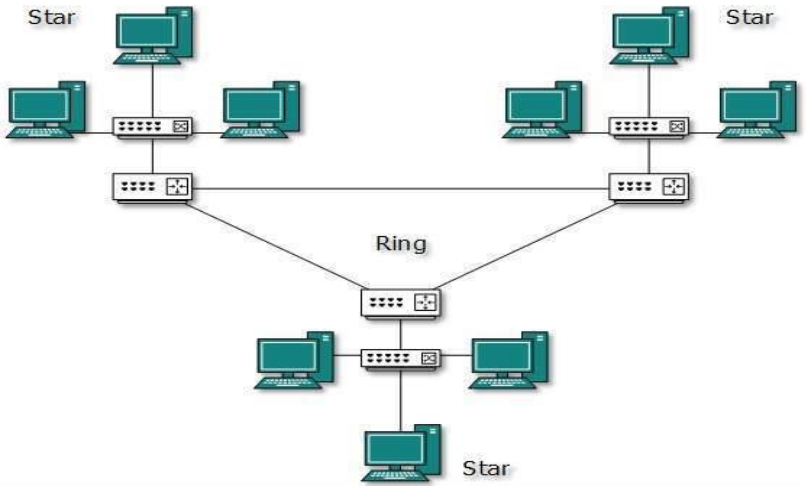
By modifying or combining some of the characteristics of the 'pure' network topologies, a more useful result may be obtained. These combinations are called hybrid topologies. Some of the hybrid topologies are:

1. **Tree network (E-STAR)**



Tree network

2. **Star-Ring or interconnected**



D) Wireless Networks:

Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. The basis of wireless systems are radio waves, an implementation that takes place at the physical level of network structure.

i. Bluetooth

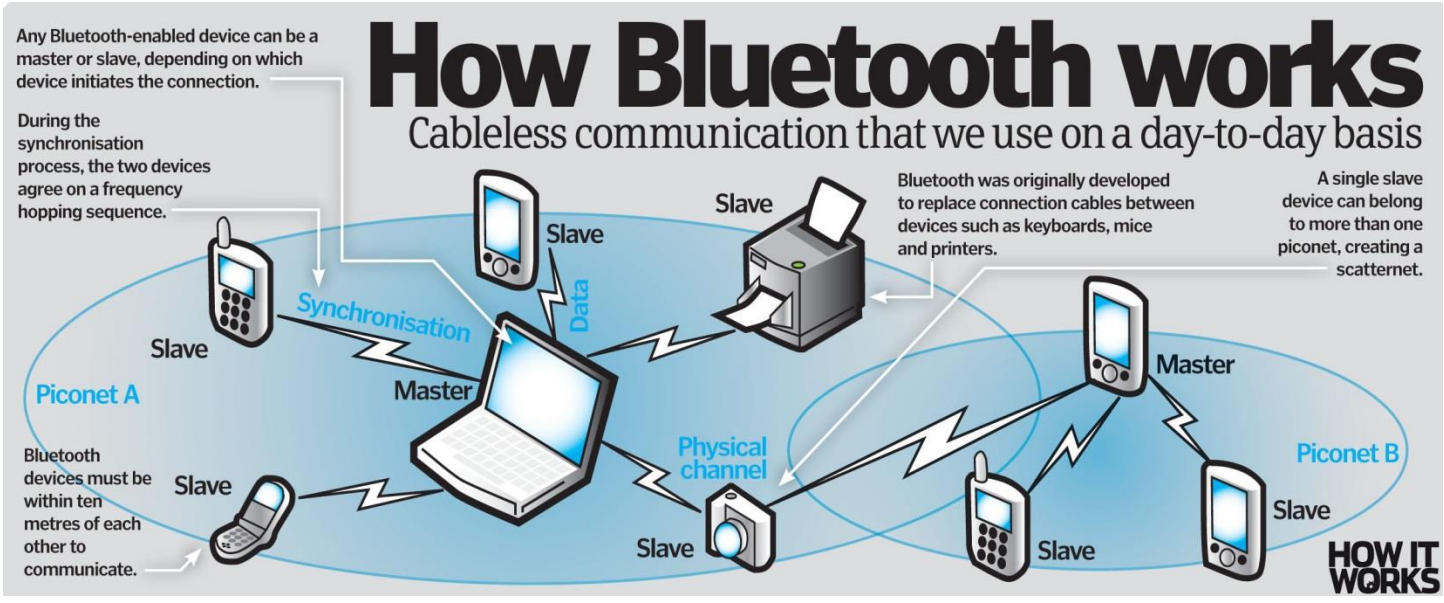
Bluetooth is a specification for the use of low-power radio communications to wirelessly link phones, computers and other network devices over short distances. **A Bluetooth is an ad hoc network**, which means that the network is formed spontaneously. The name Bluetooth is borrowed from Harald Bluetooth, a king in Denmark more than 1,000 years ago. It was originally started as a project by the Ericsson Company.

Bluetooth technology was designed primarily to support simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, and wireless headsets. Wireless signals transmitted with Bluetooth cover short distances, typically **up to 30 feet (10 meters)**. Bluetooth devices generally communicate at **less than 1 Mbps**.

Bluetooth networks feature a dynamic topology called a **piconet** or **PAN**. Piconets contain a **minimum of two and a maximum of eight Bluetooth peer devices**. Devices communicate using protocols that are part of the Bluetooth Specification. Definitions for multiple versions of the Bluetooth specification exist including versions 1.1, 1.2 and 2.0.

Although the Bluetooth standard utilizes the same 2.4 GHz range as 802.11b and 802.11g, Bluetooth technology is not a suitable Wi-Fi replacement. Compared to Wi-Fi, Bluetooth networking is much slower, a bit more limited in range, and supports many fewer devices.

As is true for Wi-Fi and other wireless technologies today, concerns with Bluetooth technology include security and interoperability with other networking standards. Bluetooth was ratified as **IEEE 802.15** standard**.**



ii. Wi-Fi

"Wi-Fi" is the nickname for Wireless Fidelity –a high speed internet and network connection without the use of wires, cables and other stuff. It is a popular technology that allows an electronic device to exchange data wirelessly using radio waves over a computer network, including high-speed Internet connections.

The Wi-Fi Alliance defines Wi-Fi as any wireless local area network (WLAN) products that are based on the IEEE 802.11(Institute of Electrical and Electronics Engineers) standards. However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN".

A device that can use Wi-Fi such as a personal computer, video game console, Smartphone, tablet, or digital audio player can connect to a network resource such as the Internet via a wireless network access point. Such an access point is called hotspot which has a range of about 20 meters indoors and a greater range outdoors. Hotspot coverage can comprise an area as small as a single room with walls that block radio waves or as large as many square miles — this is achieved by using multiple overlapping access points.
Wi-Fi uses different security measures such as WEP, an earliest encryption protocol. But it is easily breakable. Therefore, much higher quality protocols, WPA and WPA2, were added later which provide robust security than the WEP.

WiFi Standards 802.11a/b/g/n /ac:-

1. 802.11b

802.11b uses the same 2.4 GHz frequency as the original 802.11 standard. It supports a maximum theoretical rate of 11 Mbps and has a range up to 150 feet. 802.11b components are cheap, but the standard has the slowest maximum speed of all the 802.11 standards. And since 802.11b operates in the 2.4 GHz, home appliances or other 2.4 GHz Wi-Fi networks can cause interference. Today, routers that only support 802.11n are no longer manufactured.

2. 802.11a

The 'a' amendment to the standard was released at the same time as 802.11b. It introduced a more complex technique, known as OFDM (orthogonal frequency division multiplexing) for generating the wireless signal. 802.11a offers a few advantages over 802.11b: it operates in the less crowded 5 GHz frequency band, making it less prone to interference. And its bandwidth is much higher than 802.11b, with a theoretical max of 54 Mbps. You probably haven't encountered many 802.11a devices or routers. This is because 802.11b devices were cheaper and became more popular in the consumer market. 802.11a was mainly used in business applications.

3. 802.11g

The 802.11g standard uses the same OFDM technology introduced with 802.11a. Like 802.11a, it supports a maximum theoretical rate of 54 Mbps. But like 802.11b, it operates in the crowded 2.4 GHz (and thus is subject to the same interference issues as 802.11b). 802.11g is backward compatible with 802.11b devices: an 802.11b device can connect to an 802.11g access point (but at 802.11b speeds).
With 802.11g, consumers enjoyed a significant advance in Wi-Fi speeds and coverage. At the same time, consumer wireless routers were getting better, with higher power and better coverage than earlier generations.

4. 802.11n

With the 802.11n standard, Wi-Fi became even faster and more reliable. It supports a maximum theoretical transfer rate of 300 Mbps (and can reach up to 450 Mbps when using three antennae). 802.11n uses MIMO (Multiple Input Multiple Output) where multiple transmitters/receivers operate simultaneously at one or both ends of the link. This provides a significant increase in data without needing a higher bandwidth or transmit power. 802.11n operates in both the 2.4 GHz and 5 GHz bands.

5. 802.11ac

802.11ac supercharges Wi-Fi, with speeds ranging from 433 Mbps all the way up to several Gigabits per second. To achieve this kind of performance, 802.11ac works exclusively in the 5 GHz band, supports up to eight spatial streams (compared with 802.11n's four streams), doubles the channel width up to 80 MHz, and uses a technology called beamforming. With beamforming, the antennae basically transmit the radio signals so they're directed at a specific device.

Another significant advancement with 802.11ac is multi-user (MU-MIMO). While MIMO directs multiple streams to a single client, MU-MIMO can direct the spatial streams to multiple clients simultaneously. While MU-MIMO doesn't increase the speed to any single client, it can increase the overall data throughput of the entire network.

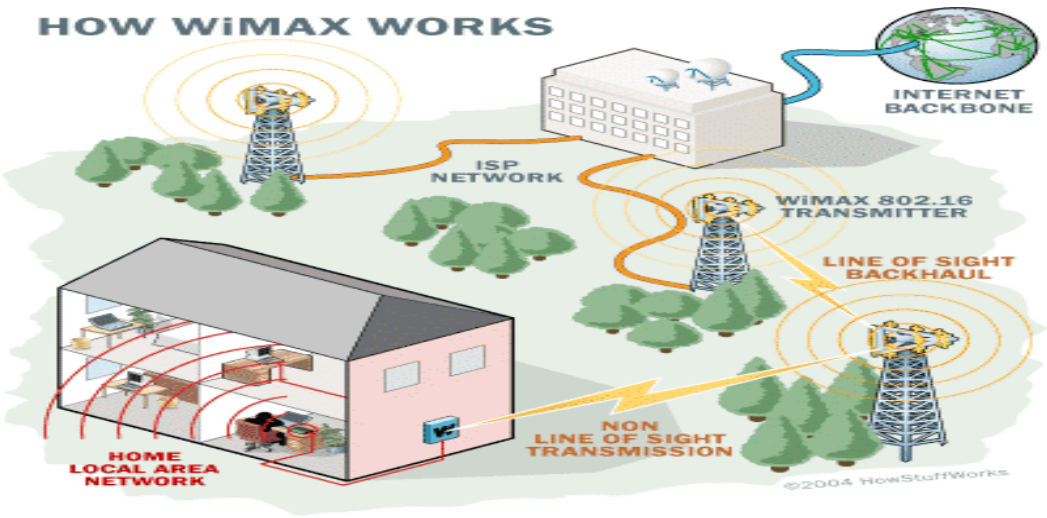
iii. WiMAX

Loosely, WiMax is a standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as Cable Modems, DSL and T1/E1 links) to provide broadband access to customer premises.

More strictly, WiMAX is an industry trade organization formed by leading communications, component, and equipment companies to promote and certify compatibility and interoperability of broadband wireless access equipment that conforms to the IEEE 802.16 and ETSI HIPERMAN standards.

WiMAX is

- Acronym for **Worldwide Interoperability for Microwave Access**.
- Based on Wireless MAN technology.
- A wireless technology optimized for the delivery of IP centric services over a wide area.
- A scalable wireless platform for constructing alternative and complementary broadband networks.
- A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard. The IEEE 802.16 Working Group develops standards that address two types of usage models −
    - A fixed usage model (IEEE 802.16-2004).
    - A portable usage model (IEEE 802.16e).



What is 802.16a ?

The 802.16a standard for 2-11 GHz is a wireless metropolitan area network (MAN) technology that will provide broadband wireless connectivity to Fixed, Portable and Nomadic devices.

WiMax Speed and Range

WiMAX is expected to offer initially up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the particular technical configuration chosen, enough to support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL speed connectivity. WiMAX can support voice and video as well as Internet data. It would not be as fast as in these fixed applications, but expectations are for about 15 Mbps capacity in a 3 km cell coverage area.

Why WiMax ?

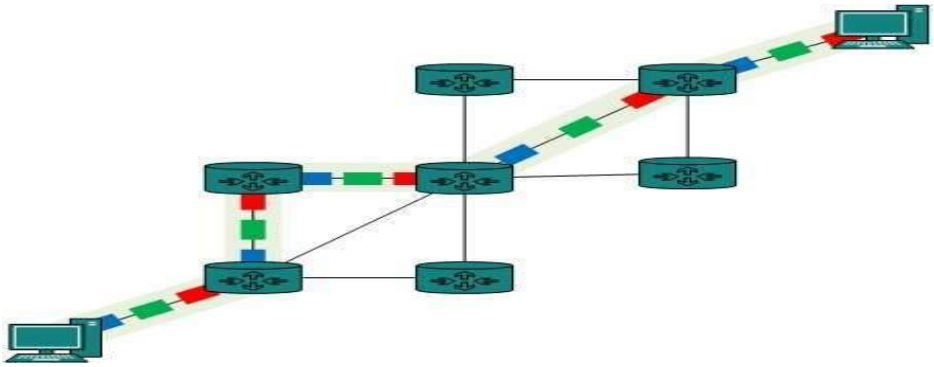
- WiMAX can satisfy a variety of access needs. Potential applications include extending broadband capabilities to bring them closer to subscribers, filling gaps in cable, DSL and T1 services, WiFi, and cellular backhaul, providing last-100 meter access from fibre to the curb and giving service providers another cost-effective option for supporting broadband services.
- WiMAX can support very high bandwidth solutions where large spectrum deployments (i.e. >10 MHz) are desired using existing infrastructure keeping costs down while delivering the bandwidth needed to support a full range of high-value multimedia services.
- WiMAX can help service providers meet many of the challenges they face due to increasing customer demands without discarding their existing infrastructure investments because it has the ability to seamlessly interoperate across various network types.
- WiMAX can provide wide area coverage and quality of service capabilities for applications ranging from real-time delay-sensitive voice-over-IP (VoIP) to real-time streaming video and non-real-time downloads, ensuring that subscribers obtain the performance they expect for all types of communications.
- WiMAX, which is an IP-based wireless broadband technology, can be integrated into both wide-area third-generation (3G) mobile and wireless and wireline networks allowing it to become part of a seamless anytime, anywhere broadband access solution.

e) Switching:

Switching is process to forward packets coming in from one port to a port leading towards the destination.
When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress.

i. Circuit Switching (Connection Oriented Internet-working)

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There 'is a need of pre-specified route from which data will travels and no other data is permitted.In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.
Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases: a) Establish a circuit b) Transfer the data c) Disconnect the circuit

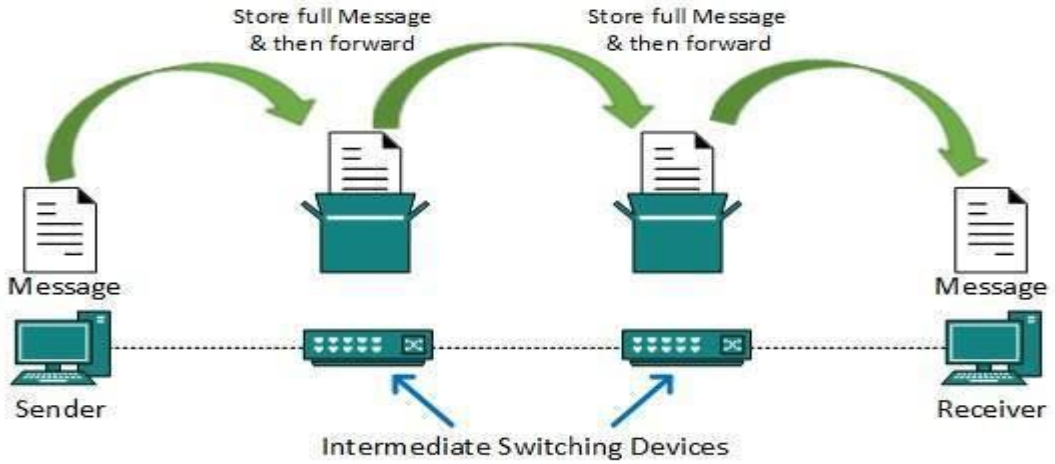


Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

ii. Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.



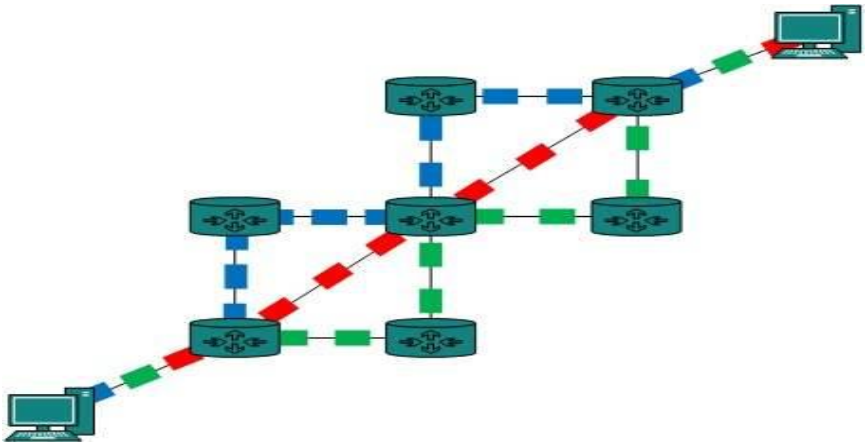
This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

iii. Packet Switching (Connectionless Interworking)

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.



Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

Differentiate between message switching, circuit switching and packet switching.

Sr. No.	Function	Message Switching	Circuit Switching	Packet Switching
1.	Concept	In message switching, each switch stores the whole message and forwards it to the next switch. Although, we don't see message switching at lower layers, it is still used in some applications like electronic mail (e-mail).	When you or your computer places a telephone call, the switching equipment within the telephone system seeks out a physical path all the way from your telephone to the receiver's telephone. This technique is called circuit switching.	With this technology, packets are sent as soon as they are available.
2.	Store and forward transmission	Yes	No	Yes
3.	Terminal	Telegraph, teletype	Telephone, modem	Computer
4.	Information representation	Morse, Baudot, ASCII	Analog Voice or PCM digital voice	Any binary information
5.	Transmission system	Digital over various media	Analog and digital over various media	Digital over various media
6.	Addressing	Geographical addresses	Hierarchical numbering plan	Hierarchical address space
7.	Routing	Manual routing	Route selected during call setup	Each packet routed independently
8.	Multiplexing	Character multiplexing, message multiplexing	Circuit multiplexing	Packet multiplexing shared media across networks
9.	Basic User and Network	Transmission of telegrams (Telegraph network)	Bidirectional real time transfer of voice signals (Telephone network)	Datagram and reliable stream service between computers (Internet).
10.	Call setup	No	Required	Not needed
11.	Dedicated physical path	Not required	Yes	No
12.	Packets arrive in order	-	Yes	No
13.	Each packet follows the same route	-	Yes	No
14.	Bandwidth available	-	Fixed	Dynamic
15.	Time of possible congestion	-	At setup time	On every packet

f) Computer network components

i. Network Interface Card

Network adapter is a device that enables a computer to talk with other computer/network. Using unique **hardware addresses (MAC address)** encoded on the card chip, the data-link protocol employs these addresses to discover other systems on the network so that it can transfer data to the right destination.

There are **two types of network cards**: **wired and wireless**. The wired NIC uses cables and connectors as a medium to transfer data, whereas in the wireless card, the connection is made using antenna that employs radio wave technology. All modern laptop computers incorporated wireless NIC in addition to the wired adapter.

Network Interface card, one of the main computer network components, comes with different speeds, 10Mbps, 100Mbps, and 1000Mbps, so on. Recent standard **network cards built with Gigabit** (1000Mbps) connection speed. It also supports to connect slower speeds such as 10Mbps and 100Mbps. However, the speed of the card depends on your LAN speed.

For example, if you have a switch that supports up to 100Mbps, your NIC will also transfer a data with this same speed even though your computer NIC has still the capability to transfer data at 1000Mbps (1Gbps). In modern computers, network adapter is integrated with a computer motherboard. However if you want advanced and fast Ethernet card, you may buy and install on your computer using the **PCI slot** found on the motherboard (desktop) and **ExpressCard slots** on laptop .

ii. Repeater –

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

iii. Hub –

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

1. **Active Hub :-** These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.
2. **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.

iv. **Bridge** –

A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

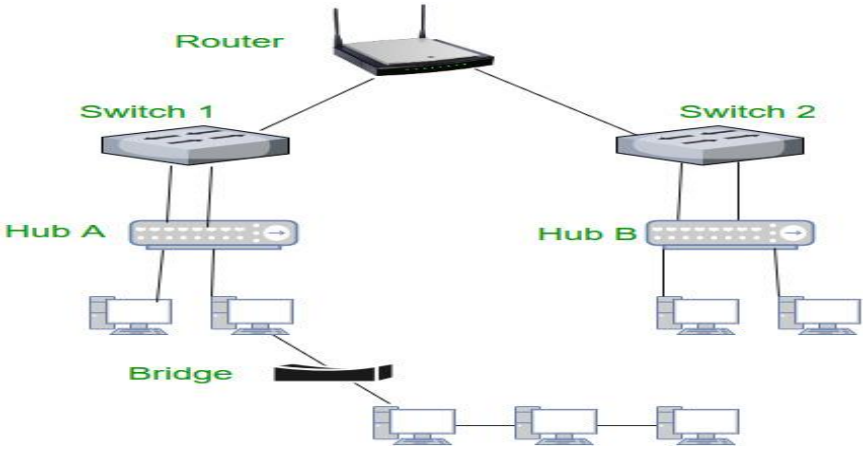
1. **Transparent Bridges :-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of the stations is unnecessary. These bridges makes use of two processes i.e. bridge forwarding and bridge learning.
2. **Source Routing Bridges :-** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The host can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

v. **Switch** –

A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

vi. **Routers** –

A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



vii. **Gateway** –

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

viii. **Brouter** –

It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

G) Layered Architecture, Interfaces, Services and Protocol Architecture:

i. Layered Architecture

Network architectures define the standards and techniques for designing and building communication systems for computers and other devices. To reduce the design complexity, most of the networks are organized as a series of **layers** or **levels**, each one build upon one below it. The basic idea of a layered architecture is to divide the design into small pieces. Each layer adds to the services provided by the lower layers in such a manner that the highest layer is provided a full set of services to manage communications and run the applications. The benefits of the layered models are modularity and clear interfaces, i.e. open architecture and comparability between the different providers' components.

A basic principle is to ensure independence of layers by defining services provided by each layer to the next higher layer without defining how the services are to be performed. This permits changes in a layer without affecting other layers.

The basic elements of a layered model are services, protocols and interfaces.

- A service is a set of actions that a layer offers to another (higher) layer.
- Protocol is a set of rules that a layer uses to exchange information with a peer entity. These rules concern both the contents and the order of the messages used.
- Between the layers service interfaces are defined. The messages from one layer to another are sent through those interfaces.

ii. Interfaces

Interfaces help to transfer messages from one layer to another.

A network interface can refer to any kind of software interface to networking hardware. For instance, if you have two network cards in your computer, you can control and configure each network interface associated with them individually.

A network interface is the point of interconnection between a computer and a private or public network. A network interface is generally a network interface card (NIC), but does not have to have a physical form. Instead, the network interface can be implemented in software.

H) TCP/IP Model

The Internet Protocol Suite, popularly known as the TCP/IP model, is a communication protocol that is used over the Internet. This model divides the entire networking functions into layers, where each layer performs a specific function.

This model gives a brief idea about the process of data formatting, transmission, and finally the reception. Each of these functions takes place in the layers, as described by the model. TCP/IP is a four- layered structure, with each layer having their individual protocol. Let us have a look at the four layers:

1. Link Layer:

As the name suggests, this layer includes the physical and logical connections from the host's link. It is also known as Network Access layer and Network Interface layer. It explains how the data is transmitted from the host, through the network. The physical connectors like the coaxial cables, twisted pair wires, the optical fiber, interface cards, etc., are a part of this layer. This layer can be used to connect different network types like ATM, Token ring, Ethernet, LAN, etc.

2. Internet Layer:

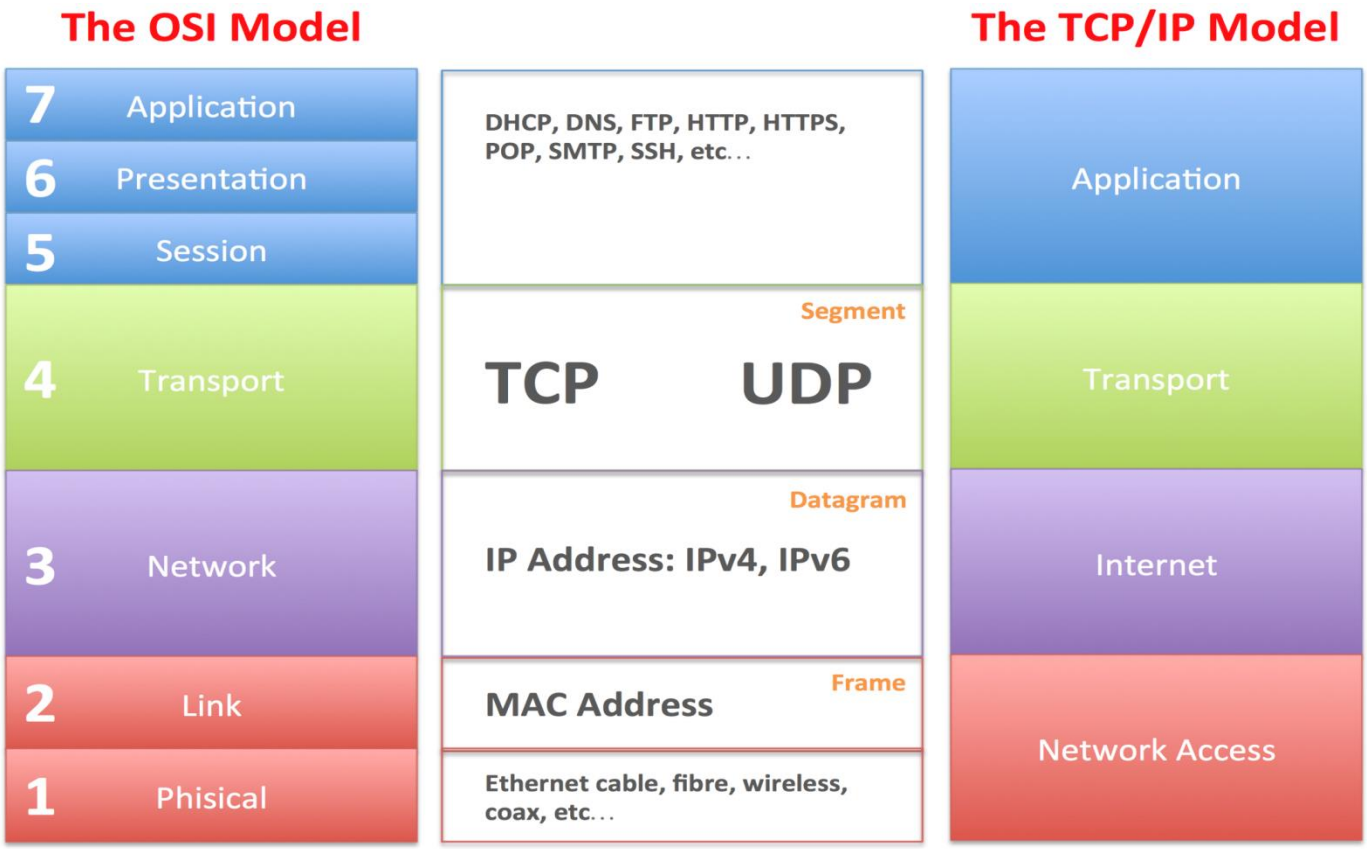
This layer is also known as the Network Layer. The main function of this layer is to route the data to its destination. The data that is received by the link layer is made into data packets (IP datagrams). The data packets contain the source and the destination IP address or logical address. These packets are sent on any network and are delivered independently. This indicates that the data is not received in the same order as it was sent. The protocols at this layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), etc.

3. Transport Layer:

This layer is responsible for providing datagram services to the Application layer. This layer allows the host and the destination devices to communicate with each other for exchanging messages, irrespective of the underlying network type. Error control, congestion control, flow control, etc., are handled by the transport layer. The protocol that this layer uses is TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP gives a reliable, end-to-end, connection-oriented data transfer, while UDP provides unreliable, connectionless data transfer between two computers.

4. Application Layer:

It provides the user interface for communication. This is the layer where email, web browsers or FTP run. The protocols in this layer are FTP, SMTP, HTTP, etc.



I) OSI Model

The Open Systems Interconnected (OSI) model divides the network into seven layers and explains the routing of the data from source to destination. It is a theoretical model which explains the working of the networks. It was developed by the International Organization for Standardization (ISO) for their network suite. Here are the details of OSI's seven layers:

1. **Physical Layer:** As the name suggests, this is the layer where the physical connection between two computers takes place. The data is transmitted via this physical medium to the destination's physical layer. The popular protocols at this layer are Fast Ethernet, ATM, RS232, etc.
   Here are the basic functionalities :
   - Responsible for electrical signals, light signal, radio signals etc.
   - Hardware layer of the OSI layer
   - Devices like repeater, hub, cables, ethernet work on this layer
   - Protocols like RS232, ATM, FDDI, Ethernet work on this layer

2. **Data Link Layer:** The main function of this layer is to convert the data packets received from the upper layer into frames, and route the same to the physical layer. Error detection and correction is done at this layer, thus making it a reliable layer in the model. It establishes a logical link between the nodes and transmits frames sequentially.
   Here are the basic functionalities :
   - Responsible for encoding and decoding of the electrical signals into bits.
   - Manages data errors from the physical layer
   - Convers electrical signals into frames
   - The data link layer is divided into two sub-layers
     - The Media Access Control (MAC) layer

    - Logical Link Control (LLC) layer.
  - The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it.
  - The LLC layer controls frame synchronization, flow control and error checking.
  - MAC address is a part of the layer 2.
  - Devices like Switch work at this layer

3. **Network Layer:** The main function of this layer is to translate the network address into physical MAC address. The data has to be routed to its intended destination on the network. This layer is also responsible to determine the efficient route for transmitting the data to its destination. While doing so, it has to manage problems like network congestion, switching problems, etc. The protocols used here are IP, ICMP, IGMP, IPX, etc.
   Here are the basic functionalities of the network layer:
   - Switching and routing technologies work here
   - Creates logical paths between two hosts across the world wide web called as virtual circuits
   - Routes the data packet to destination
   - Routing and forwarding of the data packets.
   - Internetworking, error handling, congestion control and packet sequencing work at this layer
   - Router works at layer three
   - Different network protocols like TCP/ IP, IPX, AppleTalk work at this layer

4. **Transport Layer:** This layer provides end-to-end delivery of data between two nodes. It divides data into different packets before transmitting it. On receipt of these packets, the data is reassembled and forwarded to the next layer. If the data is lost in transmission or has errors, then this layer recovers the lost data and transmits the same.
   Here are the basic functionalities of the Transport layer:
   - Responsible for the transparent transfer of data between end systems
   - Responsible for end-to-end error recovery and flow control
   - Responsible for complete data transfer.
   - Protocols like SPX, TCP, UDP work here

5. **Session Layer:** This layer is responsible to establish and terminate connections between two communicating machines. This connection is known as a session, hence the name. It establishes full-duplex, half-duplex and simplex connection for communication. The sessions are also used to keep a track of the connections to the web server.
   Here are the basic functionalities of the Session layer:
   - Responsible for establishment, management and termination of connections between applications.
   - The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end.
   - It deals with session and connection coordination.
   - Protocols like NFS, NetBios names, RPC, SQL work at this layer.

6. **Presentation Layer:** The data conversion takes place at this layer. The data that it receives from the application layer is converted into a suitable format that is recognized by the computer. For example, the conversion of a file from .wav to .mp3 takes place at this layer.

Here are the basic functionalities of the presentation layer:

- Responsible for data representation on your screen
- Encryption and decryption of the data
- Data semantics and syntax
- Layer 6 Presentation examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.

7. **Application Layer:** This layer provides a user interface by interacting with the running application. E-mail, FTP, web browsers, etc. are the network applications that run on this layer.
   Here are the basic functionalities of the Application layer:
   - Application layer supports application, apps, and end-user processes.
   - Quality of service
   - This layer is responsible for application services for file transfers, e-mail, and other network software services.
   - Protocols like Telnet, FTP, HTTP work on this layer.

Difference between OSI Layer & TCP/IP Layer

TCP/IP	OSI
It has 4 layers.	It has 7 layers.
TCP/IP Protocols are considered to be standards around which the internet has developed.	OSI Model however is a "generic, protocol-independent standard."
Follows Vertical Approach	Follows Horizontal Approach
In TCP/IP Model, Transport Layer does not Guarantees delivery of packets.	In OSI Model, Transport Layer Guarantees delivery of packets.
Network Layer in TCP/IP Model provides only Connectionless service.	Network Layer in OSI Model provides both Connection-Oriented & Connection less service.
Replacing Protocol is not easy.	Protocols are hidden in OSI model & are easily replaced as the technology changes.
TCP/IP protocols are the standards around which the internet was developed therefore it mainly gains creditability due to this reason.	Where as in contrast networks are not usually built around the OSI model as it is merely used as a guidance tool.
Not found in TCP/IP model. In TCP/IP, its characteristics are provided by the TCP protocol.	The Session layer permits two parties to hold ongoing communications called a session across a network.
The TCP/IP network model represents reality in the world.	Whereas the OSI mode represents an ideal.
Combines the session and presentation layer in the application layer.	Has separate session and presentation layer.
Protocols were developed first and then the model was developed.	Model was developed before the development of protocols.
Protocol dependent standard.	Protocol independent standard.